Comment Report

Project Name:	2016-02 Modifications to CIP Standards | Virtualization - Draft 5
Comment Period Start Date:	10/3/2023
Comment Period End Date:	11/29/2023
Associated Ballots:	2016-02 Modifications to CIP Standards | Virtualization CIP-003-9 AB 5 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-004-7 AB 5 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-005-8 AB 5 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-007-7 AB 5 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-010-5 AB 5 ST

There were 71 sets of responses, including comments from approximately 185 different people from approximately 116 companies representing 10 of the Industry Segments as shown in the table on the following pages.

Questions

1. The SDT modified the IRA definition, CIP-005 R2 and CIP-004 Applicable Systems to address IRA in routable to nonroutable (i.e., IP to serial) conversion scenarios. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

2. The SDT modified other (not related to IRA) 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 R1 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 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.

6. The SDT revised CIP-003. Do you agree with the proposed changes to these Reliability Standards? If not, please provide the basis for your disagreement and an alternate proposal.

7. The SDT revised the Implementation Plan to accommodate for the future enforceable date of CIP-003-9. Do you agree with the proposed Implementation Plan? If not, please provide the basis for your disagreement and an alternate proposal.

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

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
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
MRO	Anna Martinson	1,2,3,4,5,6	MRO	MRO Group	Shonda McCain	Omaha Public Power District (OPPD)	1,3,5,6	MRO
					Michael Brytowski	Great River Energy	1,3,5,6	MRO
					Jamison Cawley	Nebraska Public Power District	1,3,5	MRO
					Jay Sethi	Manitoba Hydro (MH)	1,3,5,6	MRO
					Jaimin Patal	Saskatchewan Power Corporation (SPC)	1	MRO
					Kimberly Bentley	Western Area Power Adminstration	1,6	MRO
					Marc Gomez	Southwestern Power Administration (SWPA)	1	MRO
					Fred Meyer	Algonquin Power Co.	3	MRO
					George Brown	Pattern Operators LP	5	MRO
					Larry Heckert	Alliant Energy (ALTE)	4	MRO
					Terry Harbour	MidAmerican Energy Company (MEC)	1,3	MRO
					Bryan Sherrow	Board Of	1	MRO

						Public Utilities (BPU)		
					Seth Shoemaker	Muscatine Power & Water	1,3,5,6	MRO
					Bobbi Welch	Midcontinent ISO, Inc.	2	MRO
					Michael Ayotte	ITC Holdings	1	MRO
Public Utility District No. 1 of Chelan County	Anne Kronshage	6		Public Utility District No. 1 of Chelan County - Voting Group	Anne Kronshage	Public Utility District No. 1 of Chelan County	6	WECC
					Diane Landry	Public Utility District No. 1 of Chelan County	1	WECC
					Rebecca Zahler	Public Utility District No. 1 of Chelan County	5	WECC
					Joyce Gundry	Public Utility District No. 1 of Chelan County	3	WECC
Tennessee Valley Authority	Brian Millard	1,3,5,6	SERC	TVA RBB	Ian Grant	Tennessee Valley Authority	3	SERC
					David Plumb	Tennessee Valley Authority	1	SERC
					Armando Rodriguez	Tennessee Valley Authority	6	SERC
					Nehtisha Rollis	Tennessee Valley Authority	5	SERC
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
					John Nierenberg	Tacoma Public Utilities (Tacoma, WA)	3	WECC
					Hien Ho	Tacoma Public Utilities	4	WECC

						(Tacoma, WA)		
					Terry Gifford	Tacoma Public Utilities (Tacoma, WA)	6	WECC
					Ozan Ferrin	Tacoma Public Utilities (Tacoma, WA)	5	WECC
ACES Power Marketing	Jodirah Green	1,3,4,5,6	MRO,RF,SERC,Texas RE,WECC	ACES Collaborators	Bob Soloman	Hoosier Energy Electric Cooperative	1	RF
					Nick Fogleman	Prairie Power, Inc.	1,3	SERC
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Jennifer Bray	Arizona Electric Power Cooperative, Inc.	1	WECC
					Marcus Perkins	Southern Maryland Electric Cooperative	3	RF
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
					Mark Garza	FirstEnergy-FirstEnergy	1,3,4,5,6	RF
					Stacey Sheehan	FirstEnergy - FirstEnergy Corporation	6	RF
California ISO	Monika Montez	2	WECC	ISO/RTO Council Standards Review Committee (SRC)	Monika Montez	CAISO	2	WECC
					Bobbi Welch	Midcontinent ISO, Inc.	2	RF
					Kathleen Goodman	ISO-NE	2	NPCC
					Gregory Campoli	New York Independent	2	NPCC

						System Operator		
					Helen Lainis	IESO	2	NPCC
					Charles Yeung	Southwest Power Pool, Inc. (RTO)	2	MRO
					Kennedy Meier	Electric Reliability Council of Texas, Inc.	2	Texas RE
					Elizabeth Davis	PJM	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
					Leslie Burke	Southern Company - Southern Company Generation	5	SERC
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	NPCC RSC	Gerry Dunbar	Northeast Power Coordinating Council	10	NPCC
					Alain Mukama	Hydro One Networks, Inc.	1	NPCC
					Deidre Altobell	Con Edison	1	NPCC
					Jeffrey Streifling	NB Power Corporation	1	NPCC
					Michele Tondalo	United Illuminating Co.	1	NPCC
					Stephanie Ullah-Mazzuca	Orange and Rockland	1	NPCC

Michael Ridolfino	Central Hudson Gas & Electric Corp.	1	NPCC
Randy Buswell	Vermont Electric Power Company	1	NPCC
James Grant	NYISO	2	NPCC
John Pearson	ISO New England, Inc.	2	NPCC
Harishkumar Subramani Vijay Kumar	Independent Electricity System Operator	2	NPCC
Randy MacDonald	New Brunswick Power Corporation	2	NPCC
Dermot Smyth	Con Ed - Consolidated Edison Co. of New York	1	NPCC
David Burke	Orange and Rockland	3	NPCC
Peter Yost	Con Ed - Consolidated Edison Co. of New York	3	NPCC
Salvatore Spagnolo	New York Power Authority	1	NPCC
Sean Bodkin	Dominion - Dominion Resources, Inc.	6	NPCC
David Kwan	Ontario Power Generation	4	NPCC
Silvia Mitchell	NextEra Energy - Florida Power and Light Co.	1	NPCC
Glen Smith	Entergy Services	4	NPCC
Sean Cavote	PSEG	4	NPCC
Jason Chandler	Con Edison	5	NPCC
Tracy MacNicoll	Utility Services	5	NPCC

					Shivaz Chopra	New York Power Authority	6	NPCC
					Vijay Puran	New York State Department of Public Service	6	NPCC
					ALAN ADAMSON	New York State Reliability Council	10	NPCC
					David Kiguel	Independent	7	NPCC
					Joel Charlebois	AESI	7	NPCC
					Joshua London	Eversource Energy	1	NPCC
Shannon Mickens	Shannon Mickens		MRO,SPP RE,WECC	SPP RTO	Shannon Mickens	Southwest Power Pool Inc.	2	MRO
					Mia Wilson	Southwest Power Pool Inc.	2	MRO
					Josh Phillips	Southwest Power Pool Inc.	2	MRO
					Shelly Young	Southwest Power Pool Inc.	2	MRO
					David Minick	Southwest Power Pool Inc.	2	MRO
					Mike Wikerson	Southwest Power Pool Inc.	2	MRO
					Chris Evans	Southwest Power Pool Inc.	2	MRO
					Barry Bull	Southwest Power Pool Inc.	2	MRO
					Rebecca Sanders	Southwest Power Pool Inc.	2	MRO
					Steve Shirley	Southwest Power Pool Inc.	2	MRO

					Cheryl Kirk	Southwest Power Pool Inc.	2	MRO
Western Electricity Coordinating Council	Steven Rueckert	10		WECC CIP	Steve Rueckert	WECC	10	WECC
					Morgan King	WECC	10	WECC
					Deb McEndaffer	WECC	10	WECC
					Tom Williams	WECC	10	WECC
Tim Kelley	Tim Kelley		WECC	SMUD and BANC	Nicole Looney	Sacramento Municipal Utility District	3	WECC
					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
					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	1	NPCC

						Cooperative, Inc.		
					John Stickley	NW Electric Power Cooperative, Inc.	3	SERC
					Tony Gott	KAMO Electric Cooperative	3	SERC
					Micah Breedlove	KAMO Electric Cooperative	1	SERC
					Kevin White	Northeast Missouri Electric Power Cooperative	1	SERC
					Skyler Wiegmann	Northeast Missouri Electric Power Cooperative	3	SERC
					Ryan Ziegler	Associated Electric Cooperative, Inc.	1	SERC
					Brian Ackermann	Associated Electric Cooperative, Inc.	6	SERC
					Brad Haralson	Associated Electric Cooperative, Inc.	5	SERC

1. The SDT modified the IRA definition, CIP-005 R2 and CIP-004 Applicable Systems to address IRA in routable to nonroutable (i.e., IP to serial) conversion scenarios. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

Sean Steffensen - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	
Comment	
Edited	
Likes 0	
Dislikes 0	
Response	

James Keele - Entergy - 1,3,6	
Answer	No
Document Name	
Comment	

CIP-004-7 - R6.1.2 provisioned physical access to physical BCSI (except for BCSI at a medium impact BCS without ERC). The definition which is listed in the CIP-004-8 Technical Rationales and justification states:

For BCSI in physical format, physical access is provisioned to a physical storage location designated for BCSI and for which access can be provisioned, such as a lockable file cabinet.

By the NERC definition of “Physical Access” ERC does not exist. The additional language of (except for BCSI at a medium impact BCS without ERC) should be removed since a lockable file cabinet is not able to have External Routable Connectivity (ERC) making this statement mute.

The term: Interactive Remote Access (IRA) needs to be defined before it is introduced in a NERC Requirement. It is listed in the Technical Rationale, there is no definition. List the difference between IRA and ERC. If you have ERC, you have IRA. You cannot have either with “Physical Access” as defined as stated above.

Remove R6.1.2 and refer to is as access to BCSI whether it is electronic or physical. Make it simple. You either have been granted access to BCSI or you have not. For R4.1.2 it doesn’t matter if the PSP has ERC or not. Access is access. By adding in ERC, it makes the entity to perform more work and create more policies that do not provide any more security. It makes the compliance piece harder to meet while not gaining any security.

Take guidance from the Nuclear Regulatory Commission (NRC) on Critical Group Membership. You either a critical group member or you are not. Critical group membership allows an individual to work on critical digital assets, whether it is physical or electronical. 1 access control for both types of access.

Medium impact BCS with IRA SCI supporting an Applicable System in this Part – this section needs more clarity on what it is asking the entity to look for. Measures would need to be added to better understand what the ask is.

Likes 0	
Dislikes 0	

Response

Anne Kronshage - Public Utility District No. 1 of Chelan County - 6, Group Name Public Utility District No. 1 of Chelan County - Voting Group

Answer	No
Document Name	

Comment

The SDT has created two different ways of scoping IRA with the current draft of the definition of IRA. In the first case, RE's determine if in-scope IRA exists within the definition, by deciding if the destination Cyber System is inside an ESP (as there are no cases where a Cyber System would be inside an ESP but would not be an Applicable System), while the second case requires RE's to first use the definition to determine if the a protocol conversion is taking place, then use the Applicable Systems of CIP-005 R2 to determine if the destination device is in-scope.

For example, in case 1: An EMS Server (high impact BCA) is inside an ESP. An engineer logs into the EMS server from a jump host outside the ESP. This access meets the first criteria of the definition IRA, and we don't need the Applicable Systems of CIP-005 R2 to determine it is in-scope because all such access would be in-scope.

Case 2: A comm server hosts telnet servers that translate IP to serial for a RTU at a remote site. A employee can initiate a telnet session to the comm server to remotely program the device. This device DOES meet the definition of IRA. But we cannot determine if it is in-scope IRA without knowing the RTU's classification. If the device is low impact or not BES, it is technically IRA, but has no requirements.

The SDT should make scoping of what is in-scope and what is out-of-scope consistent between all types of IRA. CHPD recommends an approach that classifies all remote access as IRA and only places requirements on IRA that originates from a device outside the ESP to a high or medium BCS or PCA.

Additionally, the definition of Intermediate System remains ambiguous as to whether it can cover such devices as Active Directory servers or even firewalls. The terminology should be changed to define the Intermediate System to be the device that IRA is restricted to, not the device that does the restriction (which is not the Intermediate System, but is the firewall and domain policy server).

CHPD's recommendation is as follows:

Definitions:

Interactive Remote Access - User-initiated, interactive electronic access by a person using a bi-directional routable protocol:

- To a routable Cyber System
- That is converted to a non-routable protocol that allows interactive access to a Cyber System
- To a Management Interface

Intermediate System - An Electronic Access Control or Monitoring System(s) that Interactive Remote Access to BES is permitted to originate from.

CIP-005 R2.1

Applicable Systems - High impact BCS and their PCA(s); Medium impact BCS and their PCA(s)

Requirement - Permit Interactive Remote Access (IRA) from outside an ESP, if any, only from an Intermediate System.

CIP-005 R2.2-R2.7 - Unchanged

Thus, all interactive remote access is "IRA", but only IRA that originates from outside an ESP to an Applicable System is in-scope of CIP-005 R2. The system-to-system exemption is no longer needed, as the access has to be "interactive" per the definition of IRA. The ESP-to-ESP exemption is also no longer needed, as that type of communication naturally falls out-of-scope of the updated R2.1 language. And the non-routable concern is brought into the fold by the second bullet point of the definition of IRA.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

FirstEnergy suggests including the following in the proposed IRA Definition:

· User-initiated electronic access by a person using a bi-directional routable protocol:

· That is converted by the responsible entity to a non-routable protocol that allows access to a Cyber System **when conversion is performed by an device located outside of the ESP of the Cyber System**

Likes 0	
Dislikes 0	

Response

Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC

Answer	No

Document Name	
Comment	
SMUD and BANC appreciate the Standard Drafting Team's work to modify the IRA definition. In the second bullet of the proposed definition, we recommend changing the words "To a Cyber System…" to "To a BES Cyber System…" so that the scope is not expanded to non-BES, EACMS and PACS.	
Likes 0	
Dislikes 0	
Response	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	
The gap between what is system-to-system communications and what is Interactive Remote Access (IRA) with the new IRA definition should addressed. Entities often rely on IRA ports for system-to-system communication but have not adequately enforced protections or deployed additional internal controls to ensure that malicious actors do not use the ports, or the ports are used later to establish user-initiated remote access. Additional technical measures or controls should be added to a new definition to ensure validity of declared system-to-system communications to Applicable Systems are not used for IRA. In addition, approval of CIP-005-8, with the modified IRA definition, is still conditional, based upon approval of the entire suite of proposed CIP definitions associated with virtualization and SCI terminology. With no formal definition of system-to-system, there is still lingering issues regarding where this fine line between system-to-system and IRA exists. By stipulating system-to-system communications excludes the ability for direct user-initiated electronic access at any time, better delineates IRA from system-to-system communications. Suggested Interactive Remote Access definition: User-initiated electronic access by a person using a bi-directional routable protocol: To a Cyber System protected by an Electronic Security Perimeter(s) (ESP); That is converted by the responsible entity to a non-routable protocol that allows access to a Cyber System; or To a Management Interface. Interactive Remote Access does not include: Communication that originates from a Cyber System protected by any of the Responsible Entity's ESPs; or System-to-system process communications that cannot be used to establish user-initiated electronic access.	
Likes 0	
Dislikes 0	
Response	

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	No
Document Name	
Comment	
Although IP to Serial Converters are devices within a ESP and PSP environment in which they could be manipulated if the network is compromised, they can not be directly interacted with through interactive remote access. The serial based systems down stream of the converter would only operate on non-routable serial communications protocol. The language as proposed inappropriately brings these non-IRA devices into scope of this requirement.	
Likes 0	
Dislikes 0	
Response	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	No
Document Name	
Comment	
Do not agree with the statement, "That is converted by the responsible entity to a non-routable protocol that allows access to a Cyber System;" When read, the wording implies that the connection must always be coverted to a non-routable protocol. A more correct statement would be, "To include connections, which are converted by the responsible entity to a non-routable protocol that allows access to a Cyber System".	
Likes 0	
Dislikes 0	
Response	
Ben Hammer - Western Area Power Administration - 1	
Answer	No
Document Name	
Comment	
The use of a non routable protocol ip to serial does not cover scenarios where an intermediate system is used first to get to the protocol converter. For example, a utility using a centralized EACMS (intermediate server) placed infront of the protocol converter that mitigates the security risks.	
Likes 0	

Dislikes 0	

Response

Sheila Suurmeier - Black Hills Corporation - 5	
Answer	No
Document Name	

Comment
Black Hills Corporation requests the standards drafting team consider defining the term “system-to-system process communications” as it is referenced in the current and proposed definition of Interactive Remote Access (IRA). Clearly identifying “system-to-system process communications” versus IRA would allow entities to know which controls need to be applied. The SDT should make scoping of what is in-scope and what is out-of-scope consistent between all types of IRA. We recommend an approach that classifies all remote access as IRA and only places requirements on IRA that originates from a device outside the ESP to a high or medium BCS or PCA. Additionally, the definition of Intermediate System remains ambiguous as to whether it can cover such devices as Active Directory servers or even firewalls. The terminology should be changed to define the Intermediate System to be the device that IRA is restricted to, not the device that does the restriction (which is not the Intermediate System, but is the firewall and domain policy server). Our recommendation is as follows: Definitions: **Interactive Remote Access** - User-initiated electronic access by a person using a bi-directional routable protocol: • To a Cyber System protected by an Electronic Security Perimeter(s) (ESP); • That is converted by the responsible entity to a non-routable protocol that allows access to a Cyber System; or • To a Management Interface. Interactive Remote Access does not include:Communication that originates from a Cyber System protected by any of the Responsible Entity’s ESPs; or System-to-system process communications that cannot be used to establish user-initiated electronic access.

Likes 0	
Dislikes 0	

Response

Rachel Schuldt - Rachel Schuldt On Behalf of: Claudine Bates, Black Hills Corporation, 5, 6, 1, 3; - Rachel Schuldt	
Answer	No
Document Name	

Comment

Black Hills Corporation requests the standards drafting team consider defining the term “system-to-system process communications” as it is referenced in the current and proposed definition of Interactive Remote Access (IRA). Clearly identifying “system-to-system process communications” versus IRA would allow entities to know which controls need to be applied.

The SDT should make scoping of what is in-scope and what is out-of-scope consistent between all types of IRA. We recommend an approach that classifies all remote access as IRA and only places requirements on IRA that originates from a device outside the ESP to a high or medium BCS or PCA.

Additionally, the definition of Intermediate System remains ambiguous as to whether it can cover such devices as Active Directory servers or even firewalls. The terminology should be changed to define the Intermediate System to be the device that IRA is restricted to, not the device that does the restriction (which is not the Intermediate System, but is the firewall and domain policy server).

Our recommendation is as follows:

Definitions:

Interactive Remote Access -

User-initiated electronic access by a person using a bi-directional routable protocol:

- To a Cyber System protected by an Electronic Security Perimeter(s) (ESP);
- That is converted by the responsible entity to a non-routable protocol that allows access to a Cyber System; or
- To a Management Interface.

Interactive Remote Access does not include:

Communication that originates from a Cyber System protected by any of the Responsible Entity’s ESPs; or

System-to-system process communications that cannot be used to establish user-initiated electronic access.

Likes 0	
Dislikes 0	

Response

Josh Combs - Black Hills Corporation - 3

Answer	No
Document Name	

Comment

Black Hills Corporation requests the standards drafting team consider defining the term “system-to-system process communications” as it is referenced in the current and proposed definition of Interactive Remote Access (IRA). Clearly identifying “system-to-system process communications” versus IRA would allow entities to know which controls need to be applied.

The SDT should make scoping of what is in-scope and what is out-of-scope consistent between all types of IRA. We recommend an approach that classifies all remote access as IRA and only places requirements on IRA that originates from a device outside the ESP to a high or medium BCS or PCA.

Additionally, the definition of Intermediate System remains ambiguous as to whether it can cover such devices as Active Directory servers or even

firewalls. The terminology should be changed to define the Intermediate System to be the device that IRA is restricted to, not the device that does the restriction (which is not the Intermediate System, but is the firewall and domain policy server).

Our recommendation is as follows:

Definitions:

Interactive Remote Access -

User-initiated electronic access by a person using a bi-directional routable protocol:

- To a Cyber System protected by an Electronic Security Perimeter(s) (ESP);
- That is converted by the responsible entity to a non-routable protocol that allows access to a Cyber System; or
- To a Management Interface.

Interactive Remote Access does not include:

Communication that originates from a Cyber System protected by any of the Responsible Entity's ESPs; or System-to-system process communications that cannot be used to establish user-initiated electronic access.

Likes 0	
Dislikes 0	

Response

Micah Runner - Black Hills Corporation - 1

Answer	No
Document Name	

Comment

Black Hills Corporation requests the standards drafting team consider defining the term "system-to-system process communications" as it is referenced in the current and proposed definition of Interactive Remote Access (IRA). Clearly identifying "system-to-system process communications" versus IRA would allow entities to know which controls need to be applied.

The SDT should make scoping of what is in-scope and what is out-of-scope consistent between all types of IRA. We recommend an approach that classifies all remote access as IRA and only places requirements on IRA that originates from a device outside the ESP to a high or medium BCS or PCA.

Additionally, the definition of Intermediate System remains ambiguous as to whether it can cover such devices as Active Directory servers or even firewalls. The terminology should be changed to define the Intermediate System to be the device that IRA is restricted to, not the device that does the restriction (which is not the Intermediate System, but is the firewall and domain policy server).

Our recommendation is as follows:

Definitions:

Interactive Remote Access -

User-initiated electronic access by a person using a bi-directional routable protocol:

- To a Cyber System protected by an Electronic Security Perimeter(s) (ESP);
- That is converted by the responsible entity to a non-routable protocol that allows access to a Cyber System; or
- To a Management Interface.

Interactive Remote Access does not include:

Communication that originates from a Cyber System protected by any of the Responsible Entity's ESPs; or

System-to-system process communications that cannot be used to establish user-initiated electronic access.

Likes 0	
Dislikes 0	

Response

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 comment and offers the following.

BC Hydro requests clarity on the definition of Interactive Remote Access (IRA) for the following reason: IRA definition (second bullet) uses the words "To a Cyber System..." which could lead to the understanding that the scope is expanded to non-BES, EACMS and PACS.

BC Hydro proposes that the wording is changed to "To a BES Cyber System..." to make it clear.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

MPC supports comments submitted by ACES.

Likes 0	
Dislikes 0	

Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	
NIPSCO does not agree with the proposed definition. The new definition of IRA seems to be virtually the same as ERC. It is a distinction without much of a difference.	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Shannon Mickens On Behalf of: Joshua Phillips, Southwest Power Pool, Inc. (RTO), 2; - Shannon Mickens, Group Name SPP RTO	
Answer	No
Document Name	
Comment	
Due to the non-routable protocol’s inability to cross an EAP, the definition of Interactive Remote Access (IRA) should not apply. Given this limitation, the ability to cross an EAP to access a Cyber Asset within the ESP should have its definition limited to only routable protocols.	
Likes 0	
Dislikes 0	
Response	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	No
Document Name	
Comment	
NCPA suggests editing the new IRA definition to say "To a BCS..." in the first bullet point in lieu of just "Cyber Systems" to avoid including other system types such as EACMS, PACS and PCAs.	
Likes 0	

Dislikes 0	

Response

Nicolas Turcotte - Hydro-Quebec (HQ) - 1	
Answer	No
Document Name	

Comment

HQ supports NPCC RSC comments and provides the following additional comments:

If the goal is to ensure that user interactive actions, is done remotely(i.e., not in the PSP), on a BCA and PCA, then those actions must go through an intermediate system, and the users must have training, ie CIP-004.

The IRA definition should be simple and not technologically limited (routable vs nonroutable).

The security risks associated to IRA are not dependent on the routable scenarios or routable to nonroutable (i.e., IP to serial) conversion scenarios. They are associated to the remote access.

Furthermore, if the intentionof the IRA definition is to say “Communication that originates from a BCA or a PCA protected by any of the Responsible Entity’s ESPs”, Why is this part of the definition when CIP-005 R1.1 Requires that BCA or a PCA are to be protected by an ESP ?

Also, since CIP-005 R2.4 and R2.5, include System-to-system process communication, I would remove “or System-to-system process communication.” to the definition of IRA as the concept is in the requirements.

SDT should simplify the definition. Suggested improvements include:

IRA: User-initiated electronic access by a person to a BCA or a PCA .

Interactive Remote Access does not include: Out going communication that originates from a BCA or PCA;

The modifications to CIP-004 are adequate.

The modification to CIP-005 R2, more precisely R2.7 is not required, since R1.2 is there to manage all the routable communication. Also R2.7 implies that the converter (IP to Serial) is outside of the ESP. [BCA] – IP – [F/W] – [IPtoSerial] - Serial

Likes 0	
Dislikes 0	

Response

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

Comment

Texas RE agrees that IRA definitions and requirements should be modified to address IRA in routable to nonroutable conversion scenarios. Texas RE noticed however, a gap between the glossary definition and the proposed requirements as written, specifically with regards to IRA to SCI.

The SDT has defined IRA as meeting one of the three following criteria:

- User-initiated electronic access by a person using a bi-directional routable protocol to a cyber system protected by an ESP.
- User-initiated electronic access by a person using a bi-directional routable protocol that is converted by the responsible entity to a non-routable protocol that allows access to a cyber system.
- User-initiated electronic access by a person using a bi-directional routable protocol to a management interface.

In CIP-005 R2 Part 2.1 the SDT requires that IRA only be permitted through an Intermediate System. One of the applicable systems is “SCI supporting an Applicable System in this Part.” In CIP-005 R1 Part 1.1 applicable systems are required to be protected by an ESP. SCI is not an applicable system. Since SCI are not an applicable system in CIP-005 R1 Part 1.1 they are not required to be protected by an ESP. An SCI not protected by an ESP will not match the “User-initiated electronic access by a person using a bi-directional routable protocol to a cyber system protected by an ESP” criteria. As such, these communications would not meet the definition of IRA and would therefore be out of scope for CIP-005 R2 Part 2.1.

Texas RE therefore recommends modifying the proposed glossary definition of IRA to include a “User-initiated electronic access by a person using a bi-directional routable protocol to SCI supporting a BCS.”

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

AEPC has signed on to ACES comments:

ACES feels the first sub bullet to the IRA definition is overly wordy and is confusing. ACES sugguests:

“To a BCS or a defined Electronic Access Point (EAP).”

The CIP standards are not concerened with IRA to any other systems besides Applicable Systems/BCS, so scoping the definition to just what NERC/CIP’s definition is, does not allow any scope creep.

Likes 0	

Dislikes 0	

Response

Junji Yamaguchi - Hydro-Quebec (HQ) - 5	
Answer	No
Document Name	

Comment
HQ supports NPCC RSC comments and provides the following additional comments: If the goal is to ensure that user interactive actions, is done remotely(i.e., not in the PSP), on a BCA and PCA, then those actions must go through an intermediate system, and the users must have training, ie CIP-004. The IRA definition should be simple and not technologically limited (routable vs nonroutable). The security risks associated to IRA are not dependent on the routable scenarios or routable to nonroutable (i.e., IP to serial) conversion scenarios. They are associated to the remote access. Furthermore, if the intentionof the IRA definition is to say “Communication that originates from a BCA or a PCA protected by any of the Responsible Entity’s ESPs”, Why is this part of the definition when CIP-005 R1.1 Requires that BCA or a PCA are to be protected by an ESP ? Also, since CIP-005 R2.4 and R2.5, include System-to-system process communication, I would remove “or System-to-system process communication.” to the definition of IRA as the concept is in the requirements. SDT should simplify the definition. Suggested improvements include: • IRA: User-initiated electronic access by a person to a BCA or a PCA . • Interactive Remote Access does not include: Out going communication that originates from a BCA or PCA; The modifications to CIP-004 are adequate. The modification to CIP-005 R2, more precisely R2.7 is not required, since R1.2 is there to manage all the routable communication. Also R2.7 implies that the converter (IP to Serial) is outside of the ESP. [BCA] – IP – [F/W] – [IPtoSerial] - Serial

Likes 0	
Dislikes 0	

Response

Teresa Krabe - Lower Colorado River Authority - 5	
Answer	No
Document Name	

Comment
By adding the new applicable system of medium impact with IRA in CIP-004 it causes confusion. LCRA believes the intent is to require training and background checks only for individuals with provisioned electronic access to medium impact BCS with IRA; however, it could be construed that any access to these devices requires R2 and R3 to be complied with.

Likes 0	
Dislikes 0	

Response

James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin

Answer	No
Document Name	

Comment

By adding the new applicable system of medium impact with IRA in CIP-004 it causes confusion. LCRA believes the intent is to require training and background checks only for individuals with provisioned electronic access to medium impact BCS with IRA; however, it could be construed that any access to these devices requires R2 and R3 to be complied with.

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 RSC

Answer	No
Document Name	

Comment

There seems to be an inconsistency between EACMS definition and the CIP-005 R2 requirements:

1) {C}EACMS definition includes a protocol converter for BCS where no ESP exists.

2) New R2 Applicable Systems requires an Intermediate System

3) New R2.7 requires an ESP between the Intermediate System and the BCS

Is the intent of the SDT to require the protocol converter to be an Intermediate System? In the case where no ESP exists, then R2.7 cannot be met.

Suggest change the Applicable Systems in R2.1 to exclude situations without ERC or change R2.7 requirements to exclude situations where protocol converter is used and there is no ESP

Likes 0	
Dislikes 0	

Response

Constantin Chitescu - Ontario Power Generation Inc. - 5

Answer	No
Document Name	
Comment	

OPG supports NPCC Regional Standards Committee's comments.

There seems to be an inconsistency between EACMS definition and the CIP-005 R2 requirements:
1) EACMS definition includes a protocol converter for BCS where no ESP exists.
2) New R2 Applicable Systems requires an Intermediate System
3) New R2.7 requires an ESP between the Intermediate System and the BCS
Is the intent of the SDT to require the protocol converter to be an Intermediate System? In the case where no ESP exists, then R2.7 cannot be met. Suggest change the Applicable Systems in R2.1 to exclude situations without ERC or change R2.7 requirements to exclude situations where protocol converter is used and there is no ESP

Likes 0	
Dislikes 0	
Response	

Alain Mukama - Hydro One Networks, Inc. - 1,3

Answer	No
Document Name	
Comment	

There is a conflict between the newly proposed EACMS which includes "those not protected by an Electronic Security Perimeter used by the responsible entity to convert routable protocol communications to non-routable communications to a BCS" and CIP-005-8 R2.7 that mandates ESP between Intermediate System and High/Medium Impact BCS. Please clarify how to identify ESP when protocol converter is used to connect High/Medium Impact Cyber System serially for IRA from Intermediate System. {C}{C}

Likes 0	
Dislikes 0	
Response	

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

Answer	No
Document Name	
Comment	

NST sees no reason to change the existing approved 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). If this is what the SDT intends, NST

recommends updating the CIP-005 Technical Rationale document to make this clear. NST is also concerned that as proposed, the revised definition could be interpreted to apply to any Cyber System, not just BES Cyber Systems and associated in-scope devices.

Likes 1	Central Hudson Gas & Electric Corp., 1, Ridolfino Michael
Dislikes 0	

Response

Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5 - NPCC

Answer	No
Document Name	

Comment

There seems to be an inconsistency between EACMS definition and the CIP-005 R2 requirements:
1) EACMS definition includes a protocol converter for BCS where no ESP exists.
2) New R2 Applicable Systems requires an Intermediate System
3) New R2.7 requires an ESP between the Intermediate System and the BCS
Is the intent of the SDT to require the protocol converter to be an Intermediate System? In the case where no ESP exists, then R2.7 cannot be met. Suggest change the Applicable Systems in R2.1 to exclude situations without ERC or change R2.7 requirements to exclude situations where protocol converter is used and there is no ESP

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	No
Document Name	

Comment

Tacoma Power is concerned that the exception language in CIP-004 R2 Part 2.3 invalidates the inclusion of the applicable system of “medium impact BCS with IRA”. Tacoma Power recommends deleting the “(except for medium impact BCS without ERC)” from the R2 Part 2.3 requirement language.

Additional editorial comment: “Medium” should not be capitalized in CIP-004 R5 Part 5.1 and R5.2, and R6 Part 6.3.

Likes 0	
Dislikes 0	

Response

Tracy MacNicoll - Utility Services, Inc. - 4	
Answer	No
Document Name	
Comment	
It is unclear if a protocol converter meets the proposed definitions for EACMS and EAP. The lack of clarity makes it difficult to apply the new IRA definition when protocol converters are used. The identification of a EAP on a protocol converter could establish an ESP around a BES Cyber System that does not use a routable protocol. The establishment of an ESP would also cause the non-routable BES Cyber System to meet the definition of ERC, which causes a significate increase in the number of applicable CIP requirements.	
Likes 0	
Dislikes 0	
Response	

Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
Answer	No
Document Name	
Comment	
This should specifically exclude direct access from a TCA. More detail is needed to understand the scope, for ex: are all serial addresses needed.	
Likes 0	
Dislikes 0	
Response	

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	No
Document Name	
Comment	
ACES feels the first sub bullet to the IRA definition is overly wordy and is confusing. ACES sugguests: “To a BCS or a defined Electronic Access Point (EAP).” The CIP standards are not concerened with IRA to any other systems besides Applicable Systems/BCS, so scoping the definition to just what NERC/CIP’s definition is, does not allow any scope creep.	
Likes 0	

Dislikes 0	
Response	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	Yes
Document Name	
Comment	
ISO-NE supports the ISO/RTO Council comments in this area.	
Likes 0	
Dislikes 0	
Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes
Document Name	
Comment	
The standard drafting team has done a good job in clearly defining the scope of IRA.	
Likes 0	
Dislikes 0	
Response	
Richard Vendetti - NextEra Energy - 5	
Answer	Yes
Document Name	
Comment	
NEE supports EEI comments	
Likes 0	
Dislikes 0	
Response	

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern supports the proposed changes for the IRA definition to address IRA in routable to nonroutable (i.e., IP to serial) conversion.	
Likes 0	
Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF agrees with the proposed changes to the IRA definition.	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
It appears there may be a discrepancy in the use of BES and BPS. The revised definition of BES Cyber Asset (BCA) includes the following: "Reliable Operatin of the Buld Electric System (BES) while the term Reliable Operation in the Glossary includes: "Operating the element of the Bulk-Power System ..."	
Likes 0	
Dislikes 0	
Response	

Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes
Document Name	
Comment	
ITC supports the response submitted by EEI	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI supports the modifications to the IRA definition, CIP-005 (Requirement R2) and CIP-004 (Applicable Systems) that address IRA in routable to nonrouteable (i.e., IP to serial) conversion scenarios.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon supports the comments submitted by the EEI.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	Yes

Document Name	
Comment	
Exelon is supporting EEI comments in response to this question.	
Likes 0	
Dislikes 0	
Response	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
AZPS supports the proposed changes	
Likes 0	
Dislikes 0	
Response	
Joanne Anderson - Public Utility District No. 2 of Grant County, Washington - 1,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
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	

Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
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	
Richard Jackson - U.S. Bureau of Reclamation - 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	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rebika Yitna - MEAG Power - 1,3 - SERC	
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	
Casey Jones - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Flanary - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
C. A. Campbell - LS Power Development, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Ellese Murphy On Behalf of: Marcelo Pesantez, Duke Energy - Florida Power Corporation, 3; - Ellese Murphy	
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)	
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	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
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	
David Jendras Sr - Ameren - Ameren Services - 3	
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	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

2. The SDT modified other (not related to IRA) 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.

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

Answer	No
Document Name	

Comment

ACES feels the way the definition of Electronic Access Point (EAP) is written in this draft is overly wordy. ACES suggests:

”An electronic policy enforcement point or a Cyber Asset interface on Electronic Access Control or Monitoring Systems that controls routable communication to and from BES Cyber Systems.”

ACES feels the way the definition of Intermediate System is written in this draft is overly wordy. ACES suggests:

“Electronic Access Control or Monitoring Systems (EACMS) used to restrict Interactive Remote Access to only authorized users”

ACES also noted that the definition of an Intermidiate System no longer states that it must not be located inside an ESP, combined with the removal of the language from R2.1: “such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.” Without those two statements IRA could be initiated through an ESP to an Intermediate System located in an ESP. ACES feels the removal of the language from the definition and requirement is not what was intended and needs to be added back to ensure the security of IRA. Furthermore

with the removal of the language, it allows a Cyber Asset IRA client to connect directly to Applicable Systems, if the Intermediate System is also an EACMS with an EAP. In this scenario the Cyber Asset client connects to the EACMS using a VPN client and Multi Factor Authentication. Once connected to the Intermediate System, the IRA Client could connect directly to applicable systems. There are other scenarios, but this is the most obvious.

EACMS is already plural. so adding “one or more” to the definition of Intermediate System is redundant.

ACES feels the second bullet point on the new Management Interface should be scoped down. There are a variety of vulnerabilities in “autonomous subsystems” in which one could gain access to a system’s console. Changing the scope of the definition to be ONLY those devices specifically designed and or used to allow access to a console would reduce scope creep. ACES suggests:

“Is an autonomous subsystem, specifically designed and or used to provide access to the console independently of the Cyber Asset’s CPU, firmware, and operating system;”

ACES feels the first word in bullet point one, section 4, of the TCA definition should be “to” rather than “on”

Likes 0	
Dislikes 0	

Response

Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez

Answer	No
Document Name	

Comment
Glossary, changes cause us to read many glossary terms to understand the term, then go to read standard and see how changes to glossary term has impact to the standard. EX: Management Interface. Definition should include physical interface or process, not both within the same definition. EX: term ‘unauthorized’ used, focus on the risk of unauthorized change. How is unauthorized defined?

Likes 0	
Dislikes 0	

Response

Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5 - NPCC	
Answer	No
Document Name	

Comment
PCA Definition – routable protocol missing. Please clarify ESP criteria / demarcation considerations if a Reponsible Entity takes a “policy” or ruleset based approach to an ESP; in relation to PCAs. Examples involving firewall / VLans / Switch controls… Can a Responsible Entity Choose what devices are PCAs based on the policy? The first bullet is missing the concept of being explicitly connected by a routable protocol Are protected by an Electronic Security Perimeter (ESP) but are not part of the highest impact BES Cyber System (BCS) protected by the same ESP; or.... Suggest …. Are connected to a network using a routable protocol and are protected by an Electronic Security Perimeter (ESP) but are not part of the highest impact BES Cyber System (BCS) protected by the same ESP; or.

Likes 0	
Dislikes 0	

Response

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

Comment
NST respectfully offers the following comments on proposed new and revised definitions: Intermediate System: NST recommends maintaining the "not within an ESP" language from the current definition rather than having that component be

implied by a requirement part.

Management Interface: NST recommends changing, "An administrative interface,..." to, "A dedicated physical or logical administrative interface,..."

Electronic Security Perimeter: 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.

Virtual Cyber Asset: NST suggests including some of the wording found in the definition of "Cyber Asset," such as, "including software and data." NST notes that the proposed definition, as written, would make it possible for a VCA to be hosted on a BES Cyber Asset that is itself a VCA. If this is what the SDT intends, NST recommends modifying the definition to make this clear.

Electronic Access Control and Monitoring System: NST sees no need for modifying the existing definition. We also note that not all protocol converters perform access control and/or monitoring, which makes it inappropriate to include them in a revised definition of EACMS.

External Routable Connectivity: As we did in 2022, NST believes the use of the word, "through (an ESP)" has the potential to cause confusion over the kind(s) of routable communications that may 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.

Shared Cyber Infrastructure: NST recommends adding "hardware" to "One or more programmable electronic devices, including the software,..." NST also recommends adding language to either or both of the "Cyber Asset" and "SCI" definitions that clarifies a device that hosts and/or provides storage resources for BES Cyber Systems and associated virtual devices at a single impact level (e.g., high) should be identified as a Cyber Asset, not as SCI.

Electronic Access Point: As we did in 2022, 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.

Transient Cyber Asset: As we did in 2022, NST notes the proposed definition includes a statement ("Virtual machines hosted on a physical Transient Cyber Asset (TCA) are treated as software on that physical TCA.") that directly conflicts with a statement included in the proposed definition of Cyber Asset ("VCAs are not considered software or data of Cyber Assets.").

Likes 1	Central Hudson Gas & Electric Corp., 1, Ridolfino Michael
Dislikes 0	

Response

Constantin Chitescu - Ontario Power Generation Inc. - 5

Answer	No
Document Name	

Comment

OPG supports NPCC Regional Standards Committee’s comments.

PCA Definition – routable protocol missing.
Please clarify ESP criteria / demarcation considerations if a Reponsible Entity takes a “policy” or ruleset based approach to an ESP; in relation to PCAs.
Examples involving firewall / VLans / Switch controls… Can a Responsible Entity Choose what devices are PCAs based on the policy?
The first bullet is missing the concept of being explicitly connected by a routable protocol

Are protected by an Electronic Security Perimeter (ESP) but are not part of the highest impact BES Cyber System (BCS) protected by the same ESP; or.... Suggest…. Are connected to a network using a routable protocol and are protected by an Electronic Security Perimeter (ESP) but are not part of the highest impact BES Cyber System (BCS) protected by the same ESP; or.	
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 RSC	
Answer	No
Document Name	
Comment	
PCA Definition – routable protocol missing. Please clarify ESP criteria / demarcation considerations if a Reponsible Entity takes a “policy” or ruleset based approach to an ESP; in relation to PCAs. Examples involving firewall / VLans / Switch controls… Can a Responsible Entity Choose what devices are PCAs based on the policy? The first bullet is missing the concept of being explicitly connected by a routable protocol *Are protected by an Electronic Security Perimeter (ESP) but are not part of the highest impact BES Cyber System (BCS) protected by the same ESP; or....* Suggest …. Are connected to a network using a routable protocol *and are protected by an Electronic Security Perimeter (ESP) but are not part of the highest impact BES Cyber System (BCS) protected by the same ESP; or.*	
Likes 0	
Dislikes 0	
Response	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	No
Document Name	
Comment	
LCRA believes the current CIP-002 SAR regarding serial-IP converters should be resolved prior to defining them as an EACMS.	
Likes 0	

Dislikes 0	

Response

Teresa Krabe - Lower Colorado River Authority - 5	
Answer	No
Document Name	

Comment
LCRA believes the current CIP-002 SAR regarding serial-IP converters should be resolved prior to defining them as an EACMS.

Likes 0	
Dislikes 0	

Response

Junji Yamaguchi - Hydro-Quebec (HQ) - 5	
Answer	No
Document Name	

Comment
HQ supports NPCC RSC comments and provides the following additional comments: The suggested definitions are mixing the concepts and they are making the overall understanding complicated. For example, the identification of PCA's is done through CIP-005. CIP-002 defines the BES that defines the BCS, and at the end the BCA. It's not written in CIP-002 that BCA need to be defined. No where in the standard is the PCA is directly defined. The first time you see it is in part 1.1 of the R1 table in CIP-005. For example, we have a BCA and we have a Cyber Asset they are communicating using a routable protocol, they are in the same network. Both Cyber Assets have an IP address. Theses Cyber Assets are connected via a routable protocol, thus they are in a ESP and the non qualified Cyber Asset is the PCA. In this case, the PCA is protected by an ESP. Going with a different example, we have a BCA and we have a Cyber Asset they are communicating using a non routable protocol, there's no network and both Cyber Asset don't have an IP address. Those Cyber Asset are not connected via a routable protocol; thus they are not in an ESP and the non qualified Cyber Asset is nothing. The second bullet of the PCA definition is a bit complicated, there's the mention of "isolates routable connectivity". We are no longer into PERMIT or DENY we are isolating, but we are still linked by the routable connectivity, ie routable protocol. The part that is getting more confusing is the definition of the ESP. The definition of ESP has two concepts, one is based on routable protocol which works with 1.1 of CIP-005, the other is based on a logical boundary defined by one or more Electronic Access Points (EAP). What is a logical boundary ? Is a logical boundary based on routable protocol? To add to the confusion the EAP is a policy enforcement interface and it's related to an EACMS. Is a policy a ruled based on routable protocol? Which requirement is asking to document this policy? Is it CIP-005R1.2? How to we evaluate the policy ? Regarding the EACMS definition, which is again build with two concepts. One of the concept is ", including those not protected by an Electronic

Security Perimeter used by the responsible entity to convert routable protocol communications to non routable communications to a BCS". Considering how the current proposed standard is written, a converter (routable protocol communications to non routable communications) is associated to IRA. And IRA is associated to the concept of Intermediate System, and Intermediate System is tag as an EACMS. This logic is establish with the current proposed standard. What is the added value to add this concept to the definition of EACMS ?

Overall it seems that the SDT tried to answer multiple objectives (concepts) with the same term/definition. The end result is that we have variations in the definition and the terms are cascading. The SDT should make the definition simpler and limit the number of cascades (ESP->EAP->EACMS) . Definitions are there to ease the understanding or support the requirements, they shouldn't add additional controls.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

AEPC has signed on to ACES comments:

ACES feels the way the definition of Electronic Access Point (EAP) is written in this draft is overly wordy. ACES suggests:

"An electronic policy enforcement point or a Cyber Asset interface on Electronic Access Control or Monitoring Systems that controls routable communication to and from BES Cyber Systems."

ACES feels the way the definition of Intermediate System is written in this draft is overly wordy. ACES suggests:

"Electronic Access Control or Monitoring Systems (EACMS) used to restrict Interactive Remote Access to only authorized users"

ACES also noted that the definition of an Intermidiate System no longer states that it must not be located inside an ESP, combined with the removal of the language from R2.1: "such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset." Without those two statements IRA could be initiated through an ESP to an Intermediate System located in an ESP. ACES feels the removal of the language from the definition and requirement is not what was intended and needs to be added back to ensure the security of IRA. Furthermore

with the removal of the language, it allows a Cyber Asset IRA client to connect directly to Applicable Systems, if the Intermediate System is also an EACMS with an EAP. In this scenario the Cyber Asset client connects to the EACMS using a VPN client and Multi Factor Authentication. Once connected to the Intermediate System, the IRA Client could connect directly to applicable systems. There are other scenarios, but this is the most obvious.

EACMS is already plural. so adding "one or more" to the definition of Intermediate System is redundant.

ACES feels the second bullet point on the new Management Interface should be scoped down. There are a variety of vulnerabilities in "autonomous subsystems" in which one could gain access to a system's console. Changing the scope of the definition to be ONLY those devices specifically designed and or used to allow access to a console would reduce scope creep. ACES suggests:

"Is an autonomous subsystem, specifically designed and or used to provide access to the console independently of the Cyber Asset's CPU, firmware,

and operating system;”	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Quebec (HQ) - 1	
Answer	No
Document Name	
Comment	

HQ supports NPCC RSC comments and provides the following additional comments:

The suggested definitions are mixing the concepts and they are making the overall understanding complicated. For example, the identification of PCA’s is done through CIP-005. CIP-002 defines the BES that defines the BCS, and at the end the BCA. It’s not written in CIP-002 that BCA need to be defined.

No where in the standard is the PCA is directly defined. The first time you see it is in part 1.1 of the R1 table in CIP-005.

For example, we have a BCA and we have a Cyber Asset they are communicating using a routable protocol, they are in the same network. Both Cyber Assets have an IP address. Theses Cyber Assets are connected via a routable protocol, thus they are in a ESP and the non qualified Cyber Asset is the PCA. In this case, the PCA is protected by an ESP.

Going with a different example, we have a BCA and we have a Cyber Asset they are communicating using a non routable protocol, there’s no network and both Cyber Asset don’t have an IP address. Those Cyber Asset are not connected via a routable protocol; thus they are not in an ESP and the non qualified Cyber Asset is nothing.

The second bullet of the PCA definition is a bit complicated, there’s the mention of “isolates routable connectivity”. We are no longer into PERMIT or DENY we are isolating, but we are still linked by the routable connectivity, ie routable protocol.

The part that is getting more confusing is the definition of the ESP. The definition of ESP has two concepts, one is based on routable protocol which works with 1.1 of CIP-005, the other is based on a logical boundary defined by one or more Electronic Access Points (EAP). What is a logical boundary ? Is a logical boundary based on routable protocol? To add to the confusion the EAP is a policy enforcement interface and it’s related to an EACMS. Is a policy a ruled based on routable protocol? Which requirement is asking to document this policy? Is it CIP-005R1.2? How to we evaluate the policy ?

Regarding the EACMS definition, which is again build with two concepts. One of the concept is “, including those not protected by an Electronic Security Perimeter used by the responsible entity to convert routable protocol communications to non routable communications to a BCS”. Considering how the current proposed standard is written, a converter (routable protocol communications to non routable communications) is associated to IRA. And IRA is associated to the concept of Intermediate System, and Intermediate System is tag as an EACMS. This logic is establish with the current proposed standard. What is the added value to add this concept to the definition of EACMS ?

Overall it seems that the SDT tried to answer multiple objectives (concepts) with the same term/definition. The end result is that we have variations in the definition and the terms are cascading. The SDT should make the definition simpler and limit the number of cascades (ESP->EAP->EACMS) . Definitions are there to ease the understanding or support the requirements, they shouldn’t add additional controls.

Likes 0	
Dislikes 0	

Response

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

NCPA recommends the following edits:

Cyber System should say "Two or more Cyber Assets...." as the word system implies multiples devices working together.

The proposed Intermediate System definition removed the requirement of not being inside the ESP, however in the proposed language for CIP-005-8 R2.7 it states "...communications from an Intermediate System to a high or medium impact BCS or associated PCAs must be through an ESP", which implies that it must reside outside of the ESP. NCPA suggests keeping the original language in the Intermediate System to include not being located within an ESP.

Likes 0	
Dislikes 0	

Response

Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	

SCI is superfluous considering that existing classification definitions can be applied. SCI does not clearly state what devices would be included and which are not included. Cyber Systems definition seems to rope in non-CIP assets. BES Cyber Systems definition is sufficient for grouping together Cyber Assets.

Likes 0	
Dislikes 0	

Response

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

MPC supports comments submitted by ACES.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

The definition of Intermediate System remains ambiguous as to whether it can cover such devices as Active Directory servers or firewalls. The terminology should be changed to define the Intermediate System to be the device that IRA is restricted to, not the device that does the restriction (which is not the Intermediate System, but is the firewall and/or domain policy server).

Also, the definition of BES Cyber Asset (BCA) uses the Glossary Term "Reliable Operations". This definition of BCA could increase the scope of the Cyber Assets being used for the operation of the BES since Reliable Operations defines Bulk-Power System's method of operation (which is a broader less precise term than BES).

Lastly the use of the term "Management Interface" needs clarification with use case and pertinent examples.

Likes 0	
Dislikes 0	

Response

Micah Runner - Black Hills Corporation - 1

Answer	No
Document Name	

Comment

Black Hills Corporation has the following comments regarding the CIP definition changes:

Cyber Assets: The last two sentences of the definition should be included as a note to the definition so that the term Cyber Asset is not in the definition of a Cyber Asset. Here is an example of what that could look like:

“Programmable electronic devices, excluding Shared Cyber Infrastructure, including the hardware, software, and data in those devices.

(Note – Application containers are considered software of Virtual Cyber Assets (VCAs) or Cyber Assets. VCAs are not considered software or data of Cyber Assets.)”

EAP: The definition should be revised to include the following commas to ensure clarity of the definition: “An electronic policy enforcement point, or a Cyber Asset interface on an Electronic Access Control or Monitoring Systems, that controls routable communication to and from one or more BES

Cyber Systems or their associated Protected Cyber Assets."

Likes 0	
Dislikes 0	

Response

Rachel Schuldt - Rachel Schuldt On Behalf of: Claudine Bates, Black Hills Corporation, 5, 6, 1, 3; - Rachel Schuldt

Answer	No
Document Name	

Comment

Black Hills Corporation has the following comments regarding the CIP definition changes:

Cyber Assets: The last two sentences of the definition should be included as a note to the definition so that the term Cyber Asset is not in the definition of a Cyber Asset. Here is an example of what that could look like:

"Programmable electronic devices, excluding Shared Cyber Infrastructure, including the hardware, software, and data in those devices.

(Note – Application containers are considered software of Virtual Cyber Assets (VCAs) or Cyber Assets. VCAs are not considered software or data of Cyber Assets.)"

EAP: The definition should be revised to include the following commas to ensure clarity of the definition: "An electronic policy enforcement point, or a Cyber Asset interface on an Electronic Access Control or Monitoring Systems, that controls routable communication to and from one or more BES Cyber Systems or their associated Protected Cyber Assets."

Likes 0	
Dislikes 0	

Response

Josh Combs - Black Hills Corporation - 3

Answer	No
Document Name	

Comment

Black Hills Corporation has the following comments regarding the CIP definition changes:

Cyber Assets: The last two sentences of the definition should be included as a note to the definition so that the term Cyber Asset is not in the definition of a Cyber Asset. Here is an example of what that could look like:

"Programmable electronic devices, excluding Shared Cyber Infrastructure, including the hardware, software, and data in those devices.

(Note – Application containers are considered software of Virtual Cyber Assets (VCAs) or Cyber Assets. VCAs are not considered software or data of

Cyber Assets.)”

EAP: The definition should be revised to include the following commas to ensure clarity of the definition: “An electronic policy enforcement point, or a Cyber Asset interface on an Electronic Access Control or Monitoring Systems, that controls routable communication to and from one or more BES Cyber Systems or their associated Protected Cyber Assets.”

Likes 0	
Dislikes 0	

Response

Sheila Suurmeier - Black Hills Corporation - 5

Answer	No
Document Name	

Comment

Black Hills Corporation has the following comments regarding the CIP definition changes:

Cyber Assets: The last two sentences of the definition should be included as a note to the definition so that the term Cyber Asset is not in the definition of a Cyber Asset. Here is an example of what that could look like:

“Programmable electronic devices, excluding Shared Cyber Infrastructure, including the hardware, software, and data in those devices.

(Note – Application containers are considered software of Virtual Cyber Assets (VCAs) or Cyber Assets. VCAs are not considered software or data of Cyber Assets.)”

EAP: The definition should be revised to include the following commas to ensure clarity of the definition: “An electronic policy enforcement point, or a Cyber Asset interface on an Electronic Access Control or Monitoring Systems, that controls routable communication to and from one or more BES Cyber Systems or their associated Protected Cyber Assets.”

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

The BCA definition changes include the defined term "Reliable Operation" which applies to the BPS by definition rather than just the BES. AECI supports the use of the previous "reliabile operation" undefined term as it would eliminate the risk of scope expansion to non-BES assets.

Likes 0	

Dislikes 0	

Response

Lindsey Mannion - ReliabilityFirst - 10	
Answer	No
Document Name	

Comment
The new Electronic Security Perimeter (ESP) definition still complicates the situation with respect to mixed-trust environments where a Responsible entity may choose to create ESPs and corresponding EAP's per individual Cyber System (zero trust paradigm). While this may be easier with standalone physical Cyber Assets – introducing SCI, VCA, virtual clusters, and virtual networking creates complexity that could allow unauthorized access if not carefully configured for applicable VM guests and virtual networks – especially if affinity controls are not strictly created and enforced. 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 directly internet-facing. 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 Applicable Systems by limiting ingress/egress points and access to these BCS. For the Shared Cyber Infrastructure definition, where is this to be identified and categorized? CIP-002 only requires the identification of BCS while the associated Technical Rationale warns of Assets with Multiple Classifications regarding high water marking. Is the entity to assume SCI must be included in CIP-002 even though it is not specifically included in the BCS definition?

Likes 0	
Dislikes 0	

Response

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

Comment
SMUD and BANC have the following comments regarding the CIP definition changes: **Cyber Assets:** The last two sentence of the definition should be included as a note to the definition so that the term Cyber Asset is not in the definition of a Cyber Asset. Here is an example of what that could look like: "Programmable electronic devices, excluding Shared Cyber Infrastructure, including the hardware, software, and data in those devices. (Note – Application containers are considered software of Virtual Cyber Assets (VCAs) or Cyber Assets. VCAs are not considered software or data of

Cyber Assets.)"

Cyber System: The definition should be changed to the following: "Two or more Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure working together to provide or perform a specific function."

EAP: The definition should be revised to include the following commas to ensure clarity of the definition: "An electronic policy enforcement point, or a Cyber Asset interface on an Electronic Access Control or Monitoring Systems, that controls routable communication to and from one or more BES Cyber Systems or their associated Protected Cyber Assets."

BCA: The proposed BES Cyber Asset (BCA) definition now capitalizes "Reliable Operation", which describes/ defines how to operate the **Bulk Electric System (BES)**. However, Reliable Operations specifically refers to the **Bulk-Power System** in its definition:

*"Operating the elements of the **[Bulk-Power System]** within equipment and electric system thermal, voltage, and stability limits so that instability, uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance, including a cybersecurity incident, or unanticipated failure of system elements."*

The Bulk-Power System is defined as:

"(A) facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof); and

(B) electric energy from generation facilities needed to maintain transmission system reliability. The term does not include facilities used in the local distribution of electric energy. (Note that the terms "Bulk-Power System" or "Bulk Power System" shall have the same meaning.)"

The Bulk-Power System term is broader in scope and less precise than the Bulk Electric System term. The Bulk Electric System is defined as:

"...all Transmission Elements operated at 100 kV or higher and Real Power and Reactive Power resources connected at 100 kV or higher. This does not include facilities used in the local distribution of electric energy..."

With the capitalization of "Reliable Operations", it could be interpreted that the proposed definition of BCA could increase the scope of the Cyber Assets used for operating the BES since Reliable Operations describes/defines how to operate the Bulk-Power System, which is a broader less precise term than BES.

SMUD and BANC would like to understand why the defined term, Reliable Operation, was used and if the intent of the revision is to broaden the scope of Cyber Assets.

Likes 0	
Dislikes 0	

Response

Tracy MacNicoll - Utility Services, Inc. - 4

Answer	Yes
Document Name	

Comment

USV support the comments made by NPCC RSC.

The proposed ESP definition uses the terms "border" and "boundary". It is unclear what difference is between these two terms and how this difference impacts the proposed definition.

Likes 0	
Dislikes 0	

Response

David Jendras Sr - Ameren - Ameren Services - 3

Answer	Yes
Document Name	

Comment

In the CIP Senior Manager definition, the words "cyber security" should be deleted. As proposed it implies that the CSM is no longer responsible for physical security Standards CIP-006 & CIP-014.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

AZPS supports the changes to definitions within draft 5.

Likes 0	
Dislikes 0	

Response

Kinte Whitehead - Exelon - 3

Answer	Yes
Document Name	

Comment

Exelon is supporting EEI comments in response to this question.

Likes 0	
Dislikes 0	

Response	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon supports the comments submitted by the EEI.	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI supports the changes made to the definitions as posted in this Draft 5 posting.	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes
Document Name	
Comment	
ITC supports the response submitted by EEI	
Likes 0	
Dislikes 0	
Response	

Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF agrees with the definition changes.	
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 supports the changes to the definitions in Draft 5.	
Likes 0	
Dislikes 0	
Response	
Richard Vendetti - NextEra Energy - 5	
Answer	Yes
Document Name	
Comment	
NEE supports EEI comments	
Likes 0	
Dislikes 0	
Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes

Document Name	
Comment	
The work the standard drafting team has done to move requirements out of the definitions and in to the standards improves the reliability standards overall.	
Likes 0	
Dislikes 0	
Response	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	Yes
Document Name	
Comment	
ISO-NE supports the ISO/RTO Council comments in this area.	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
BPA has two recommendations: Cyber Asset definition: recommend improving the grammar by rewriting so there is not an “excluding” phrase separated from an “including” phrase by nothing but a comma. As written it will cause confusion. ERC definition: Given that the EAP definition would be modified to refer to EACMS as the ‘location’ of the EAP, the definition of ERC might read better if it stated “through an EAP” or “through its EACMS” rather than "through its ESP.”	
Likes 0	
Dislikes 0	

Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
FirstEnergy does not opposed the other definitions.	
Likes 0	
Dislikes 0	
Response	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
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	
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	
Alain Mukama - Hydro One Networks, Inc. - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
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	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Shannon Mickens On Behalf of: Joshua Phillips, Southwest Power Pool, Inc. (RTO), 2; - Shannon Mickens, Group Name SPP RTO	

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)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Ellese Murphy On Behalf of: Marcelo Pesantez, Duke Energy - Florida Power Corporation, 3; - Ellese Murphy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
C. A. Campbell - LS Power Development, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Mark Flanary - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Casey Jones - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ben Hammer - Western Area Power Administration - 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	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Rebika Yitna - MEAG Power - 1,3 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Robert Follini - Avista - Avista Corporation - 3	
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	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Anne Kronshage - Public Utility District No. 1 of Chelan County - 6, Group Name Public Utility District No. 1 of Chelan County - Voting Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Keele - Entergy - 1,3,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Joanne Anderson - Public Utility District No. 2 of Grant County, Washington - 1,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

3. The SDT revised CIP-005 R1 based on industry comments. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC

Answer	No
Document Name	

Comment

SMUD and BANC disagree with the new definitions for IRA and Cyber System as the proposed definition changes may expand the scope of CIP-005, Requirement R1 to non-BES Cyber Systems.

Likes 1	Central Hudson Gas & Electric Corp., 1, Ridolfino Michael
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

As with Draft 4, 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.

BPA does support the replacement of “protect” with “permit” in R 1 Part 1.3; this adds clarity to the intent of the requirement.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

The STD proposed a change to specify EAP as applicable systems. BC Hydro recommends providing additional clarity on evidence expectations where network-like evidence is expected at the BCS level.	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	No
Document Name	
Comment	
MPC supports comments submitted by the MRO NERC Standards Review Forum (NSRF) and ACES.	
Likes 0	
Dislikes 0	
Response	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	No
Document Name	
Comment	
NCPA does not agree based on comments made in question 1 related to the proposed IRA definition change.	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Quebec (HQ) - 1	
Answer	No
Document Name	
Comment	

HQ supports NPCC RSC comments and provides the following additional comments:

R1.2 We support the following modification “excluding time sensitive communications of Protection Systems” (replacing “communications using protocol IEC TR 61850-90-5 R-GOOSE”) assuming that the intentof the SDT was to link with the definition of Protection System (Glossary of terms)

In the column Measures, the SDT mentions VLAN and VXLAN, they are not routable protocoles. Please refer to the OSI model.

R1.3 The objective of Requirement R1.2 is to protect the BCA and the PCA through the management of the routable protocol communications (Permit/Deny). The EACMS and SCI assist in the delivery of the BCA/PCA functionalities. The EACMS and SCI Management interface are just as important, we suggest wording the requirement R1.2 and R1.3 the same way. R1.2 could be worded as: “Protect Applicable System by implementing policy enforcement to permit only needed network accessibility documenting the reason, and deny all other communications, through the ESP.” Doing so would removed the need of R1.3 or would be more “inline”.

Please note the usage of the word policy, this usage is to ensure a logical link between the requirements and the definitions.

The definition of ESP brings the concept of routable protocol and the concept of logical boundary.

R1.4 This requirement should consider including the introduction of Management interface concept. Management interface is another mean to interact with the Cyber Asset and should be address.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

AEPC has signed on to ACES comments:

ACES feels R1.3 should be reworded:

“EACMS, and their supporting SCI, that control access to and from an ESP for an Applicable System in Part 1.1”

ACES feels in R1.4: “if any” is not necessary.

Likes 0	
Dislikes 0	

Response

Junji Yamaguchi - Hydro-Quebec (HQ) - 5

Answer	No

Document Name	

Comment

HQ supports NPCC RSC comments and provides the following additional comments:

R1.2 We support the following modification “excluding time sensitive communications of Protection Systems” (replacing “communications using protocol IEC TR 61850-90-5 R-GOOSE”) assuming that the intentof the SDT was to link with the definition of Protection System (Glossary of terms)

In the column Measures, the SDT mentions VLAN and VXLAN, they are not routable protocoles. Please refer to the OSI model.

R1.3 The objective of Requirement R1.2 is to protect the BCA and the PCA through the management of the routable protocol communications (Permit/Deny). The EACMS and SCI assist in the delivery of the BCA/PCA functionalities. The EACMS and SCI Management interface are just as important, we suggest wording the requirement R1.2 and R1.3 the same way. R1.2 could be worded as: “Protect Applicable System by implementing policy enforcement to permit only needed network accessibility documenting the reason, and deny all other communications, through the ESP.” Doing so would removed the need of R1.3 or would be more “inline”.

Please note the usage of the word policy, this usage is to ensure a logical link between the requirements and the definitions.

The definition of ESP brings the concept of routable protocol and the concept of logical boundary.

R1.4 This requirement should consider including the introduction of Management interface concept. Management interface is another mean to interact with the Cyber Asset and should be address.

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 RSC

Answer	No
Document Name	

Comment

1.3 broaden from *network accessibility* to be more objective = “*protect configuration”* in order to allow other methods to protect the configuration

Protect ESP and SCI configurations by implementing methods to permit only needed network accessibility to Management Interfaces of Applicable Systems, per system capability.

Suggest

Implement methods to protect ESP and SCI configurations at Management Interfaces of Applicable Systems, per system capability, per system capability.

Likes 0	
Dislikes 0	

Response

Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee's comments. 1.3 broaden from network accessibility to be more objective = "protect configuration" in order to allow other methods to protect the configuration Protect ESP and SCI configurations by implementing methods to permit only needed network accessibility to Management Interfaces of Applicable Systems, per system capability. Suggest Implement methods to protect ESP and SCI configurations at Management Interfaces of Applicable Systems, per system capability, per system capability.	
Likes 0	
Dislikes 0	
Response	
Alain Mukama - Hydro One Networks, Inc. - 1,3	
Answer	No
Document Name	
Comment	
Part 1.5 -> Suggestion to consider IPS/IDS on the edge of a facility instead of between discrete ESPs (E.g. if a facility has a number of ESP and non-ESP network segments, but has IPS/IDS controls at the routing edge of the facility) Part 2.6 -> Use wording from CIP-007 that explicitly excludes storage resources (consistency in language) Part 2.7 -> It could be clearer if this requirement just explicitly states that the intermediate system is required to be outside of the ESP that it is providing access to. The requirement to route through an EAP is then covered by R1.2 and not needed to re-stated in this requirement.	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	

Comment
As we did in 2022, NST objects to the use of the phrase "through the ESP," as in, "Permit only needed routable protocol communications, documenting the reason, and deny all other routable protocol communications, through the ESP;..." (R1.2). Data packets don't go "through" an ESP, they go into or out of an ESP through an access point. NST also notes that while R1.3 requires a Responsible Entity to control network access to the Management Interfaces of SCI, there is no comparable requirement for devices (e.g., Hypervisors) that are not SCI according to the SDT's proposed definition but that still host virtual machines that are in scope for R1. This inconsistency should be addressed.

Likes 1	Central Hudson Gas & Electric Corp., 1, Ridolfino Michael
Dislikes 0	

Response

Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5 - NPCC	
Answer	No
Document Name	

Comment
1.3 broaden from network accessibility to be more objective = “protect configuration” in order to allow other methods to protect the configuration Protect ESP and SCI configurations by implementing methods to permit only needed network accessibility to Management Interfaces of Applicable Systems, per system capability. Suggest Implement methods to protect ESP and SCI configurations at Management Interfaces of Applicable Systems, per system capability, per system capability.

Likes 0	
Dislikes 0	

Response

Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
Answer	No
Document Name	

Comment
No, due to lack of understanding of scope of impact to our systems. Better understanding of ‘applicable systems’ is needed. Provide examples. Implementation plan guidance needed to better understand how to be in compliance.

Likes 0	

Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	No
Document Name	
Comment	
ACES feels R1.3 should be reworded: “EACMS, and their supporting SCI, that control access to and from an ESP for an Applicable System in Part 1.1” ACES feels in R1.4: “if any” is not necessary.	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Shannon Mickens On Behalf of: Joshua Phillips, Southwest Power Pool, Inc. (RTO), 2; - Shannon Mickens, Group Name SPP RTO	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
FirstEnergy does not opposed these changes.	
Likes 0	

Dislikes 0	
Response	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	Yes
Document Name	
Comment	
ISO-NE supports the ISO/RTO Council comments in this area.	
Likes 0	
Dislikes 0	
Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes
Document Name	
Comment	
The standard drafting team has done an excellent job in addressing comments in CIP-005 and compliance to the new wording is backwards compatible. Manitoba Hydro notes that the definition of Intermediate System was updated to remove the phrase “The Intermediate System must not be located inside the Electronic Security Perimeter” and requirement R2.7 was added requiring “Routable protocol communications from an Intermediate System to a high or medium impact BCS or associated PCAs must be through an ESP.”. The new requirement does not make it clear that an EACMS that contains an EAP cannot also be the intermediate system. The following wording is suggested to clarify that a separate system such as a "jump host" must be used as an Intermediate System: “Routable protocol communications from an Intermediate System to a high or medium impact BCS or associated PCAs must be through an EAP in a separate Cyber Asset or Virtual Cyber Asset.”	
Likes 0	
Dislikes 0	
Response	
Mark Flanary - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	

While we can agree with the changes as they stand, should circumstances arise where additional changes to CIP-005 are necessary, we offer the following recommendations:

Part 1.3 - We recommend against the changing of "to and from" to simply "to". Controlling outbound communication is vital protection to prevent connectivity of a compromised system out to a comand-and-control server.

Part 2.3 - Consider the scenario of low impact SCI as the initiating system. The requirement phrase "Cyber Asset or Virtual Cyber Asset" excludes SCI from the set of possible initiating systems. We recommend updating the language to encapsulate all forms by using the defined term "Cyber Systems" or adding SCI.

Likes 0	
Dislikes 0	

Response

Richard Vendetti - NextEra Energy - 5

Answer	Yes
Document Name	

Comment

NEE supports EEI comments

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

Southern agrees and supports the changes to the Applicable Systems, Requirements, and Measures in CIP-005 R1.

Likes 0	
Dislikes 0	

Response

Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF

Answer	Yes
Document Name	
Comment	
The NAGF agrees with the proposed changes to CIP-005 Requirement R1.	
Likes 0	
Dislikes 0	
Response	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	Yes
Document Name	
Comment	
The standard drafting team has done an excellent job in addressing comments in CIP-005. The NSRF notes that the definition of Intermediate System was updated to remove the phrase “The Intermediate System must not be located inside the Electronic Security Perimeter” and requirement R2.7 was added requiring “Routable protocol communications from an Intermediate System to a high or medium impact BCS or associated PCAs must be through an ESP.”. The new requirement does not make it clear that an EACMS that contains an EAP cannot also be the intermediate system. The following wording is suggested: “Routable protocol communications from an Intermediate System to a high or medium impact BCS or associated PCAs must be through an EAP in a separate Cyber Asset or Virtual Cyber Asset.”	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes
Document Name	
Comment	
ITC supports the response submitted by EEI	
Likes 0	
Dislikes 0	

Response
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable
Answer	Yes
Document Name	
Comment
EEI supports the changes made to CIP-005, Requirement R1.
Likes 0	
Dislikes 0	
Response
Daniel Gacek - Exelon - 1
Answer	Yes
Document Name	
Comment
Exelon supports the comments submitted by the EEI.
Likes 0	
Dislikes 0	
Response
Kinte Whitehead - Exelon - 3
Answer	Yes
Document Name	
Comment
Exelon is supporting EEI comments in response to this question.
Likes 0	
Dislikes 0	
Response

Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
AZPS supports the proposed changes	
Likes 0	
Dislikes 0	
Response	
Tracy MacNicoll - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
USV supports the comments made by NPCC RSC The R1.5 requirement language limits the scope of this requirement to “routable communication entering or leaving an ESP”. Suggest moving this scoping language to the applicability column by adding “with ERC” to both high and medium impact BCS listed.	
Likes 0	
Dislikes 0	
Response	
Joanne Anderson - Public Utility District No. 2 of Grant County, Washington - 1,4,5,6 - WECC	
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	
James Keele - Entergy - 1,3,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anne Kronshage - Public Utility District No. 1 of Chelan County - 6, Group Name Public Utility District No. 1 of Chelan County - Voting Group	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsey Mannion - ReliabilityFirst - 10	
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	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rebika Yitna - MEAG Power - 1,3 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
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	
Ben Hammer - Western Area Power Administration - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sheila Suurmeier - Black Hills Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Rachel Schuldt - Rachel Schuldt On Behalf of: Claudine Bates, Black Hills Corporation, 5, 6, 1, 3; - Rachel Schuldt	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Josh Combs - Black Hills Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Micah Runner - Black Hills Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Casey Jones - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
C. A. Campbell - LS Power Development, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Ellese Murphy On Behalf of: Marcelo Pesantez, Duke Energy - Florida Power Corporation, 3; - Ellese Murphy	
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)	
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	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
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	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
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	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 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	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

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.

Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2

Answer	No
Document Name	

Comment

ERCOT joins the comments submitted by the ISO/RTO Council (IRC) Standards Review Committee (SRC) and adopts them as its own.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

NST believes R1.3 needs to be re-worded to make it clear it applies to SCI hosting both high and medium impact BES Cyber Systems if a Responsible Entity doesn't want "high water marking" to compel treating the medium impact BCS as PCAs associated with the high impact BCS.

Likes 0	
Dislikes 0	

Response

Alain Mukama - Hydro One Networks, Inc. - 1,3

Answer	No
Document Name	

Comment

Part R1.3 -> The requirement outlines controls/evidence recommended for non-BCS VCAs sharing SCI, but does not provide options potential options of classifying/securing non-BCS VCAs where physical/logical isolation cannot be achieved or is finacially restrictive.

Likes 0	

Dislikes 0	

Response

Junji Yamaguchi - Hydro-Quebec (HQ) - 5	
Answer	No
Document Name	

Comment

HQ supports NPCC RSC comments and provides the following additional comments:

R1.1 The requirement “Disable or prevent unneeded routable protocol network accessibility on each Applicable System, per system capability. “ This requirement is ambiguous and the column measure is still referencing logical ports. Furthermore, how will this requirement will be evaluated ? The previous version of this requirement was less ambiguous.

R1.3 the definition of SCI includes the storage resource but this requirement exclude the storage resources. How is the shared storage resources managed ? What about the shared network resource ?

For some requirements the TFE was removed for “per system capability.”We do understand that TFE process isn’t optimal but it permitted more nuance than per system capability. For example, the TFE basis for approval of a technical feasibility exception are, at least the two following points;

{C}(i) is not technically possible or is precluded by technical limitations; or

{C}(ii) is operationally infeasible or could adversely affect reliability of the Bulk Electric System to an extent that outweighs the reliability benefits of Strict Compliance with the Applicable Requirement;

Per system capability is only equal to the first point but doesn’t equal to the second or to the other three. The SDT should define per system capability.

Likes 0	
Dislikes 0	

Response

Nicolas Turcotte - Hydro-Quebec (HQ) - 1	
Answer	No
Document Name	

Comment

HQ supports NPCC RSC comments and provides the following additional comments:

R1.1 The requirement “Disable or prevent unneeded routable protocol network accessibility on each Applicable System, per system capability. “ This requirement is ambiguous and the column measure is still referencing logical ports. Furthermore, how will this requirement will be evaluated ? The previous version of this requirement was less ambiguous.

R1.3 the definition of SCI includes the storage resource but this requirement exclude the storage resources. How is the shared storage resources

managed ? What about the shared network resource ?

For some requirements the TFE was removed for “per system capability.”We do understand that TFE process isn’t optimal but it permitted more nuance than per system capability. For example, the TFE basis for approval of a technical feasibility exception are, at least the two following points;

(i) is not technically possible or is precluded by technical limitations; or

(ii) is operationally infeasible or could adversely affect reliability of the Bulk Electric System to an extent that outweighs the reliability benefits of Strict Compliance with the Applicable Requirement;

Per system capability is only equal to the first point but doesn’t equal to the second or to the other three. The SDT should define per system capability.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

SCI is superfluous considering that existing classification definitions can be applied. SCI does not clearly state what devices would be included and which are not included. Cyber Systems definition seems to rope in non-CIP assets. BES Cyber Systems definition is sufficient for grouping together Cyber Assets.

Likes 0	
Dislikes 0	

Response

Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)

Answer	No
Document Name	

Comment

The ISO/RTO Council (IRC) Standards Review Committee (SRC) requests clarification of the term “network accessibility” used within requirement R1 Part1.1, which reads as follows: “Disable or prevent unneeded routable protocol **network accessibility** on each Applicable System, per system capability.” One of the measures also references this term: “Identity or process based access policy or workload configuration demonstrating needed **network accessibility**.” Specifically, the SRC requests that the drafting team clarify whether entities will need to define the term “network accessibility” in their documented processes or whether a standardized definition will apply. If there is a specific definition that entities are intended to use, the SRC requests that the SDT provide the definition that will apply.

Likes 0	

Dislikes 0	
Response	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	No
Document Name	
Comment	
SMUD and BANC appreciate the Standard Drafting Team's work to modify CIP-007. However, we note that the word "system" is used inconsistently, especially with regards to "per system capability", and this makes the High and Medium impact requirements less stringent than the requirements for Low impact. We recommend changing the language to "per Cyber Asset capability."	
Likes 0	
Dislikes 0	
Response	
James Keele - Entergy - 1,3,6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Ameren would like clarity on the change from where technically feasible to per system capability. Does this mean that the TFE process is going away or are they changing it to a different name?	
Likes 0	

Dislikes 0	
Response	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
AZPS supports the proposed changes	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon is supporting EEI comments in response to this question.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon supports the comments submitted by the EEI.	
Likes 0	
Dislikes 0	
Response	

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI supports the changes made to CIP-007.	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes
Document Name	
Comment	
ITC supports the response submitted by EEI	
Likes 0	
Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF agrees with the proposed changes to CIP-007.	
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 supports the changes made to CIP-007.	
Likes 0	
Dislikes 0	
Response	
Richard Vendetti - NextEra Energy - 5	
Answer	Yes
Document Name	
Comment	
NEE supports EEI comments	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
BC Hydro agrees with the changes however seeks further clarification as follows. BC Hydro seeks clarification with use cases or examples on proposed changes to CIP-007 R1.1, whether, “per system capability” means entities are compelled to install software (if possible) that can be used to block network accessibility? Specifically, if a Cyber Asset uses a method (e.g.: host firewall) that can block the unneeded network accessibility, but that method has been determined to be detrimental to reliable operations, does this mean entities are compelled to continue to use that method although it affects the operation? BC Hydro also seeks clarification on Routable protocol network accessibility particularly, as Technical Feasibility Exception (TFE) is replaced by "per system capability", are the entities expected to make decisions on whether to document or not to document exceptions on per system capability? Please provide some use case examples and further guidance.	
Likes 0	
Dislikes 0	

Response	
Micah Runner - Black Hills Corporation - 1	
Answer	Yes
Document Name	
Comment	
Black Hills Corporation agrees with the comments from Public Utility District No. 1 of Chelan County: in our review of the proposed changes, we identified an opportunity to enhance the clarity of the requirement section of R1.3. Our proposed wording for R1.3 is as follows: Mitigate the risk of CPU or memory vulnerabilities by preventing the sharing of CPU resources and memory resources, excluding storage resources, between VCAs that are within an ESP, and VCAs that are not within an ESP.	
Likes 0	
Dislikes 0	
Response	
Rachel Schuldt - Rachel Schuldt On Behalf of: Claudine Bates, Black Hills Corporation, 5, 6, 1, 3; - Rachel Schuldt	
Answer	Yes
Document Name	
Comment	
Black Hills Corporation agrees with the comments from Public Utility District No. 1 of Chelan County: in our review of the proposed changes, we identified an opportunity to enhance the clarity of the requirement section of R1.3. Our proposed wording for R1.3 is as follows: Mitigate the risk of CPU or memory vulnerabilities by preventing the sharing of CPU resources and memory resources, excluding storage resources, between VCAs that are within an ESP, and VCAs that are not within an ESP.	
Likes 0	
Dislikes 0	
Response	
Josh Combs - Black Hills Corporation - 3	
Answer	Yes
Document Name	
Comment	
Black Hills Corporation agrees with the comments from Public Utility District No. 1 of Chelan County: in our review of the proposed changes, we identified an opportunity to enhance the clarity of the requirement section of R1.3. Our proposed wording for R1.3 is as follows: Mitigate the risk of CPU or memory vulnerabilities by preventing the sharing of CPU resources and memory resources, excluding storage resources, between VCAs that are	

within an ESP, and VCAs that are not within an ESP.

Likes 0	
Dislikes 0	

Response

Sheila Suurmeier - Black Hills Corporation - 5

Answer	Yes
Document Name	

Comment

Black Hills Corporation agrees with the comments from Public Utility District No. 1 of Chelan County: in our review of the proposed changes, we identified an opportunity to enhance the clarity of the requirement section of R1.3. Our proposed wording for R1.3 is as follows: Mitigate the risk of CPU or memory vulnerabilities by preventing the sharing of CPU resources and memory resources, excluding storage resources, between VCAs that are within an ESP, and VCAs that are not within an ESP.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

BPA notes that implementation of and documenting compliance with Part 1.1 may pose technical challenges depending on an entity’s architecture or processes.

Likes 0	
Dislikes 0	

Response

Lindsey Mannion - ReliabilityFirst - 10

Answer	Yes
Document Name	

Comment

Consider rewording R1.3 for clarity.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

FirstEnergy does not opposed these changes.

Likes 0	
Dislikes 0	

Response

Anne Kronshage - Public Utility District No. 1 of Chelan County - 6, Group Name Public Utility District No. 1 of Chelan County - Voting Group

Answer	Yes
Document Name	

Comment

CHPD agrees with the proposed changed to CIP-007 R1.3.

We would also like to express our support for the decision to remove the Electronic Access Control and Monitoring Systems (EACMS) and Physical Access Control Systems (PACS) from the list of applicable systems in CIP-007 R1.3. This change is a positive step forward, as it helps support backward compatibility with the standard.

However, in our review of the proposed changes, we identified an opportunity to enhance the clarity of the requirement section of R1.3. Our proposed wording for R1.3 is as follows: Mitigate the risk of CPU or memory vulnerabilities by preventing the sharing of CPU resources and memory resources, excluding storage resources, between VCAs that are within an ESP, and VCAs that are not within an ESP.

We believe this reworded requirement maintains the original intent of the section while making it more straightforward and easier to understand. By replacing "VCAs that are, or are associated with, a medium or high impact BCS" with "VCAs that are within an ESP," we simplify the language while preserving the core security objectives of the requirement.

Likes 0	
Dislikes 0	

Response

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
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	
Tracy MacNicoll - Utility Services, Inc. - 4	
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	
Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5 - NPCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation 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	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 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	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
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 Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
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	
Shannon Mickens - Shannon Mickens On Behalf of: Joshua Phillips, Southwest Power Pool, Inc. (RTO), 2; - Shannon Mickens, Group Name SPP RTO	
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	
Ellese Murphy - Ellese Murphy On Behalf of: Marcelo Pesantez, Duke Energy - Florida Power Corporation, 3; - Ellese Murphy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
C. A. Campbell - LS Power Development, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Mark Flanary - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Casey Jones - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ben Hammer - Western Area Power Administration - 1	
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	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rebika Yitna - MEAG Power - 1,3 - SERC	
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	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Robert Follini - Avista - Avista Corporation - 3	

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	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joanne Anderson - Public Utility District No. 2 of Grant County, Washington - 1,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

5. 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.

James Keele - Entergy - 1,3,6	
Answer	No
Document Name	

Comment

Entergy disagrees with CIP-010 R1.1 as written for two reasons.

First, the requirements as written is difficult to follow as a single sentence with many oxford commas and could benefit from a rewrite to reduce confusion. Entergy proposes the requirement be rewritten similar to the following:
“Authorize changes that affect Applicable Systems and alter the behavior of one or more cyber security controls (as defined by the Responsible Entity) that serve one or more requirement parts in CIP-005 or CIP-007. This excludes procedural and physical controls.”
Secondly, Entergy is concerned regarding the removal of the previous CIP-010 R1.4 language that allowed an assessment of potentially impacted security controls, the ambiguity of the “as defined by the Responsible Entity” language, and how this could expand the scope of testing and change authorization.
As written the standard implies that any potential change to a control “defined by the Responsible Entity” would require authorization and subsequent testing, which would result in Responsible Entity security controls testing expanding from a list of potentially impacted security controls to a verification of all security controls regardless on the actual nature of the change to prove a control wasn’t impacted. As written the “defined by the Responsible Entity” could be interpreted as being related to the defining of the controls, not the defining by the Responsible Entity of a change to a control.
Entergy believes the intent of this requirement is still to perform authorizations and testing of potential and identified impacts to CIP-005 and CIP-007 controls prior to deployment. This is supported by the proposed CIP-010 R1.4 language to “verify the behavior(s) of the altered cyber security controls” which implies a verification of a pre-determined set of impacts, not a verification of ***all*** controls.
If Entergy is interpreting this correctly, then Entergy proposes that CIP-010 R1.1 be rewritten to something similar to the following, which replaces “defined” with “determined”:
“Authorize changes that the Reponsible Entity determines will affect Applicable Systems and alter the behavior of one or more cyber security controls that serve one or more requirement parts in CIP-005 or CIP-007. This excludes procedural and physical controls.”

Likes 0	
Dislikes 0	

Response

Anne Kronshage - Public Utility District No. 1 of Chelan County - 6, Group Name Public Utility District No. 1 of Chelan County - Voting Group	
Answer	No
Document Name	

Comment

The problem with the current standard verbiage is that there is no requirement for a baseline, but there is no way to accomplish what the standard requires without creating baselines to monitor. Knowing you are going to be making a change that affects the baseline is a much more straightforward measure than trying to predict which/if any changes will affect CIP-005 or CIP-007 security controls tests and to what extent these should be re-tested after a change that may or may not affect the test results. For example in R1.2 the measure to include evidence such as "…a list of differences between the production and test environments with descriptions of how any differences were accounted for" cannot be accomplished without a baseline to

compare against.

R2.1's requirement is unclear whether we should be monitoring for different test results, or if we should be monitoring for changes to a baseline (again, there is no mention of baselines so I'm not convinced this is a valid interpretation). If it is the case that we need to test all CIP-005 and CIP-007 controls (except physical and procedural), these are the bulk of bookending tasks for any new system. Performing this for hundreds of devices monthly is not feasible. We are a smaller entity, and we can't imagine how a larger entity could perform hundreds or thousands of bookends every month.

In Attachment 2 Section 2.1 there are two instances of the same typo for "..Responsible Entity **that that** document.."

Likes 0	
Dislikes 0	

Response

Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC

Answer	No
Document Name	

Comment

SMUD and BANC do not agree with the changes to CIP-010 for the following reasons:

- CIP-010 should be reverted to its current state with the simple addition to the “Applicable Systems column” with the newly added SCI, like how it is being done for the CIP-007 revisions, to accommodate for the addition of SCI.

- The Technical Feasibility Exception was removed and not replaced with “per system capability?” If an entity has an approved TFE for CIP-010-4 R1.5, the changes proposed in CIP-010-5 R1.2 would now be applicable to that entity with no relief. Therefore, with CIP-010-5 R1.2 the entity would now be noncompliant.

- The Technical Rational for Requirement R2 is “to keep the scope of R2 to those things for which there are an ***automated solution*** that can monitor these areas and alert entities to changes.” Additionally, “The SDT also added “***per system capability***” in recognition that not all changes in scope can be monitored on every potential in-scope Cyber System. This addition makes the requirement conditional if a system is incapable of monitoring a particular unauthorized change category.” However, there is no mention that CIP-010-5 R2 Part 2.1 is only applicable for automated solutions and no automated solutions are excluded. Is that assumed/implied/allowed with the “***per system capability***” statement? Furthermore, in the Measures it states, “Examples of evidence may include, but are not limited to, reports generated from ***automated tools or manual reviews*** along with records of investigation for any unauthorized changes that were detected.” This statement causes further confusion for which the Standard Drafting Team (SDT) should address.

- The SDT should clarify if the term “per system capability” applies to Parts 2.1.1 through 2.1.7. The language that precedes the Parts reads, “...that include ***at least one cyber security control for each of the following***:” which refutes the “per system capability” statement. Is there a way for the SDT to incorporate the “per system capability” for each sub-requirement?

Likes 0	
Dislikes 0	

Response

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.

Likes 0	
Dislikes 0	
Response	

John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	No
Document Name	
Comment	

ISO-NE supports the ISO/RTO Council comments in this area, which are replicated here:

ISO/RTO Council is looking for clarification regarding the R2 requirement language that is mandating specific and prescriptive security controls to be monitored for change relevant to CIP-007 standard. In particular, the proposed requirement language of "… that include at least one cyber security control for each of the following…" is the area of confusion. See underlined section within the proposed requirement language below:

"Methods to monitor, per system capability, at least once every 35 calendar days, for unauthorized changes that affect Applicable Systems, where those changes alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-007, as defined by the Responsible Entity; that include at least one cyber security control for each of the following:

2.1.1. Configuration on each Applicable System that affects its routable protocol network accessibility;

2.1.2. Configuration of CPU or memory sharing of VCAs on SCI;

2.1.3. Installation, removal, and update of operating system, firmware, software, and cyber security patches.

2.1.4. Configuration of malicious code protection methods;

2.1.5. Configuration of security event logging or alerting;

2.1.6. Configuration of authentication methods; and

2.1.7. Changes to the enabled or disabled status of accounts."

ISO/RTO Council would like for the SDT to clarify if the intent of this requirement is to monitor for changes to all of the CIP-007 controls? If this is meant to be defined by the entity, ISO-NE recommends moving the sub-bullets language to the measures section similar to R1.

ISO-NE adds the following comment:

With respect to the proposed 2.1.7 sub-requirement, changes to account access should be considered part of CIP-004 Access Management as a subject and not be administered from the CIP-007 requirements. ISO-NE recommends striking the 2.1.7 sub-requirement if the sub-requirements are retained in the proposed version of CIP-010 R2.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

With respect to R1.4, BC Hydro seeks clarity, if evidence from a representative test system is sufficient OR if evidence from a production system(s) is also required in all cases.

Requirement R1.4 uses "behavior" which is a very open term and can be used in many ways. BC Hydro seeks clarity on this with examples or use cases to explain the scope of the word behavior.

Likes 0	
Dislikes 0	

Response

Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)

Answer	No
Document Name	

Comment

The SRC requests clarification regarding the language in requirement R2 that mandates the use of specific and prescriptive security controls to be monitored for changes relevant to the CIP-007 standard. In particular, the SRC requests clarification of the proposed requirement language of "… that include at least one cyber security control for each of the following…." See the underlined section within the proposed requirement language below:

"Methods to monitor, per system capability, at least once every 35 calendar days, for unauthorized changes that affect Applicable Systems, where those changes alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in

CIP-007, as defined by the Responsible Entity; **that include at least one cyber security control for each of the following**:

2.1.1. Configuration on each Applicable System that affects its routable protocol network accessibility;

2.1.2. Configuration of CPU or memory sharing of VCAs on SCI;

2.1.3. Installation, removal, and update of operating system, firmware, software, and cyber security patches.

2.1.4. Configuration of malicious code protection methods;

2.1.5. Configuration of security event logging or alerting;

2.1.6. Configuration of authentication methods; and

2.1.7. Changes to the enabled or disabled status of accounts."

The requirements contained in the draft of CIP-007-7 have a combined total of 21 Parts, but the draft CIP-010-5 R2 language only lists seven controls (Parts 2.1.1 – 2.1.7). It is therefore unclear whether R2 is intended to require entities to monitor for changes that impact all CIP-007 controls or only for changes that impact the items listed in R2. The SRC requests that the SDT clarify this ambiguity. If the intent is for entities to determine which controls to include in their monitoring to detect changes that would impact CIP-007 protections, the SRC recommends moving the language in Parts 2.1.1 – 2.1.7 to the measures section, similar to the way the measures section associated with requirement R1 Part 1.1 is structured.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

NIPSCO disagrees with the changes as "security controls" needs to be better scoped and defined.

Likes 0	
Dislikes 0	

Response

Shannon Mickens - Shannon Mickens On Behalf of: Joshua Phillips, Southwest Power Pool, Inc. (RTO), 2; - Shannon Mickens, Group Name SPP RTO

Answer	No
Document Name	

Comment

There appears to be inconsistency in the CIP-010-5 proposed draft language for Requirements R1 (authorization) and R2 (monitoring). The draft R2 language is more prescriptive for a set of CIP-007 controls while the draft R1 language is now non-prescriptive and related to the “behavior” of CIP-005 and CIP-007 controls, which is subjective and does not align with the list of CIP-007 controls listed in the draft R2 language. In addition, the CIP-010-5 proposed draft language is unclear whether R2 is intended to require entities to monitor for changes that impact all CIP-007 controls or only for changes that impact the items listed in R2. SPP recommends keeping the currently approved requirement language of CIP-010-4, Requirements R1 and R2, as entities have already established virtualized environments that comply with CIP-010-4 today.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

The proposed language removes the baseline requirements that had previously outlined specifically what needed authorization change requests and has been replaced with referencing all of CIP-005 and CIP-007 controls. As the standards evolve over time this makes is unclear and left open for interpretation of what changes an Entity must consider for authorization requests for compliance purposes vs. “best practices”. NCPA recommends including language in 1.1 to include the specific criteria that an Entity will be held accountable to in the requirement.

Likes 0	
Dislikes 0	

Response

Nicolas Turcotte - Hydro-Quebec (HQ) - 1

Answer	No
Document Name	

Comment

HQ supports NPCC RSC comments and provides the following additional comments:

Considering the ambiguity of the controls defined in CIP-005 5 and CIP-007 the updated version of Table R1, part 1.1 deteriorates the cyber security of the cyber assets,. The Measures column contains more explicit examples than the requirement themselves. As an example, for CIP-007 the requirement is “Disable or prevent unneeded routable protocol network accessibility on each Applicable System, per system capability.”. The column Measures of CIP-007 R1.1 contains the following :

• Installation, removal, or update of operating system, firmware, software, or cyber security patches, including changes to VCA parent images from which Applicable Systems will be instantiated (CIP-007 R1.1, R2)

• Configuration changes that affect routable protocol network accessibility (CIP-007 R1.1)

The SDT should ensure that controls are clearly defined in CIP-005 and CIP-007 .The SDT should also ensure that the requirements are easy measurable, and limit interpretations.

The suggested version of requirement 1.3 is defining the applicability by listing the following components; the operating systems, firmware, software, or software patches In the previous version of this requirement, the applicability was 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; and 1.1.5. Any security patches applied. The SDT should evaluate if the intent, of the new version, was it to increase the scope of the requirement.

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	No
Document Name	

Comment

Regarding CIP-010 R1, Texas RE continues to be concerned security obligations will be reduced by removing the reference to baseline configurations. Establishing and maintaining baseline configurations represent best practices for system hardening. Texas RE recommends adhering to NIST Special Publication 800-53 (Rev. 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.” See also CM-7 Least Functionality, which states: Review and update the list of authorized software programs.

Regarding CIP-010 R2, Texas RE is concerned the proposed changes to CIP-010 R1 do not include a control to verify that unintended changes have not been made. For medium impact BCS this is currently captured in requirements to authorize changes and update baseline configuration documentation within 30 calendar days. Texas RE recommends adding medium impact BCS and their associated EACMS and PCA to the Applicable Systems column of CIP-010 R2 and its subpart(s). In FERC Order 706, paragraph 398 FERC states 'We agree with ISO/RTO Council that the phrase “verification that unintended changes have not been made” captures the core issue. Our concern is that some form of verification is performed to detect when unauthorized changes have been made and to identify those changes, as well as ensuring that the proper alerts are issued.'

Further, Texas RE recommends dividing CIP-010 R2 Part 2.1 into two parts for clarity:

CIP-010 R2 Part 2.1:

The Responsible Entity shall define its cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-007, to include at least one cyber security control from each of the following:

2.1.1. Configuration on each Applicable System that affects its routable protocol network accessibility;

2.1.2. Configuration of CPU or memory sharing of VCAs on SCI;

2.1.3. Installation, removal, and update of operating system, firmware, software, and cyber security patches.

2.1.4. Configuration of malicious code protection methods;

2.1.5. Configuration of security event logging or alerting;

2.1.6. Configuration of authentication methods; and

2.1.7. Changes to the enabled or disabled status of accounts.

CIP-010 R2 Part 2.2:

The Responsible Entity shall implement methods to monitor, per system capability, at least once every 35 calendar days, for unauthorized changes that affect Applicable Systems, where those changes alter the behavior of one or more cyber security controls defined in Part 2.1.

Likes 0	
Dislikes 0	

Response

Junji Yamaguchi - Hydro-Quebec (HQ) - 5

Answer	No
Document Name	

Comment

HQ supports NPCC RSC comments and provides the following additional comments:

Considering the ambiguity of the controls defined in CIP-005 5 and CIP-007 the updated version of Table R1, part 1.1 deteriorates the cyber security of the cyber assets,. The Measures column contains more explicit examples than the requirement themselves. As an example, for CIP-007 the requirement is “Disable or prevent unneeded routable protocol network accessibility on each Applicable System, per system capability.”. The column Measures of CIP-007 R1.1 contains the following :

• Installation, removal, or update of operating system, firmware, software, or cyber security patches, including changes to VCA parent images from which Applicable Systems will be instantiated (CIP-007 R1.1, R2)

• Configuration changes that affect routable protocol network accessibility (CIP-007 R1.1)

The SDT should ensure that controls are clearly defined in CIP-005 and CIP-007 .The SDT should also ensure that the requirements are easy measurable, and limit interpretations.

The suggested version of requirement 1.3 is defining the applicability by listing the following components; the operating systems, firmware, software, or software patches In the previous version of this requirement, the applicability was 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; and 1.1.5. Any security patches applied. The SDT should evaluate if the intent, of the new version, was it to increase the scope of the requirement.	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	No
Document Name	
Comment	
The new language in CIP-010 has become more complex adding to compliance risk. Additionally, CIP-010 R2 may become harder to monitor and some of the configurations required to be monitored may require new tools than the current baseline monitoring tools.	
Likes 0	
Dislikes 0	
Response	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	No
Document Name	
Comment	
The new language in CIP-010 has become more complex adding to compliance risk. Additionally, CIP-010 R2 may become harder to monitor and some of the configurations required to be monitored may require new tools than the current baseline monitoring tools.	
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 RSC	
Answer	No
Document Name	
Comment	

Please clarify if the change management approach or objective is shifting from change managing a device configuration to change managing a “policy” or process approach. The confusion is if the shift of focus is from managing assets determined by CIP 2 criteria towards Responsible Entity methods / processes / “policy” based documented plan.

Example would be dealing with planned patch management (based on schedule or plan). If the patch does not impact CIP 5 or CIP 7 security controls, does change management only apply from a deviation of the patch management plan / policy?

Suggest adding the concept of intent or “intended changes” into R1.1 and R1.4, otherwise R1.4 becomes a defacto full vulnerability assessment for any change

Suggest

R1.1

Authorize intended changes that affect Applicable Systems where those intended changes 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.

R1.4

As a part of the intended changes authorized per Part 1.1, verify that the behavior(s) any cyber security controls that were intentionally altered, or previously assessed as potentially being altered, were not adversely affected.

Likes 0	
Dislikes 0	

Response

Constantin Chitescu - Ontario Power Generation Inc. - 5

Answer	No
Document Name	

Comment

OPG supports NPCC Regional Standards Committee’s comments.

Please clarify if the change management approach or objective is shifting from change managing a device configuration to change managing a “policy” or process approach. The confusion is if the shift of focus is from managing assets determined by CIP 2 criteria towards Responsible Entity methods / processes / “policy” based documented plan.
Example would be dealing with planned patch management (based on schedule or plan). If the patch does not impact CIP 5 or CIP 7 security controls, does change management only apply from a deviation of the patch management plan / policy?

Suggest adding the concept of intent or “intended changes” into R1.1 and R1.4, otherwise R1.4 becomes a defacto full vulnerability assessment for any change
Suggest
R1.1
Authorize intended changes that affect Applicable Systems where those intended changes 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.
R1.4
As a part of the intended changes authorized per Part 1.1, verify that the behavior(s) any cyber security controls that were intentionally altered, or

previously assessed as potentially being altered, were not adversely affected.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

NST is unpersuaded by the SDT's argument that in modern computing environments, configuration baselines are of sufficiently limited value, while also being burdensome to maintain, that they can quite reasonably be downgraded from being included in CIP-010 requirements, and instead offered as merely one possible approach to compliance. Establishing and maintaining configuration baselines are identified as key elements of any good cyber security program in several NIST publications, including recently released SP 800-82 Release 3 ("Guide to Operational Technology (OT) Security") and the one cited by the SDT in its most recent Technical Justification document. Given the long-standing enthusiasm among both FERC and NERC personnel for examining and enhancing the mapping between CIP and NIST Standards, dropping a requirement to maintain documented configuration baselines seems oddly out of step with that and other related initiatives.

Regarding R1.1, it is NST's opinion that if the proposed language was adopted, there would be no end to arguments between Responsible Entities and Regional Entity audit teams about whether compliance had been adequately demonstrated. There are many possible changes to a Cyber Asset's installed software, such as security patches for data packet handlers, that would have no impact on the behavior of CIP-005 or CIP-007 controls. Should changes of this nature be exempt from a requirement to formally authorize them? NST is also concerned that allowing Responsible Entities to define the specific CIP-005 and CIP-007 controls within the scope of R1.1 could result in significant disparities among Responsible Entities and/or Regions in how these controls are identified. NST agrees CIP requirements should be written in a manner that avoids making them overly prescriptive, but at a time when NERC is seeking to impose greater consistency on Entities' CIP-008 programs (universal "attempts to compromise" criteria), it seems counterintuitive for a drafting team to be proposing changes to CIP-010 that would, in our opinion, reduce consistency.

Regarding R2.1:

NST notes that CIP-005 controls are omitted. We presume this to have been an oversight.

NST considers the proposed list of monitored items to be reasonable, but as with R1.1, we believe that it's a mistake to limit the scope to only those changes that could impact CIP-005 or CIP-007 controls, and that allowing Entities to decide on their own what they'll monitor could lead to many and varied interpretations of what R2.1 is intended to require. For example, 2.1.3 specifies monitoring for unauthorized "Installation, removal, and update of operating system, firmware, software, and cyber security patches." As noted previously, many such changes wouldn't alter CIP-005 and/or CIP-007 controls. Would it be permissible for an Entity to not consider 2.1.3 at all unless changes to a Cyber Asset's CIP-005 and/or CIP-007 behavior is detected?

Likes 0	
Dislikes 0	

Response

Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5 - NPCC	
Answer	No
Document Name	

Comment

Please clarify if the change management approach or objective is shifting from change managing a device configuration to change managing a “policy” or process approach. The confusion is if the shift of focus is from managing assets determined by CIP 2 criteria towards Responsible Entity methods / processes / “policy” based documented plan.
Example would be dealing with planned patch management (based on schedule or plan). If the patch does not impact CIP 5 or CIP 7 security controls, does change management only apply from a deviation of the patch management plan / policy?

Suggest adding the concept of intent or “intended changes” into R1.1 and R1.4, otherwise R1.4 becomes a defacto full vulnerability assessment for any change
Suggest
R1.1
Authorize intended changes that affect Applicable Systems where those intended changes 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.
R1.4
As a part of the intended changes authorized per Part 1.1, verify that the behavior(s) any cyber security controls that were intentionally altered, or previously assessed as potentially being altered, were not adversely affected.

Likes 0	
Dislikes 0	

Response

Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
Answer	No
Document Name	

Comment

1) With the Guidelines and Technical Basis section removed from the CIP-010-5 standard and currently nothing in the Technical Rationale or Implementation documents outlining what a CIP-010-5 R3 paper based or active vulnerability assessment should contain, does the SDT plan to add any guidance for vulnerability assessments as it relates to SCI in these aforementioned documents?

2) We need to better understand the timeline, since the 30 day timeframe is no longer listed. Also need to better understand what evidence to provide for a “baseline”, since the R1 has been changed. Remove the phrase "the behavior of".

Justification:

1) adding "the behavior of" might make the requirement not backwards compatible

2) adding "the behavior of" could give an impression to an auditor that we need to have additional detailed testing such as penetration testing of each altered control

3) this word will cause security teams to spend a lot of time needlessly testing low-value controls rather than looking for adversaries in their networks	
Likes 0	
Dislikes 0	
Response	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
ERCOT joins the comments submitted by the IRC SRC and adopts them as its own.	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
FirstEnergy does not opposed these changes.	
Likes 0	
Dislikes 0	
Response	
Richard Vendetti - NextEra Energy - 5	
Answer	Yes
Document Name	
Comment	
NEE supports EEI comments	
Likes 0	

Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern agrees with the changes in CIP-010 regarding the updates to change management controls. They include the change behaviors as well as the excluded physical and procedural controls, serving one or more requirement parts in CIP-005 or CIP-007.	
Likes 0	
Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF agrees with the proposed changes to CIP-010.	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes
Document Name	
Comment	
ITC supports the response submitted by EEI	
Likes 0	
Dislikes 0	
Response	

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI supports the proposed changes to CIP-010.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon supports the comments submitted by the EEI.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon is supporting EEI comments in response to this question.	
Likes 0	
Dislikes 0	
Response	
Marcus Bortman - APS - Arizona Public Service Co. - 6	

Answer	Yes
Document Name	
Comment	
AZPS supports the proposed changes	
Likes 0	
Dislikes 0	
Response	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Ameren supports the proposed changes to CIP-010.	
Likes 0	
Dislikes 0	
Response	
Tracy MacNicoll - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
USV supports the comments made by NPCC RSC	
Likes 0	
Dislikes 0	
Response	
Joanne Anderson - Public Utility District No. 2 of Grant County, Washington - 1,4,5,6 - WECC	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
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	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
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	
Richard Jackson - U.S. Bureau of Reclamation - 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	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Rebika Yitna - MEAG Power - 1,3 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
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	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ben Hammer - Western Area Power Administration - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sheila Suurmeier - Black Hills Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Rachel Schuldt - Rachel Schuldt On Behalf of: Claudine Bates, Black Hills Corporation, 5, 6, 1, 3; - Rachel Schuldt	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Josh Combs - Black Hills Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Micah Runner - Black Hills Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Casey Jones - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Flanary - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
C. A. Campbell - LS Power Development, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Ellese Murphy On Behalf of: Marcelo Pesantez, Duke Energy - Florida Power Corporation, 3; - Ellese Murphy	

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	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
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	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
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	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alain Mukama - Hydro One Networks, Inc. - 1,3	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 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	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	

6. The SDT revised CIP-003. Do you agree with the proposed changes to these Reliability Standards? If not, please provide the basis for your disagreement and an alternate proposal.

Kristine Martz - Amazon Web Services - 7

Answer	No
Document Name	

Comment

The inclusion of “Shared Cyber Infrastructure (SCI) that supports a low impact BCS” in the applicable systems identified in CIP-003 R2, may be confusing to Responsible Entities who only have low impact BCS because the proposed SCI definition only identifies as SCI those programmable electronic devices that host or are associated with applicable systems of different impact ratings.

First, it appears that if a Responsible Entity is using infrastructure to host only low impact VCAs, the proposed SCI definition would make CIP-003-10 R2 inapplicable to such shared infrastructure.

Second, if the Responsible Entity is using SCI to host VCAs with a low impact and another different impact rating, the proposed standard suggests that the SCI (and all of its VCAs) would need to be protected at the level applicable to the impact rating of the highest impact system(s) hosted, which would apparently subject the SCI hosting a low impact BCS to the requirements for SCI hosting medium or high impact BCS, making the requirements in CIP-003-10 R2 unnecessary or redundant.

AWS encourages the Standard Drafting Team for Project 2016-02 to develop implementation guidance, include statements in the CIP-003 Technical Rationale, or other appropriate industry supporting documents, to clarify how Responsible Entities should implement the new requirements for SCI supporting low impact BCS under CIP-003 R2 given the two issues identified above.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

NST believes Appendix 1 Section 2 (Physical Security Controls) should include supporting SCI, if any, for consistency with other revised CIP-003 requirements.

Likes 0	
Dislikes 0	

Response

Ben Hammer - Western Area Power Administration - 1

Answer	No
Document Name	

Comment

The changes to CIP-003 Specifically R2 attachment 1. should be incorporated into the CIP-004, CIP-005, CIP-006, CIP-007, and CIP-010 standards, add requirements to those standards as they pertain to low impact BES Cyber systems, either to existing requirements or to new requirements. Leave CIP-003 specifically to establishing responsibility and accountability. For Section 3 part 3.1 add an and after the 1st bullet, as shown below:

3.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are:

i. Between:

- a low impact BCS; or
- An SCI that supports a low impact BCS and a Cyber System(s) outside the asset containing:
  - the low impact BCS(s); or
  - the SCI that supports a low impact BCS; **and**

ii. using a routable protocol when entering or leaving the asset containing the low impact BCS or SCI that supports a low impact BCS; and

iii. not used for time-sensitive communications of Protection Systems.

Likes 0	
Dislikes 0	

Response

Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC

Answer	No
Document Name	

Comment

SMUD and BANC feel that inconsistent use of the word “system”, especially with regards to “per system capability” is making the High and Medium impact requirements less stringent than the Low impact requirements. We recommend changing the language to “per Cyber Asset capability”.

Likes 0	
Dislikes 0	

Response

Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez

Answer	Yes

Document Name	
Comment	
CIP Virtualization Standard proposed is CIP-003-10 is not clear. Choppy jump from section 3 to section 6, need to combine. Recommend skip this version, go to or wait for CIP-003-a	
Likes 0	
Dislikes 0	
Response	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
AZPS supports the proposed changes	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon is supporting EEI comments in response to this question.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	

Comment	
Exelon supports the comments submitted by the EEI.	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI supports the proposed changes made to CIP-003.	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes
Document Name	
Comment	
ITC supports the response submitted by EEI	
Likes 0	
Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	

The NAGF agrees with the proposed changes to CIP-003.	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern agrees with and supports the proposed changes to CIP-003.	
Likes 0	
Dislikes 0	
Response	
Richard Vendetti - NextEra Energy - 5	
Answer	Yes
Document Name	
Comment	
NEE supports EEI comments	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
FirstEnergy does not opposed these changes.	

Likes 0	
Dislikes 0	
Response	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
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	
Tracy MacNicoll - Utility Services, Inc. - 4	

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	
Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5 - NPCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Alain Mukama - Hydro One Networks, Inc. - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation 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	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Junji Yamaguchi - Hydro-Quebec (HQ) - 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	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
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	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Quebec (HQ) - 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	
Shannon Mickens - Shannon Mickens On Behalf of: Joshua Phillips, Southwest Power Pool, Inc. (RTO), 2; - Shannon Mickens, Group Name SPP RTO	
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	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)	
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	
Ellese Murphy - Ellese Murphy On Behalf of: Marcelo Pesantez, Duke Energy - Florida Power Corporation, 3; - Ellese Murphy	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
C. A. Campbell - LS Power Development, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Flanary - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Casey Jones - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Micah Runner - Black Hills Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Schuldt - Rachel Schuldt On Behalf of: Claudine Bates, Black Hills Corporation, 5, 6, 1, 3; - Rachel Schuldt	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Josh Combs - Black Hills Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sheila Suurmeier - Black Hills Corporation - 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	

Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rebika Yitna - MEAG Power - 1,3 - SERC	
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	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Robert Follini - Avista - Avista Corporation - 3	
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	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anne Kronshage - Public Utility District No. 1 of Chelan County - 6, Group Name Public Utility District No. 1 of Chelan County - Voting Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert	

Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Keele - Entergy - 1,3,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joanne Anderson - Public Utility District No. 2 of Grant County, Washington - 1,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	
Document Name	
Comment	
Answer is yes.	
Likes 0	
Dislikes 0	
Response	

7. The SDT revised the Implementation Plan to accommodate for the future enforceable date of CIP-003-9. Do you agree with the proposed Implementation Plan? If not, please provide the basis for your disagreement and an alternate proposal.

Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF

Answer	No
Document Name	

Comment

The NAGF believes that NERC needs to clarify the process and time lines for reconciliation of the multiple CIP-003 Standards Under Development and CIP-003-09 before being able to answer Question 7 accurately.

Likes 0	
Dislikes 0	

Response

Teresa Krabe - Lower Colorado River Authority - 5

Answer	No
Document Name	

Comment

Unintended consequences of IRA definition could increase cost of physical access controls for medium impact with IRA.

Likes 0	
Dislikes 0	

Response

James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin

Answer	No
Document Name	

Comment

Unintended consequences of IRA definition could increase cost of physical access controls for medium impact with IRA.

Likes 0	
Dislikes 0	

Response

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
NST's "No" on this question reflects our concerns about several proposed or revised definitions and about proposed changes to CIP-003, CIP-004, CIP-005, CIP-007, and CIP-010.	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
FirstEnergy does not opposed these changes.	
Likes 0	
Dislikes 0	
Response	
Richard Vendetti - NextEra Energy - 5	
Answer	Yes
Document Name	
Comment	
NEE supports EEI comments	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	

Answer	Yes
Document Name	
Comment	
Southern agrees with the revised Implementation Plan to become effective on or about April 1, 2026 or the first day of the first calendar quarter that is twenty-four (24) months after the effective date of the applicable governmental authority's order approving the Revised CIP Standards and Definitions.	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes
Document Name	
Comment	
ITC supports the response submitted by EEI	
Likes 0	
Dislikes 0	
Response	
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	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	

Comment	
Exelon supports the comments submitted by the EEI.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon is supporting EEI comments in response to this question.	
Likes 0	
Dislikes 0	
Response	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
AZPS supports the revised implementation plan.	
Likes 0	
Dislikes 0	
Response	
Joanne Anderson - Public Utility District No. 2 of Grant County, Washington - 1,4,5,6 - WECC	
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	
James Keele - Entergy - 1,3,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Anne Kronshage - Public Utility District No. 1 of Chelan County - 6, Group Name Public Utility District No. 1 of Chelan County - Voting Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsey Mannion - ReliabilityFirst - 10	
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	
Richard Jackson - U.S. Bureau of Reclamation - 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	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
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	
Rebika Yitna - MEAG Power - 1,3 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Karen Artola - CPS Energy - 1,3,5 - Texas RE	
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	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ben Hammer - Western Area Power Administration - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Sheila Suurmeier - Black Hills Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Schuldt - Rachel Schuldt On Behalf of: Claudine Bates, Black Hills Corporation, 5, 6, 1, 3; - Rachel Schuldt	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Josh Combs - Black Hills Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Micah Runner - Black Hills Corporation - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Casey Jones - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Flanary - Midwest Reliability Organization - 10	
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	
C. A. Campbell - LS Power Development, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Ellese Murphy On Behalf of: Marcelo Pesantez, Duke Energy - Florida Power Corporation, 3; - Ellese Murphy	
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	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)	
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	
Shannon Mickens - Shannon Mickens On Behalf of: Joshua Phillips, Southwest Power Pool, Inc. (RTO), 2; - Shannon Mickens, Group Name SPP RTO	
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	
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	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC	

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	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alain Mukama - Hydro One Networks, Inc. - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5 - NPCC	
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	
Tracy MacNicoll - Utility Services, Inc. - 4	

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	
Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	
Document Name	
Comment	
Answer is yes.	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	
Document Name	
Comment	
No Comment	
Likes 0	
Dislikes 0	
Response	

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

Kristine Martz - Amazon Web Services - 7

Answer	
Document Name	

Comment

AWS supports the efforts of the Project 2016-02 SDT in addressing industry comments and feedback. We understand that the proposed revisions address on-premises virtualization, though we appreciate that these changes, such as the removal of Cyber Asset references directly in requirement language, could enable further consideration of cloud technology in future standards development projects.

Should these revisions not achieve industry consensus to move forward, we encourage the SDT to consider alternatives to the standards development process to achieve the outcomes set forth in the SAR including the development of ERO endorsed implementation guidance based on the many educational resources the SDT has already created to educate industry on cyber security for virtualized environments. Additionally, we encourage NERC to develop Risk-Based Compliance Monitoring and Enforcement Program (CMEP) Practice Guides to provide direction to ERO Enterprise CMEP staff on approaches to carry out compliance monitoring and enforcement activities related to virtualization, which is already widely employed across the industry and provides a number of oprtational and cost efficiencies as well as other benefits. Clear guidance on CIP compliance for virtual assets would greatly benefit the industry and its stakeholders by allowing for compliance certainty when moving towards greater virtualization.

Likes 0	
Dislikes 0	

Response

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

Answer	
Document Name	

Comment

ACES and it’s members would like to thank the SDT for their continued hard work.

Likes 0	
Dislikes 0	

Response

Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez

Answer	
Document Name	

Comment

With the Guidelines and Technical Basis section removed from the CIP-010-5 standard and currently nothing in the Technical Rationale or Implementation documents outlining what a CIP-010-5 R3 paper based or active vulnerability assessment should contain, does the SDT plan to add any guidance for vulnerability assessments as it relates to SCI in these aforementioned documents?

Likes 0	
Dislikes 0	

Response

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

Answer	
Document Name	

Comment

No additional comments at this time.

Likes 0	
Dislikes 0	

Response

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

Daniel Gacek - Exelon - 1

Answer	
Document Name	

Comment

Exelon supports the comments submitted by the EEI.

Likes 0	
Dislikes 0	

Response

Teresa Krabe - Lower Colorado River Authority - 5

Answer	
Document Name	

Comment

None at this time.

Likes 0	
Dislikes 0	

Response

Junji Yamaguchi - Hydro-Quebec (HQ) - 5

Answer	
Document Name	

Comment

The SDT added this exemption 4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations. Our understanding is that “communication networks” is associated with routable protocol (layer 3 of the OSI model) and that “data communication links” is associated with non routable protocol (layer 2 of the OSI model). SDT should clarify the intend if this is not the case.

The SDT should ensure the security posture of the Cyber Assets and not only facilitating the adoption of new technology by introducing ambiguous requirements.

The SDT should evaluate the requirements against the ERT tool approach. In other words, can the requirement be evaluated with the ERT tool.

The SDT should ensure that the requirements are clear and precise and stand by themselves and that no additional reading is required, i.e., technical rational. The technical rational should be viewed as a rational and not provide explanation on how to understand the requirement.

The SDT should review the requirements with the concept of applying Protection Systems definition.

Likes 0	
Dislikes 0	

Response

Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	
Document Name	
Comment	
The CIP-004-8 R2.3, R4.1.2, R5.1, R5.2, R6.1.2, R6.3, exclusion '(except for medium impact without ERC)' appears to be unnecessary considering medium impact without ERC is not an applicable system of the requirement.	
Likes 0	
Dislikes 0	
Response	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	
Document Name	
Comment	
In the draft standards there is inconsistency in the wording of section "C. Compliance | 1. Compliance Monitoring Process | 1.1. Compliance Enforcement Authority:". The following wording is used in CIP-003-10, and is suggested for the other standards as it matches the definition in the NERC Rules of Procedures: **1.1. Compliance Enforcement Authority:** As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with mandatory and enforceable Reliability Standards. The following is used in CIP-004-8, CIP-005-8, CIP-007-7 and CIP-010-5 **1.1. Compliance Enforcement Authority:** "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.	
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
No additional comments.
Likes 0	
Dislikes 0	
Response
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1
Answer	
Document Name	
Comment
Thank you for the ability to comment.
Likes 0	
Dislikes 0	
Response
Nicolas Turcotte - Hydro-Quebec (HQ) - 1
Answer	
Document Name	
Comment
The SDT added this exemption 4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations. Our understanding is that “communication networks” is associated with routable protocol (layer 3 of the OSI model) and that “data communication links” is associated with non routable protocol (layer 2 of the OSI model). SDT should clarify the intend if this is not the case. The SDT should ensure the security posture of the Cyber Assets and not only facilitating the adoption of new technology by introducing ambiguous requirements.

The SDT should evaluate the requirements against the ERT tool approach. In other words, can the requirement be evaluated with the ERT tool.

The SDT should ensure that the requirements are clear and precise and stand by themselves and that no additional reading is required, i.e., technical rational. The technical rational should be viewed as a rational and not provide explanation on how to understand the requirement.

The SDT should review the requirements with the concept of applying Protection Systems definition.

Likes 0	
Dislikes 0	

Response

Richard Vendetti - NextEra Energy - 5

Answer	
Document Name	

Comment

NEE supports EEI comments

Likes 0	
Dislikes 0	

Response

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

Answer	
Document Name	

Comment

MPC supports comments submitted by the MRO NERC Standards Review Forum (NSRF).

Likes 0	
Dislikes 0	

Response

Ellese Murphy - Ellese Murphy On Behalf of: Marcelo Pesantez, Duke Energy - Florida Power Corporation, 3; - Ellese Murphy

Answer	
Document Name	

Comment

Duke Energy thanks the Virtualization Standard Drafting Team for their hard work to get to Draft 5, and for their careful consideration of industry comments from Draft 4.

Likes 0	
Dislikes 0	

Response

Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO

Answer	
Document Name	

Comment

In the draft standards there is inconsistency in the wording of section “C. Compliance | 1. Compliance Monitoring Process | 1.1. Compliance Enforcement Authority:”. The following wording is used in CIP-003-10, and is suggested for the other standards as it matches the definition in the NERC Rules of Procedures:

1.1. Compliance Enforcement Authority: As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with mandatory and enforceable Reliability Standards.

The following is used in CIP-004-8, CIP-005-8, CIP-007-7 and CIP-010-5

1.1. Compliance Enforcement Authority: “Compliance Enforcement Authority” (CEA)

means NERC or the Regional Entity, or any entity as otherwise designated by an

Applicable Governmental Authority, in their respective roles of monitoring and/or

enforcing compliance with mandatory and enforceable Reliability Standards in

their respective jurisdictions.

Likes 0	
Dislikes 0	

Response

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

Answer	
Document Name	

Comment	
CIP-005 R2.6: BPA reiterates disagreement with the requirement to prevent sharing of memory resources in R2.6. 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. 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	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	
Document Name	
Comment	
No additional comments	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	
Document Name	
Comment	
NA	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	
Document Name	

Comment
FirstEnergy asks the DT for clarification training requirements for CIP-004. Training requirement 2.2 and 2.3 appear to be inconsistent in the description with the use of “includes Mediums with ERC” as well as Access Authorization/verification in requirement 4.1 and 4.2.

Likes 0	
Dislikes 0	

Response