

Comment Report

Project Name:	2016-02 Modifications to CIP Standards Virtualization - Draft 3
Comment Period Start Date:	2/18/2022
Comment Period End Date:	4/12/2022
Associated Ballots:	2016-02 Modifications to CIP Standards Virtualization CIP-002-7 AB 3 ST 2016-02 Modifications to CIP Standards Virtualization CIP-003-9 AB 3 ST 2016-02 Modifications to CIP Standards Virtualization CIP-004-7 AB 3 ST 2016-02 Modifications to CIP Standards Virtualization CIP-005-8 AB 3 ST 2016-02 Modifications to CIP Standards Virtualization CIP-006-7 AB 3 ST 2016-02 Modifications to CIP Standards Virtualization CIP-007-7 AB 3 ST 2016-02 Modifications to CIP Standards Virtualization CIP-008-7 AB 3 ST 2016-02 Modifications to CIP Standards Virtualization CIP-009-7 AB 3 ST 2016-02 Modifications to CIP Standards Virtualization CIP-010-5 AB 3 ST 2016-02 Modifications to CIP Standards Virtualization CIP-011-3 AB 3 ST 2016-02 Modifications to CIP Standards Virtualization CIP-013-3 AB 3 ST

There were 85 sets of responses, including comments from approximately 187 different people from approximately 125 companies representing 10 of the Industry Segments as shown in the table on the following pages.

Questions

- 1. The SDT has redefined Shared Cyber Infrastructure (SCI) such that it now focuses on cyber infrastructure that shares its hardware resources among VCAs of different impact levels only, which then subjects the SCI to additional requirements. Virtualization infrastructure that only hosts VCAs or associated VCAs of the same impact level is no longer SCI and requires no recategorization from current state. The SDT also removed the SCI identification changes from CIP-002. The SDT believes this greatly simplifies SCI. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.**
- 2. The SDT has reinstated the currently approved ESP definition and appended language to allow for zero trust models. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal. Please also include any comments on the proposed EAP definition in the response to this question.**
- 3. The SDT modified the ERC definition from the “outside the asset containing” reference point in the previous draft back to an ESP reference point. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.**
- 4. The SDT has modified the IRA definition to simplify it, primarily in regards to the routable protocol to serial conversion scenario. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.**
- 5. The SDT modified the VCA definition primarily to include the ability to host them on numerous asset types other than SCI. This allows for current state, where entities consider hypervisors as BCA, EACMS, etc. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.**
- 6. The SDT modified numerous other glossary terms. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.**
- 7. The SDT revised CIP-005 based on industry comments. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.**
- 8. 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.**
- 9. The SDT revised CIP-010 R1 to focus on defining change, authorizing change, and verifying that CIP-005 and CIP-007 related security controls are not affected by changes. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.**
- 10. The SDT made other revisions 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.**

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

12. The SDT has revised numerous VSL's for simplification. Do you agree with the proposed changes? If not, please provide the basis for your disagreement.

13. The SDT has revised the Implementation Plan to include the Planned and Unplanned Changes provisions and to allow for early adoption. Do you agree with the proposed Implementation Plan? If not, please provide the basis for your disagreement and an alternate proposal.

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

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
BC Hydro and Power Authority	Adrian Andreoiu	1	WECC	BC Hydro	Hootan Jarollahi	BC Hydro and Power Authority	3	WECC
					Helen Hamilton Harding	BC Hydro and Power Authority	5	WECC
					Adrian Andreoiu	BC Hydro and Power Authority	1	WECC
Tennessee Valley Authority	Brian Millard	1,3,5,6	SERC	Tennessee Valley Authority	Kurtz, Bryan G.	Tennessee Valley Authority	1	SERC
					Grant, Ian S.	Tennessee Valley Authority	3	SERC
					Thomas, M. Lee	Tennessee Valley Authority	5	SERC
					Parsons, Marjorie S.	Tennessee Valley Authority	6	SERC
Santee Cooper	Chris Wagner	1,3,5,6		Santee Cooper	Jennifer Richards	Santee Cooper	1,3,5,6	SERC
					LaChelle Brooks	Santee Cooper	1,3,5,6	SERC
					Rene' Free	Santee Cooper	1,3,5,6	SERC
					Rodger Blakely	Santee Cooper	1,3,5,6	SERC
					Kris Andrews	Santee Cooper	1,3,5,6	SERC
					Wanda Williams	Santee Cooper	1,3,5,6	SERC
MRO	Kendra Buesgens	1,2,3,4,5,6	MRO	MRO NSRF	Bobbi Welch	Midcontinent ISO, Inc.	2	MRO
					Christopher Bills	City of Independence Power & Light	3,5	MRO
					Fred Meyer	Algonquin Power Co.	3	MRO

					Jamie Monette	Allite - Minnesota Power, Inc.	1	MRO
					Larry Heckert	Alliant Energy Corporation Services, Inc.	4	MRO
					Marc Gomez	Southwestern Power Administration	1	MRO
					Matthew Harward	Southwest Power Pool, Inc.	2	MRO
					LaTroy Brumfield	American Transmission Company, LLC	1	MRO
					Bryan Sherrow	Kansas City Board Of Public Utilities	1	MRO
					Terry Harbour	MidAmerican Energy	1,3	MRO
					Jamison Cawley	Nebraska Public Power	1,3,5	MRO
					Seth Shoemaker	Muscatine Power & Water	1,3,5,6	MRO
					Michael Brytowski	Great River Energy	1,3,5,6	MRO
					David Heins	Omaha Public Power District	1,3,5,6	MRO
					George Brown	Acciona Energy North America	5	MRO
FirstEnergy - FirstEnergy Corporation	Mark Garza	4		FE Voter	Julie Severino	FirstEnergy - FirstEnergy Corporation	1	RF
					Aaron Ghodooshim	FirstEnergy - FirstEnergy Corporation	3	RF
					Robert Loy	FirstEnergy - FirstEnergy Solutions	5	RF
					Tricia Bynum	FirstEnergy - FirstEnergy Corporation	6	RF

					Mark Garza	FirstEnergy-FirstEnergy	4	RF
Public Utility District No. 1 of Chelan County	Meaghan Connell	5		PUD No. 1 of Chelan County	Joyce Gundry	Public Utility District No. 1 of Chelan County	3	WECC
					Diane Landry	Public Utility District No. 1 of Chelan County	1	WECC
					Glen Pruitt	Public Utility District No. 1 of Chelan County	6	WECC
					Meaghan Connell	Public Utility District No. 1 Chelan County	5	WECC
California ISO	Monika Montez	2	WECC	ISO/RTO Council Standards Review Committee (SRC) 2016-02 Virtualization (Draft 3)	Monika Montez	CAISO	2	WECC
					Bobbi Welch	Midcontinent ISO, Inc.	2	MRO
					Dana Showalter	Electric Reliability Council of Texas, Inc.	2	Texas RE
					Helen Lainis	IESO	2	NPCC
					Kathleen Goodman	IS-NE	2	NPCC
					Greg Campoli	NY-ISO	2	NPCC
					Michael Del Viscio	PJM	2	RF
					Charles Yeung	Southwest Power Pool, Inc. (RTO)	2	SERC
Southern Company - Southern Company Services, Inc.	Pamela Hunter	1,3,5,6	SERC	Southern Company	Matt Carden	Southern Company - Southern Company Services, Inc.	1	SERC
					Joel Dembowski	Southern Company - Alabama Power Company	3	SERC

					Ron Carlsen	Southern Company - Southern Company Generation	6	SERC
					Jim Howell	Southern Company - Southern Company Services, Inc. - Gen	5	SERC
Eversource Energy	Quintin Lee	1		Eversource Group	Quintin Lee	Eversource Energy	1	NPCC
					Christopher McKinnon	Eversource Energy	3	NPCC
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	NPCC Regional Standards Committee	Gerry Dunbar	Northeast Power Coordinating Council	10	NPCC
					Randy MacDonald	New Brunswick Power	2	NPCC
					Glen Smith	Entergy Services	4	NPCC
					Alan Adamson	New York State Reliability Council	7	NPCC
					David Burke	Orange & Rockland Utilities	3	NPCC
					Helen Lainis	IESO	2	NPCC
					David Kiguel	Independent	7	NPCC
					Nick Kowalczyk	Orange and Rockland	1	NPCC
					Joel Charlebois	AESI - Acumen Engineered Solutions International Inc.	5	NPCC
					Mike Cooke	Ontario Power Generation, Inc.	4	NPCC

Salvatore Spagnolo	New York Power Authority	1	NPCC
Shivaz Chopra	New York Power Authority	5	NPCC
Deidre Altobell	Con Ed - Consolidated Edison	4	NPCC
Dermot Smyth	Con Ed - Consolidated Edison Co. of New York	1	NPCC
Peter Yost	Con Ed - Consolidated Edison Co. of New York	3	NPCC
Cristhian Godoy	Con Ed - Consolidated Edison Co. of New York	6	NPCC
Nurul Abser	NB Power Corporation	1	NPCC
Randy MacDonald	NB Power Corporation	2	NPCC
Michael Ridolfino	Central Hudson Gas and Electric	1	NPCC
Vijay Puran	NYSPS	6	NPCC
ALAN ADAMSON	New York State Reliability Council	10	NPCC
Sean Cavote	PSEG - Public Service Electric and Gas Co.	1	NPCC
Brian Robinson	Utility Services	5	NPCC
Quintin Lee	Eversource Energy	1	NPCC
Jim Grant	NYISO	2	NPCC
John Pearson	ISONE	2	NPCC
Nicolas Turcotte	Hydro-Qu?bec TransEnergie	1	NPCC

					Chantal Mazza	Hydro-Quebec	2	NPCC
					Michele Tondalo	United Illuminating Co.	1	NPCC
					Paul Malozewski	Hydro One Networks, Inc.	3	NPCC
					Sean Bodkin	Dominion - Dominion Resources, Inc.	6	NPCC
					John Hastings	National Grid USA	1	NPCC
					Michael Jones	National Grid USA	1	NPCC
Dominion - Dominion Resources, Inc.	Sean Bodkin	6		Dominion	Connie Lowe	Dominion - Dominion Resources, Inc.	3	NA - Not Applicable
					Lou Oberski	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
					Larry Nash	Dominion - Dominion Virginia Power	1	NA - Not Applicable
					Rachel Snead	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
Southwest Power Pool, Inc. (RTO)	Shannon Mickens	2	MRO,SPP RE,WECC	SPP RTO	Shannon Mickens	Southwest Power Pool Inc.	2	MRO
					Steven Keller	Southwest Power Pool Inc	2	MRO
Western Electricity Coordinating Council	Steven Rueckert	10		WECC Entity Monitoring	Steve Rueckert	WECC	10	WECC
					Phil O'Donnell	WECC	10	WECC
Lower Colorado River Authority	Teresa Krabe	5		LCRA Compliance	Michael Shaw	LCRA	6	Texas RE
					Dixie Wells	LCRA	5	Texas RE
					Teresa Cantwell	LCRA	1	Texas RE
Associated Electric	Todd Bennett	3		AECI	Michael Bax	Central Electric Power	1	SERC

Cooperative, Inc.						Cooperative (Missouri)		
					Adam Weber	Central Electric Power Cooperative (Missouri)	3	SERC
					Stephen Pogue	M and A Electric Power Cooperative	3	SERC
					William Price	M and A Electric Power Cooperative	1	SERC
					Peter Dawson	Sho-Me Power Electric Cooperative	1	SERC
					Mark Ramsey	N.W. Electric Power Cooperative, Inc.	1	NPCC
					John Stickley	NW Electric Power Cooperative, Inc.	3	SERC
					Tony Gott	KAMO Electric Cooperative	3	SERC
					Micah Breedlove	KAMO Electric Cooperative	1	SERC
					Kevin White	Northeast Missouri Electric Power Cooperative	1	SERC
					Skyler Wiegmann	Northeast Missouri Electric Power Cooperative	3	SERC
					Ryan Ziegler	Associated Electric Cooperative, Inc.	1	SERC
					Brian Ackermann	Associated Electric Cooperative, Inc.	6	SERC
					Brad Haralson	Associated Electric Cooperative, Inc.	5	SERC

1. The SDT has redefined Shared Cyber Infrastructure (SCI) such that it now focuses on cyber infrastructure that shares its hardware resources among VCAs of different impact levels only, which then subjects the SCI to additional requirements. Virtualization infrastructure that only hosts VCAs or associated VCAs of the same impact level is no longer SCI and requires no recategorization from current state. The SDT also removed the SCI identification changes from CIP-002. The SDT believes this greatly simplifies SCI. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

George Brown - Acciona Energy North America - 5

Answer No

Document Name

Comment

Acciona Energy supports Midwest Reliability Organization's (MRO) NERC Standards Review Forum's (NSRF) comments on this question.

Likes 0

Dislikes 0

Response

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

Answer No

Document Name

Comment

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

Likes 0

Dislikes 0

Response

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

Answer No

Document Name

Comment

Changes to the definitions have not provided clarity necessary. Diagrams that include examples as to how the definition correlates will be necessary if the redefined definition is not further clarified.

Likes 0

Dislikes 0

Response

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

Answer No

Document Name

Comment

We believe the inclusion of “Cyber Assets” in the second bullet expands the scope of applicability to include non virtual storage resources that are not currently subject to CIP requirements. This increase of in-scope Cyber Assets goes beyond the standards authorization request. We request “Cyber Assets” be deleted from the second bullet.

Likes 0

Dislikes 0

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer No

Document Name

Comment

Texas RE is concerned with the following statement: “Virtualization infrastructure that only hosts VCAs or associated VCAs of the same impact level is no longer SCI and requires no recategorization from current state” as it assumes industry consensus on how to categorize virtualization infrastructure, where consensus has not been reached.

Texas RE is concerned that the following scenario can still occur: virtualized BCAs or associated virtualized Cyber Assets of the same or associated impact level hosted on virtualization infrastructure where the Registered Entities categorized the virtualization infrastructure as BCAs, EACMS, PCAs, or non-CIP Cyber Assets.

To ensure that virtualization infrastructure that only hosts VCAs or associated VCAs of the same impact level is categorized and protected in a consistent manner, Texas RE recommends clear and concise language on the categorization and impact rating the hosting virtualization infrastructure should have. Specifically, Texas RE recommends virtualization infrastructure inherit the highest impact rating and categorizations of the VCAs that the virtualization infrastructure is hosting. For example, if virtualization infrastructure is hosting two high impact BCS, three PCAs associated with high impact BCS, and an EACMS associated with high impact BCS, then the virtualization infrastructure should be categorized as a high impact BCS. Implementing high watermarking practices could ensure that the virtualization infrastructure is more reliable and secure.

Likes 0

Dislikes 0

Response

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

Answer No

Document Name

Comment

CHPD believes that the proposed definition for Shared Cyber Infrastructure (SCI) does not meet the SDT's intent and instead increases the complexity of SCI by creating an extra test (does this SCI host multiple impact ratings?) and introducing significant compliance risk, where something as simple as a configuration change in a VCA (adding a new managed system to an EACMS for example) could inadvertently cause a virtual environment to become SCI. Additionally, if a VCA EACMS is associated with both High and Medium impact BCS, does that make its virtual infrastructure SCI?

CHPD suggests revising the definition of SCI to:

SCI - One or more electronic programmable devices, including the software that shares the devices' resources that:

- In a clustered configuration host one or more Virtual Cyber Assets that include one or more BES Cyber Systems or their associated Electronic Access Control Systems or Physical Access Control Systems.
- Provide storage resources required for system functionality of one or more BES Cyber Systems or their associated Electronic Access Control Systems or Physical Access Control Systems.
- SCI does not include the VCAs or Cyber Assets that utilizes its resources. An SCI supporting an EACMS or PACS is associated with the BES Cyber System the EACMS or PACS is associated with.

CHPD is of the opinion that SCI should be treated like it is an EACMS, except that it is also subject to the respective requirements of CIP-005 R1 and R2. The Applicable Systems column would then read as:

High Impact BES Cyber Systems and their associated:

- EACMS;
- PACS;
- PCA; or
- SCI

Likes 0

Dislikes 0

Response

Joseph Amato - Joseph Amato On Behalf of: Darnez Gresham, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Joseph Amato

Answer No

Document Name

Comment

We believe the inclusion of “Cyber Assets” in the second bullet expands the scope of applicability to include non virtual storage resources that are not currently subject to CIP requirements. This increase of in-scope Cyber Assets goes beyond the standards authorization request. We request “Cyber Assets” be deleted from the second bullet.

Likes 0

Dislikes 0

Response

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

Answer

No

Document Name

Comment

Reclamation recommends including Management Modules within the SCI definition.

Likes 0

Dislikes 0

Response

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

Answer

No

Document Name

Comment

- CIP-002 has always laid a foundation for CIP with an introduction including the term definitions. Consideration incorporating an introduction and clarification of CIP in CIP-002-7 for first time readers. CIP-002-7 should set the stage with a clear picture and foundation for the cyber asset life cycle.
- In CIP-002-7 Attachment 1 BROS needs the support of the definitions for Entity staff to have a complete process view. Including the definitions, diagrams and potential examples for the CIP is needed. Please introduce the definition and supporting details for the new terms impact cyber assets including function as BCS, BCA, PCA, EACMS, PACS and Form: SCI, MI, VCA, and CS. The form and function concept are addressed in CIP-005-7 and CIP-007-7 but should be referenced in CIP-002-7.

Proposed Definitions for incorporation in CIP-002-7:

- BES Cyber Asset (BCA)
- BES Cyber System (BCS)
- Cyber Assets (CA)

- Cyber System (CS)
- Electronic Access Control or Monitoring Systems (EACMS)
- Electronic Access Point (EAP)
- External Routable Connectivity (ERC)
- Electronic Security Perimeter (ESP)
- Interactive Remote Access (IRA)
- Intermediate System (IS)
- Management Interface (MI)
- Physical Access Control Systems
- (PACS)
- Physical Security Perimeter (PSP)
- Protected Cyber Asset (PCA)
- Shared Cyber Infrastructure (SCI)
- Virtual Cyber Asset (VCA)

Likes 0

Dislikes 0

Response

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

Answer

No

Document Name

Comment

The direction of the drafting team and new definition greatly simplify SCI. Further clarification is required in the definition for storage associated with SCI and for SCI that supports EACMS and PACS. With respect to the first bullet point, it is possible for SCI to exist outside of a clustered configuration, for example a standalone VMware ESXi system that hosts both a Medium Impact and Low Impact BCS. The clustered configuration wording can be removed to ensure this case is captured.

For SCI that hosts EACMS or PACS, the definition does not clearly identify if it would be acceptable to host VCA that are not in scope of NERC CIP compliance rather than being associated with BCS of a lower impact level. The following wording is suggested:

hosts one or more Virtual Cyber Assets (VCA) included in a BES Cyber Systems (BCS) or their associated Electronic Access Control or Monitoring Systems (EACMS) or Physical Access Control Systems (PACS); and hosts one or more VCAs that are not included in, or associated with, BCS OR BCS of the same impact categorization

With respect to the second bullet point, it does not completely define what is included in providing storage resources. For example, the following scenarios are not addressed:

If storage is implemented using a SAN, are the fibre channel switches included in SCI?

If storage is implemented using Network Attached Storage (NAS), are the network switches included in SCI?

If storage is located at a geographically different location than the Hypervisor, are Cyber Systems associated with communication networks and data communication links exempt from the definition of SCI. For example, for SCI supporting a VCA that is an EACMS, if a fiber connection goes through a DWDM device for multiplexing, is this device considered SCI since it is required for the VCA to function?

The following wording is proposed that limits the definition to the storage device only and leaves other components to be assessed using the existing criteria:

STORES DATA required for system functionality of one or more Cyber Assets or VCAs included in a BCS or their associated EACMS or PACS; and also for one or more Cyber Assets or VCAs that are not included in, or associated with, BCS OR BCS of the same impact categorization.

Likes 0

Dislikes 0

Response

Dwanique Spiller - Dwanique Spiller On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Berkshire Hathaway - NV Energy - 5 - WECC

Answer

No

Document Name

Comment

We believe the inclusion of "Cyber Assets" in the second bullet expands the scope of applicability to include non virtual storage resources that are not currently subject to CIP requirements. This increase of in-scope Cyber Assets goes beyond the standards authorization request. We request "Cyber Assets" be deleted from the second bullet.

Likes 0

Dislikes 0

Response

Donald Lock - Talen Generation, LLC - 5

Answer

No

Document Name

Comment

The sea change being attempted in NERC’s CIP definitions makes the success of the virtualization initiative highly dependent on clear communications, making significantly expanded explanations (with examples) appropriate, including clarifying that the new term, “Shared Cyber Infrastructure,” applies to hypervisors and not GO-TO communications systems.

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

Since Management Interface pertains to SCI, we request clarification of the combination of 1) the definition of Management Interface and 2) CIP-005 R1 Part 1.3 Requirement. That Requirement says, “Permit only needed routable protocol communications to and from Management Interfaces, and deny all other routable protocol communications, per system capability.” This combination implies new CIP-002 categorizations for assets with SCI and/or Management Interface. If this conclusion is not correct, please explain why this conclusion is incorrect. If this conclusion is correct, should CIP-002 explicitly state this Requirement?

Request clarification. Does the SDT intend CIP-008 Reportable Cyber Incident to include SCI but not PCA? Does the SDT intend that a SCI must have a PSP but not ESP? Does the SDT intend CIP-008 Reportable Cyber Incident include ESP but not PSP?

Request clarification. Does the SDT intend Low Impact to require more evidence (at the asset level) than BES Cyber Systems because of the addition of SCI (CIP-002 vs CIP-003)? SCI may require more granular evidence.

Request clarification of the combination of 1) the definition of Management Interface and 2) CIP-005 R1 Part 1.3 Requirement. That Requirement says, “Permit only needed routable protocol communications to and from Management Interfaces, and deny all other routable protocol communications, per system capability.” This combination implies new CIP-002 categorizations for assets with SCI and/or Management Interface. If this conclusion is not correct, please explain why this conclusion is incorrect. If this conclusion is correct, should CIP-002 explicitly state this Requirement?

Request clarification of CIP-007, Part 1.3. It appears that applications operating on a SCI platform where memory and CPU hardware devices are shared MUST all be classified at the same impact level. Is this a correct interpretation? If not, please explain. Memory and CPU are both implemented in hardware devices which are naturally shared across multiple processes and system functions. There is no known method to prevent the physical sharing of memory and CPU hardware devices in a virtual platform (SCI) based on the application and operating system processes that share these hardware devices.

Request clarification of CIP-007, Part 1.3 since there are two scenarios. In the first scenario there is one SCI for everything - BES Cyber Assets, PCAs, EACMS, PACS, potentially non-CIP VMs. In the second scenario there are two SCIs. The first SCI includes BES Cyber Assets and PCAs (within the ESP). The second SCI includes assets outside the ESP, like EACMS, PACS, potentially non-CIP VMs. These two SCIs do not have the same risk. Should we expect different Requirements for these two SCIs?

Likes 0

Dislikes 0

Response	
<p>Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh</p>	
Answer	No
Document Name	
Comment	
<p>NST believes the definition of “SCI” should not be limited to only hardware-based platforms hosting “mixed trust” virtual Cyber Assets (e.g., CIP and non-CIP, medium and low impact BCS). Proposed additional requirements for SCI, esp. those addressing control of logical access to management interfaces, should in our opinion apply to shared platforms regardless of whether they are hosting only one impact level of BCS and associated systems or supporting a mixed-trust computing environment. Given that the SDT’s proposed changes to CIP-002 through CIP-011 and CIP-013 would require nearly all Responsible Entities, including those with no virtualized environments, to revise most or all of their compliance documents, NST believes the additional effort to “reategorize” existing shared platforms would be acceptably small.</p> <p>NST opposes the SDT proposal to not compel Responsible Entities to identify and maintain a list of SCI that support BES Cyber Systems. In order to demonstrate compliance with various CIP-003 – CIP-013 requirements for SCI, a Responsible Entity would surely have to demonstrate that all its SCI were accounted for. NST is aware of the fact there is no existing CIP requirement to maintain an inventory of “associated” devices including PCAs, EACMS, and PACS, but doing so was some years ago memorably characterized by a well-known representative of a Regional Entity as an "implied requirement." NST believes an SDT goal should be to avoid adding to the list of "implied requirements."</p>	
Likes	0
Dislikes	0
Response	
<p>Carl Pineault - Hydro-Qu?bec Production - 5</p>	
Answer	No
Document Name	
Comment	
<p>Since Management Interface pertains to SCI, we request clarification of the combination of 1) the definition of Management Interface and 2) CIP-005 R1 Part 1.3 Requirement. That Requirement says, “Permit only needed routable protocol communications to and from Management Interfaces, and deny all other routable protocol communications, per system capability.” This combination implies new CIP-002 categorizations for assets with SCI and/or Management Interface. If this conclusion is not correct, please explain why this conclusion is incorrect. If this conclusion is correct, should CIP-002 explicitly state this Requirement?</p> <p>Request clarification. Does the SDT intend CIP-008 Reportable Cyber Incident to include SCI but not PCA? Does the SDT intend that a SCI must have a PSP but not ESP? Does the SDT intend CIP-008 Reportable Cyber Incident include ESP but not PSP?</p> <p>Request clarification. Does the SDT intend Low Impact to require more evidence (at the asset level) than BES Cyber Systems because of the addition of SCI (CIP-002 vs CIP-003)? SCI may require more granular evidence.</p> <p>Request clarification of the combination of 1) the definition of Management Interface and 2) CIP-005 R1 Part 1.3 Requirement. That Requirement says, “Permit only needed routable protocol communications to and from Management Interfaces, and deny all other routable protocol communications, per</p>	

system capability.” This combination implies new CIP-002 categorizations for assets with SCI and/or Management Interface. If this conclusion is not correct, please explain why this conclusion is incorrect. If this conclusion is correct, should CIP-002 explicitly state this Requirement?

Request clarification of CIP-007, Part 1.3. It appears that applications operating on a SCI platform where memory and CPU hardware devices are shared MUST all be classified at the same impact level. Is this a correct interpretation? If not, please explain. Memory and CPU are both implemented in hardware devices which are naturally shared across multiple processes and system functions. There is no known method to prevent the physical sharing of memory and CPU hardware devices in a virtual platform (SCI) based on the application and operating system processes that share these hardware devices.

Request clarification of CIP-007, Part 1.3 since there are two scenarios. In the first scenario there is one SCI for everything - BES Cyber Assets, PCAs, EACMS, PACS, potentially non-CIP VMs. In the second scenario there are two SCIs. The first SCI includes BES Cyber Assets and PCAs (within the ESP). The second SCI includes assets outside the ESP, like EACMS, PACS, potentially non-CIP VMs. These two SCIs do not have the same risk. Should we expect different Requirements for these two SCIs?

Likes 0

Dislikes 0

Response

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

Answer No

Document Name

Comment

Comments: Delete the phrase “Cyber Assets” from the second bullet point in the proposed definition. The inclusion of “Cyber Assets” in the second bullet as worded could expand the scope of applicability to include non virtual storage resources that are not currently subject to CIP requirements.

If a given cyber system implements computational workload sharing, but does not implement clustering, does it have to be categorized as SCI (“In a clustered configuration,...”)?

More clarification is needed with the distinction between a label (applicable system) and a transition process (non-dormant vs. dormant). Some definitions seem to incorporate aspects of both, which may lead to confusion with interpretation of the definition.

Lastly we would urge the use of diagrams to demonstrate concepts associated with the SCI definition and required aspects of the proposed modifications.

Likes 0

Dislikes 0

Response

Lindsey Mannion - ReliabilityFirst - 10

Answer No

Document Name

Comment

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

Introducing Shared Cyber Infrastructure (SCI) increases the number of Requirements and Parts that a Responsible Entity needs to track compared to simply identifying the hypervisor and associated hardware and “high-water marking” them with the highest identified impact rating BCA/VCA and creating a BCS. Attempting to segregate VM guests by their shared memory and CPU, or by using an undefined “clustered configuration,” increases the opportunity for misconfiguration should the underlying hypervisor move a VM Client to the wrong location or cluster member.

According to publications from the Cloud Security Alliance (see ***Best Practices for Mitigating Risks Virtual Environments April 2015 4-1-15_GLM5.pdf***), a risk factor unique to virtual environments is the hypervisor. Hypervisor is the software and/or firmware responsible for hosting and managing VMs. It provides a single point of access into the virtual environment and is also potentially a single point of failure. A misconfigured hypervisor can result in a single point of compromise of the security of all its hosted components. It does not matter how individual VMs are hardened—a compromised hypervisor can override those controls and provide a convenient single point of unauthorized access to all the VMs. Since all SCI is controlled by the hypervisor, all hypervisors should be high-water marked with any associated level of impact of the VM guests (VCAs) that are identified.

Likes 0

Dislikes 0

Response

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name SPP RTO

Answer

No

Document Name

Comment

SPP appreciates the time and resources the SDT has expended to provide Draft 3 of the virtualization standards. This is not an easy lift. SPP is supportive of the overall approach and structure of the proposed standards. SPP does have concerns with the interpretation of new definitions; and can support with a few clarifications, as described below.

SPP is concerned with how to interpret the definition of Shared Cyber Infrastructure (SCI) and would appreciate clarification by the SDT. First, is clustering included in the definition of SCI. If an entity does not use or implement clustering in its definition, it is still classified as a SCI or would it be a Cyber Asset?

Additionally, of the definition of Virtual Cyber Asset(VCA) describes a “non-dormant logical instance.” What does the SDT mean by non-dormant in regards to a VCA? If a virtual machine is not in use, would that be classified as dormant and then once it is needed it becomes a VCA? Would a Golden Image be classified as dormant? Is the term “non-dormant” a permanent state? To help with interpretation, SPP would appreciate the SDT providing examples of what is meant by “Non-Dormant.”

Likes 0

Dislikes 0

Response

Maggy Powell - Amazon Web Services - 7

Answer No

Document Name

Comment

AWS supports the SCI definition that focuses on cyber infrastructure that shares its hardware resources among VCAs of different impact levels only, which then subjects the SCI to additional requirements to address different cyber security concerns. However, removing SCI from CIP-002 may lead Entities to miss the need to identify, track and apply controls to SCI.

Likes 0

Dislikes 0

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer No

Document Name

Comment

IESO supports the comments provided by NPCC and IRC.

Likes 0

Dislikes 0

Response

Thomas Breene - WEC Energy Group, Inc. - 3

Answer No

Document Name

Comment

The use of the term "Cyber Asset" in the 2nd bullet of the SCI definition differs from the intent of a "shared virtual machine" environment. A Cyber Asset is a single programmable electronic device and hence would not reside on a Shared Cyber Infrastructure.

By including the reference to Cyber Asset in this definition could potentially bring additional non virtual storage resources into scope.

Likes 0

Dislikes 0

Response

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

Answer No

Document Name

Comment

Since Management Interface pertains to SCI, we request clarification of the combination of 1) the definition of Management Interface and 2) CIP-005 R1 Part 1.3 Requirement. That Requirement says, "Permit only needed routable protocol communications to and from Management Interfaces, and deny all other routable protocol communications, per system capability." This combination implies new CIP-002 categorizations for assets with SCI and/or Management Interface. If this conclusion is not correct, please explain why this conclusion is incorrect. If this conclusion is correct, should CIP-002 explicitly state this Requirement?

Request clarification. Does the SDT intend CIP-008 Reportable Cyber Incident to include SCI but not PCA? Does the SDT intend that an SCI must have a PSP but not ESP? Does the SDT intend for CIP-008 Reportable Cyber Incident to include ESP but not PSP?

Request clarification. Does the SDT intend Low Impact to require more evidence (at the asset level) than BES Cyber Systems because of the addition of SCI (CIP-002 vs CIP-003)? SCI may require more granular evidence.

Request clarification of the combination of 1) the definition of Management Interface and 2) CIP-005 R1 Part 1.3 Requirement. That Requirement says, "Permit only needed routable protocol communications to and from Management Interfaces, and deny all other routable protocol communications, per system capability." This combination implies new CIP-002 categorizations for assets with SCI and/or Management Interface. If this conclusion is not correct, please explain why this conclusion is incorrect. If this conclusion is correct, should CIP-002 explicitly state this Requirement?

Request clarification of CIP-007, Part 1.3. It appears that applications operating on an SCI platform where memory and CPU hardware devices are shared MUST all be classified at the same impact level. Is this a correct interpretation? If not, please explain. Memory and CPU are both implemented in hardware devices which are naturally shared across multiple processes and system functions. There is no known method to prevent the physical sharing of memory and CPU hardware devices in a virtual platform (SCI) based on the application and operating system processes that share these hardware devices.

Request clarification of CIP-007, Part 1.3 since there are two scenarios. In the first scenario, there is one SCI for everything - BES Cyber Assets, PCAs, EACMS, PACS, and potentially non-CIP VMs. In the second scenario, there are two SCIs. The first SCI includes BES Cyber Assets and PCAs (within the ESP). The second SCI includes assets outside the ESP, like EACMS, PACS, and potentially non-CIP VMs. These two SCIs do not have the same risk. Should we expect different Requirements for these two SCIs?

Likes 1 Orlando Utilities Commission, 5, Colon Dania

Dislikes 0

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1

Answer No

Document Name

Comment

We support NPCC TFIST's comments. Since Management Interface pertains to SCI, we request clarification of the combination of 1) the definition of Management Interface and 2) CIP-005 R1 Part 1.3 Requirement. That Requirement says, "Permit only needed routable protocol communications to and

from Management Interfaces, and deny all other routable protocol communications, per system capability.” This combination implies new CIP-002 categorizations for assets with SCI and/or Management Interface. If this conclusion is not correct, please explain why this conclusion is incorrect. If this conclusion is correct, should CIP-002 explicitly state this Requirement?

Request clarification. Does the SDT intend CIP-008 Reportable Cyber Incident to include SCI but not PCA? Does the SDT intend that a SCI must have a PSP but not ESP? Does the SDT intend CIP-008 Reportable Cyber Incident include ESP but not PSP?

Request clarification. Does the SDT intend Low Impact to require more evidence (at the asset level) than BES Cyber Systems because of the addition of SCI (CIP-002 vs CIP-003)? SCI may require more granular evidence.

Request clarification of the combination of 1) the definition of Management Interface and 2) CIP-005 R1 Part 1.3 Requirement. That Requirement says, “Permit only needed routable protocol communications to and from Management Interfaces, and deny all other routable protocol communications, per system capability.” This combination implies new CIP-002 categorizations for assets with SCI and/or Management Interface. If this conclusion is not correct, please explain why this conclusion is incorrect. If this conclusion is correct, should CIP-002 explicitly state this Requirement?

Request clarification of CIP-007, Part 1.3. It appears that applications operating on a SCI platform where memory and CPU hardware devices are shared MUST all be classified at the same impact level. Is this a correct interpretation? If not, please explain. Memory and CPU are both implemented in hardware devices which are naturally shared across multiple processes and system functions. There is no known method to prevent the physical sharing of memory and CPU hardware devices in a virtual platform (SCI) based on the application and operating system processes that share these hardware devices.

Request clarification of CIP-007, Part 1.3 since there are two scenarios. In the first scenario there is one SCI for everything - BES Cyber Assets, PCAs, EACMS, PACS, potentially non-CIP VMs. In the second scenario there are two SCIs. The first SCI includes BES Cyber Assets and PCAs (within the ESP). The second SCI includes assets outside the ESP, like EACMS, PACS, potentially non-CIP VMs. These two SCIs do not have the same risk. Should we expect different Requirements for these two SCIs?

Likes 0

Dislikes 0

Response

David Jendras - Ameren - Ameren Services - 3

Answer

No

Document Name

Comment

Definition of SCI should be consistent regardless of impact rating.

Likes 0

Dislikes 0

Response

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6

Answer

No

Document Name	
Comment	
We believe the inclusion of “Cyber Assets” in the second bullet expands the scope of applicability to include non virtual storage resources that are not currently subject to CIP requirements. This increase of in-scope Cyber Assets goes beyond the standards authorization request. We request “Cyber Assets” be deleted from the second bullet.	
Likes	0
Dislikes	0
Response	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC) 2016-02 Virtualization (Draft 3)	
Answer	No
Document Name	
Comment	
<p><i>The SRC agrees with the concept of Shared Cyber Infrastructure (SCI) but does not agree with the proposed wholesale re-write of large parts of existing CIP standards to accommodate the SCI. The proposed changes to existing standards would lead to re-interpretation and change in interpretation of currently effective requirements. This approach also puts a significant operational and financial burden on entities necessitating key program changes and re-investment in CIP tools and protections. The SRC recommends the drafting team consider simpler, lower-impact implementation guidance updates to address SCI which would be applicable to existing CIP requirements.</i></p> <p><i>The SRC notes that the SCI definition seems to incorporate assumptions about the architecture and implementation of virtualization management systems. For this reason, the SRC recommends the use of diagrams within the implementation guidance to demonstrate concepts associated with the SCI definition and required aspects of the applicable standards.</i></p> <p><i>The SRC also notes that further clarification is needed in the following areas which SRC recommends be outlined in the implementation guidance:</i></p> <ul style="list-style-type: none"> - <i>There is distinction between a label (applicable system) and a transition process (non-dormant vs. dormant). However, SRC notes that some definitions seem to incorporate aspects of both, which may lead to confusion with interpretation of the definition.</i> <p><i>When a cyber-system implements computational workload sharing but does not implement clustering guidance to help the entities determine whether the system meets the categorization of SCI (e.g., “In a clustered configuration,...”).</i></p>	
Likes	0
Dislikes	0
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	No
Document Name	

Comment

Alliant Energy supports the comments submitted by the MRO NSRF.

Likes 0

Dislikes 0

Response

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

Answer

No

Document Name

Comment

Likes 0

Dislikes 0

Response

Joni Jones - Wabash Valley Power Association - 1

Answer

Yes

Document Name

Comment

Acceptable but convoluted definition. However, does this effectively pull in the current implementation of software defined networking?

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

SRP would like more clarification on the SCI definition and how it relates CIP-007 R1.3, this seems like a contradiction.

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

AZPS agrees with the redefined Share Cyber Infrastructure (SCI) definition.

Likes 0

Dislikes 0

Response

Ellese Murphy - Duke Energy - 1,3,5,6 - SERC,RF

Answer Yes

Document Name

Comment

We agree that the new Shared Cyber Infrastructure definition is much clearer.

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

CenterPoint Energy Houston Electric, LLC (CEHE) agrees with the proposed SCI definition.

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Although we agree with the proposed change, it is not explicitly clear that a hypervisor environment hosting VCAs must be categorized as a BCA, EACMS, etc. To avoid confusion the definition for SCI could state that a hypervisor environment hosting virtual cyber assets of the same classification must be categorized as the same type of cyber asset

Likes 0

Dislikes 0

Response

JT Kuehne - AEP - 6

Answer Yes

Document Name

Comment

AEP supports the proposed changes made to the definition of SCI.

Likes 0

Dislikes 0

Response

patricia ireland - DTE Energy - 4

Answer Yes

Document Name

Comment

Patty Ireland on behalf of DTE Energy, Segments 3 and 4

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 to the SCI definition.

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

EEl supports the proposed changes made to the definition of SCI noting the language has been streamlined.

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

SMUD agrees with these changes.

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

We feel the definition greatly simplifies applicable SCI, but we feel prior to the implementation, the concepts associated with the SCI definition and other aspects of the proposed modifications be illustrated to aid in meeting strict compliance. Obviously the modifications have been a moving target, so implementation guidance is on the back burner. Compliance guidance is necessary before the implementation plan starts.

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

We support NPCC RSC's comments.

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

ITC supports the comments submitted by EEI

Likes 0

Dislikes 0

Response

Kimberly Turco - Constellation - 6**Answer** Yes**Document Name****Comment**

Constellation has elected to align with Exelon in response to this question.

Kim Turco, on behalf of Constellation Segments 5 and 6

Likes 0

Dislikes 0

Response**Alison Mackellar - Constellation - 5****Answer** Yes**Document Name****Comment**

Constellation has elected to align with Exelon in response to this question.

Kim Turco, on behalf of Constellation Segments 5 and 6

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 Hirschak, 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**

See EEI comment.

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

AEPCO is signing on to ACES comments below.

ACES Comments: We feel the definition greatly simplifies applicable SCI, but we feel prior to the implementation, the concepts associated with the SCI definition and other aspects of the proposed modifications be illustrated to aid in meeting strict compliance. Obviously the modifications have been a moving target, so implementation guidance is on the back burner. Compliance guidance is necessary before the implementation plan starts.

Likes 0

Dislikes 0

Response

Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,5 - RF

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Mike Marshall - IDACORP - Idaho Power Company - 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

Ryan Strom - Buckeye Power, Inc. - 5

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Josh Johnson - Lincoln Electric System - 1

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Bryan Koyle - Southern Indiana Gas and Electric Co. - 3,5,6 - RF

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Hien Ho - Tacoma Public Utilities (Tacoma, WA) - 4

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Jennifer Malon - Jennifer Malon On Behalf of: Brooke Voorhees, Black Hills Corporation, 3, 5, 1, 6; Derek Silbaugh, Black Hills Corporation, 3, 5, 1, 6; Don Stahl, Black Hills Corporation, 3, 5, 1, 6; Seth Nelson, Black Hills Corporation, 3, 5, 1, 6; - Jennifer Malon

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

William Steiner - Midwest Reliability Organization - 10

Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0

Response

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

Answer	Yes
Document Name	
Comment	

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Glen Farmer - Avista - Avista Corporation - 5

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Jesus Sammy Alcaraz - Imperial Irrigation District - 1

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

James Baldwin - Lower Colorado River Authority - 1

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

John Merrell - Tacoma Public Utilities (Tacoma, WA) - 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

Justin MacDonald - Midwest Energy, Inc. - 1

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

Scott Kinney - Avista - Avista Corporation - 3**Answer** Yes**Document Name****Comment**

Likes 0

Dislikes 0

Response**Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones****Answer** Yes**Document Name** [2016-02_CIP_Virtualization_DRAFT_3 Unofficial_Comment_Form_02182022-WAPA.docx](#)**Comment**

Likes 0

Dislikes 0

Response**Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC****Answer****Document Name****Comment**

Xcel Energy supports the comments previously filed by the MRO NSRF and EEI.

Likes 0

Dislikes 0

Response**Daniel Gacek - Exelon - 1****Answer****Document Name****Comment**

Exelon will align with EEI in response to this question.

Likes 0

Dislikes 0

Response

Kinte Whitehead - Exelon - 3

Answer

Document Name

Comment

Exelon will align with EEI in response to this question.

Likes 0

Dislikes 0

Response

2. The SDT has reinstated the currently approved ESP definition and appended language to allow for zero trust models. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal. Please also include any comments on the proposed EAP definition in the response to this question.

Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC) 2016-02 Virtualization (Draft 3)

Answer No

Document Name

Comment

The SRC agrees with the reinstatement of currently approved ESP definition but notes that the EAP definition appears to focus on control of traffic to/from a single BCS and recommends the definition to state "one or more BCS" instead of "a BCS." The SRC also recommends that host-based firewalls not be considered in scope of the EAP definition. Additionally, the SRC recommends further clarification be provided regarding EAP definition in the following areas:

- *Does the EAP apply to host-based firewalls?*
- *Would each host firewall be a single EAP?*
- *Could an entity identify all such host-based firewalls as an EAP in a group?*

Likes 0

Dislikes 0

Response

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name SPP RTO

Answer No

Document Name

Comment

SPP would like the clarification whether the EAP definition applies to host-based firewalls? Would each host firewall be a single EAP? Could an entity identify all such host-based firewalls as an EAP in a group?

Likes 0

Dislikes 0

Response

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

Answer No

Document Name

Comment

Zero trust does not appear to be included in the revised definition. Please provide more clarification for the added language and its application to zero trust.

Likes 0

Dislikes 0

Response**Lindsey Mannion - ReliabilityFirst - 10**

Answer

No

Document Name

Comment

The new Electronic Security Perimeter (ESP) definition further complicates the situation with respect to mixed-trust environments where a Responsible Entity may choose to create ESPs (Electronic Access Points) for a single Cyber Asset (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 via the virtual networking, firewall, and policies required to segregate VM guests. Virtual environments still require hypervisor overview for controlling VM guests as well as implementing policies for sizing, network access, and complete lifecycle of the VM guest. Removal of the ESP not only creates a more complex environment by randomly determining where CIP BCS resides within the corporation, it removes the concept of defense-in-depth that is afforded by limiting outside access into these identified BCS through a limited number of points on the ESP.

Marrying both ESP and zero-trust within an overall ESP would better serve our Responsible Entities and create a more secure environment as zero-trust Cyber Assets would not be internet-facing while simplifying the management of the environment. Maintaining the ESP, and fully incorporating virtualization and zero trust paradigms within an identified ESP allows Responsible Entities to leverage another layer of defense for BCS by limiting ingress/egress points and access to these Cyber Assets.

Likes 0

Dislikes 0

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

Answer

No

Document Name

Comment

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.

NST believes the proposed definition of EAP (“An electronic policy enforcement point or a Cyber Asset interface that controls routable communication to

and from a BES Cyber System”) 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 another Cyber Asset, regardless of whether that device is within or outside of an ESP protecting the BCS. Second, by saying an EAP can be "a Cyber Asset interface" without qualification, the definition could be interpreted to allow for the use of host-based firewalls on BES Cyber Assets and BES Cyber Systems, something the previous set of proposed modifications to CIP-005 expressly prohibited for CIP-005. NST suggests making only minor changes to the well-understood existing definition of EAP, such as: "An electronic policy enforcement point or a Cyber Asset interface on an Electronic Security Perimeter that controls routable communication between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter."

Likes 0

Dislikes 0

Response

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

Answer

No

Document Name

Comment

This definition is very broad and could be considered to include every interface on every asset inside the ESP as well (even in a non-zero trust model) which is used to communicate with each other. This would complicate maintaining the "ESP". The language around communications between assets outside the ESP to assets inside the ESP, and vice-versa, needs to be kept.

Likes 0

Dislikes 0

Response

JT Kuehne - AEP - 6

Answer

No

Document Name

Comment

AEP does not support the proposed changes made to the definition of ESP. The SDT added "; or a logical boundary defined by one of more EAPs" to the definition of ESP. With this addition, ESP now exclusively requires the use of EAPs and conflicts with the measures in CIP-005-7 R1.2 where an EAP is one of many options to restrict inbound and outbound communications. AEP recommend reverting to the existing ESP definition.

Likes 0

Dislikes 0

Response

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

Answer	No
Document Name	
Comment	
<p>The definition of ESP is overly redundant and is not cohesive with the definition of EAP. It does not seem necessary to state that ESPs can be a border defined by EAPs, as that this is already handled by the definition of EAP. It also fails to include PCAs in the definition, which is now required given that VCAs that share CPU/memory with a BCA become PCAs even if they do not share network space, and it does not establish ESPs for non-routable devices, which is now needed with the new IRA protections. CHPD suggests revising the definition of ESP and EAP to:</p> <p>ESP - A logical boundary surrounding one or more BES Cyber Systems or Protected Cyber Assets.</p> <p>EAP - An electronic policy enforcement point or Cyber Asset interface that controls routable communication through the ESP.</p>	
Likes	0
Dislikes	0
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	No
Document Name	
Comment	
<p>Texas RE agrees with the proposed definition of ESP.</p> <p>Texas RE recommends the EAP definition be revised to include “or PCA” after “from a BES Cyber System”. The definition as currently written states that the EAP controls routable communication to and from a BES Cyber System. PCAs are also required to be protected by an ESP, however if a PCA is directly connected to a firewall then that interface would not be considered an EAP, as it does not control routable communication to and from a BCS.</p>	
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 Hirschak, 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	

See EEI comment.

Likes 0

Dislikes 0

Response

Alison Mackellar - Constellation - 5

Answer

Yes

Document Name

Comment

Constellation has elected to align with Exelon in response to this question.

Kim Turco, on behalf of Constellation Segments 5 and 6

Likes 0

Dislikes 0

Response

Kimberly Turco - Constellation - 6

Answer

Yes

Document Name

Comment

Constellation has elected to align with Exelon in response to this question.

Kim Turco, on behalf of Constellation Segments 5 and 6

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 comments submitted by EEI	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
We support NPCC RSC's comments.	
Additionally, the definition of EAP may be interpreted to include Cyber Assets that convert routable communicatoin to non-routable. Would the port on a serial to IP converter (that meets the CA defintion) meet the definition of EAP? If it does than a BCA that is communicating serial to the converter could be outside of the ESP. The serial to IP converter would be an EACMS?	
Would the serial or TCP/IP ports on a RTU that communicates to BCAs (protection system relays) using a routable protocol but to the outside word using a non-routable protocol be an EAP and make the RTU an EACMS? If the TCP/IP ports are are EAPs than the RTU is outside the ESP	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI supports the reinstatement of ESPs and agrees with the change made to allow zero trust models.	
Likes 0	
Dislikes 0	
Response	

Nicolas Turcotte - Hydro-Quebec TransEnergie - 1

Answer Yes

Document Name

Comment

We support the NPCC TFIST comments. We support the ESP and EAP modifications.

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

We support the ESP and EAP modifications.

Likes 0

Dislikes 0

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer Yes

Document Name

Comment

IESO supports the comments provided by NPCC and IRC

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 reinstatement of ESPs and the appended language to allow for zero trust models.	
Likes 0	
Dislikes 0	
Response	
Maggy Powell - Amazon Web Services - 7	
Answer	Yes
Document Name	
Comment	
AWS supports the SDT's proposal to reinstate the currently approved ESP definition and appended language to allow for zero trust models. The language allows Entities to adopt a defense-in-depth approach that leverages both traditional perimeter-based security and zero-trust concepts.	
AWS suggests that the SDT develops detailed implementation guidance that supports traditional perimeter-based security, zero-trust and hybrid approaches, including defining the term zero-trust and/or directing Entities to reference NIST Special Publication 800-207 on the topic for additional clarity.	
Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	Yes
Document Name	
Comment	
We support the ESP and EAP modifications	
Likes 0	
Dislikes 0	
Response	

patricia ireland - DTE Energy - 4	
Answer	Yes
Document Name	
Comment	
Patty Ireland on behalf of DTE Energy, Segments 3 and 4	
Likes 1	Orlando Utilities Commission, 5, Colon Dania
Dislikes 0	
Response	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	Yes
Document Name	
Comment	
We support the ESP and EAP modifications.	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
CEHE agrees with the proposed ESP definition.	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - SERC,RF	
Answer	Yes

Document Name	
Comment	
We agree with the proposed changes to the ESP definition.	
Likes 0	
Dislikes 0	
Response	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
AZPS agrees with the proposed changes/reinstatement of the ESP and EAP definitions.	
Likes 0	
Dislikes 0	
Response	
Justin Welty - NextEra Energy - Florida Power and Light Co. - 6	
Answer	Yes
Document Name	
Comment	
Please include the applicable definitions in CIP-002-7, CIP-005-7, CIP-007-7, and CIP-010-5 for orientation especially for those new to NERC CIP.	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	

Returning to the original ESP definition resolves the concerns that BPA previously had with the definition change.

Likes 0

Dislikes 0

Response

George Brown - Acciona Energy North America - 5

Answer

Yes

Document Name

Comment

Acciona Energy supports Midwest Reliability Organization's (MRO) NERC Standards Review Forum's (NSRF) comments on this question.

Likes 0

Dislikes 0

Response

Joni Jones - Wabash Valley Power Association - 1

Answer

Yes

Document Name

Comment

Need to ensure an extremely clear understanding by the industry for the revised definitions of ESP and EAP to ensure that the level of security is not reduced. This will require a common understanding across both industry and auditors for effective implementation that will not be easy to achieve. Further, by allowing the each individual end device to be the logical access point, the language essentially allows an entity to compliantly just run a well configured copy of Windows Firewall as their only EAP control. Not sure if that is the intent.

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

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

Scott Kinney - Avista - Avista Corporation - 3

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

Justin MacDonald - Midwest Energy, Inc. - 1

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

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

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

James Baldwin - Lower Colorado River Authority - 1

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

David Jendras - Ameren - Ameren Services - 3

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Jesus Sammy Alcaraz - Imperial Irrigation District - 1

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Glen Farmer - Avista - Avista Corporation - 5

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Thomas Breene - WEC Energy Group, Inc. - 3

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

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

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

William Steiner - Midwest Reliability Organization - 10

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Jennifer Malon - Jennifer Malon On Behalf of: Brooke Voorhees, Black Hills Corporation, 3, 5, 1, 6; Derek Silbaugh, Black Hills Corporation, 3, 5, 1, 6; Don Stahl, Black Hills Corporation, 3, 5, 1, 6; Seth Nelson, Black Hills Corporation, 3, 5, 1, 6; - Jennifer Malon

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Hien Ho - Tacoma Public Utilities (Tacoma, WA) - 4

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Donald Lock - Talen Generation, LLC - 5

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Dwanique Spiller - Dwanique Spiller On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Berkshire Hathaway - NV Energy - 5 - WECC

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response**Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter****Answer**

Yes

Document Name**Comment**

Likes 0

Dislikes 0

Response**Bryan Koyle - Southern Indiana Gas and Electric Co. - 3,5,6 - RF****Answer**

Yes

Document Name**Comment**

Likes 0

Dislikes 0

Response**Josh Johnson - Lincoln Electric System - 1****Answer**

Yes

Document Name**Comment**

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Joseph Amato - Joseph Amato On Behalf of: Darnez Gresham, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Joseph Amato

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Ryan Strom - Buckeye Power, Inc. - 5

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Mike Marshall - IDACORP - Idaho Power Company - 1

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

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

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Patricia Lynch - NRG - NRG Energy, 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

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

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon will align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	

Exelon will align with EEI in response to this question.

Likes 0

Dislikes 0

Response

3. The SDT modified the ERC definition from the “outside the asset containing” reference point in the previous draft back to an ESP reference point. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

Joni Jones - Wabash Valley Power Association - 1

Answer No

Document Name

Comment

Language needs to say EAP, not ESP. An EAP is the policy enforcement point or interface, not the ESP.

Likes 0

Dislikes 0

Response

Mike Marshall - IDACORP - Idaho Power Company - 1

Answer No

Document Name

Comment

Idaho Power believes the previous definition provided more clarity.

Likes 0

Dislikes 0

Response

JT Kuehne - AEP - 6

Answer No

Document Name

Comment

AEP does not support the proposed changes made to the definition of External Routable Connectivity (ERC) and recommends that ERC should maintain its existing definition. AEP further recommends the SDT to create a new term to address the need for the zero-trust model. The word “External” in “External Routable Connectivity” is defined in the existing definition as “outside of its associated ESP”, while the proposed definition of ERC uses “**through** its ESP”.

Likes 0

Dislikes 0

Response

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

Answer

No

Document Name

Comment

NST believes the use of the word, "through (an ESP)" has the potential to cause confusion over what kind of routable communications qualify as ERC. ERC to or from a Cyber Asset should be clearly defined as "through" an ESP boundary or access point, not "through" an ESP (the online Merriam Webster dictionary defines "through" as "a function word to indicate movement into at one side or point and out at another and especially the opposite side of // 'drove a nail through the board"). NST believes the existing definition of ERC can and should be retained as-is.

Likes 0

Dislikes 0

Response

Lindsey Mannion - ReliabilityFirst - 10

Answer

No

Document Name

Comment

Removing “outside the asset containing” and identifying the ESP as the boundary where electronic access is required is welcomed. However, specifically identifying EAPs as an ESP in the new definition could potentially create confusion. Further, with no NERC definition for “electronic policy enforcement point” there may be a question as to what constitutes this “enforcement point.” In addition, the “logical boundary defined by one or more EAPs” may inadvertently allow access if an EAP was not correctly identified and configured. Since zero trust is a strategic approach and there is no formal definition, Responsible Entities can create their own definition of what zero trust represents, which creates potential monitoring issues and would require additional Practice and Implementation Guides to find common ground. Modification to the ESP definition to include individual BCS (BCA/VCA via a host firewall or other application) would be preferable, as in most cases the ESP must be identified before an EAP can be. In other words, a zero trust Cyber Asset would have both an identified ESP and an associated EAP allowing access to the Cyber Asset.

Likes 0

Dislikes 0

Response

George Brown - Acciona Energy North America - 5

Answer

Yes

Document Name

Comment

Acciona Energy supports Midwest Reliability Organization's (MRO) NERC Standards Review Forum's (NSRF) comments on this question.

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

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

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

Please include the applicable definitions in CIP-002-7, CIP-005-7, CIP-007-7, and CIP-010-5 for orientation especially for those new to NERC CIP

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

AZPS agrees with the proposed modifications to the ERC definition.

Likes 0

Dislikes 0

Response

Ellese Murphy - Duke Energy - 1,3,5,6 - SERC,RF

Answer Yes

Document Name

Comment

Yes, this language is much clearer. Now that the ESP definition has been revised, it makes sense to point back to the ESP as a reference point.

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

CEHE agrees with the proposed ERC definition.

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

No comment

Likes 0

Dislikes 0

Response

patricia ireland - DTE Energy - 4

Answer Yes

Document Name

Comment

Patty Ireland on behalf of DTE Energy, Segments 3 and 4

Likes 1 Orlando Utilities Commission, 5, Colon Dania

Dislikes 0

Response

Carl Pineault - Hydro-Qu?bec Production - 5

Answer Yes

Document Name

Comment

No comment

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Comments: We request more clarification regarding whether traffic between ESPs would be included in the category of ERC, as this may impact interpretation of such traffic as involved with IRA.

Likes 0

Dislikes 0

Response

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name SPP RTO

Answer Yes

Document Name

Comment

SPP agrees with the proposed change of the ERC definition and recommends further clarification be provided to help entities determine if traffic between ESPs would be included in the category of ERC. This may impact interpretation of such traffic as involved with IRA.

Likes 0

Dislikes 0

Response

Maggy Powell - Amazon Web Services - 7

Answer Yes

Document Name

Comment

N/A

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Southern supports the modified ERC definition back to the ESP reference point.

Likes 0

Dislikes 0

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer Yes

Document Name	
Comment	
No comment	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
The revised definition is clear and aligns with the current definition of ERC.	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
We support NPCC RSC's comments.	
Likes 0	
Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC) 2016-02 Virtualization (Draft 3)	
Answer	Yes
Document Name	
Comment	

The SRC agrees with the proposed change of the ERC definition and recommends further clarification be provided to help entities determine if traffic between ESPs would be included in the category of ERC. This may impact interpretation of such traffic as involved with IRA.

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 comments submitted by EEI

Likes 0

Dislikes 0

Response

Kimberly Turco - Constellation - 6

Answer

Yes

Document Name

Comment

Constellation has elected to align with Exelon in response to this question.

Kim Turco, on behalf of Constellation Segments 5 and 6

Likes 0

Dislikes 0

Response

Alison Mackellar - Constellation - 5

Answer

Yes

Document Name

Comment

Constellation has elected to align with Exelon in response to this question.

Kim Turco, on behalf of Constellation Segments 5 and 6

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

See EEI comment.

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

Alliant Energy supports the comments submitted by the MRO NSRF.

Likes 0

Dislikes 0

Response

Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,5 - RF

Answer

Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC Entity Monitoring	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0

Response	
Israel Perez - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0

Response	
Chris Wagner - Santee Cooper - 1,3,5,6, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0

Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	Yes
Document Name	

Comment

Likes 0

Dislikes 0

Response**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**Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1****Answer**

Yes

Document Name**Comment**

Likes 0

Dislikes 0

Response

Ryan Strom - Buckeye Power, Inc. - 5

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy 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

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Joseph Amato - Joseph Amato On Behalf of: Darnez Gresham, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Joseph Amato

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

Josh Johnson - Lincoln Electric System - 1

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Bryan Koyle - Southern Indiana Gas and Electric Co. - 3,5,6 - RF

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Dwanique Spiller - Dwanique Spiller On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Berkshire Hathaway - NV Energy - 5 - WECC

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Donald Lock - Talen Generation, LLC - 5

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Hien Ho - Tacoma Public Utilities (Tacoma, WA) - 4

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Jennifer Malon - Jennifer Malon On Behalf of: Brooke Voorhees, Black Hills Corporation, 3, 5, 1, 6; Derek Silbaugh, Black Hills Corporation, 3, 5, 1, 6; Don Stahl, Black Hills Corporation, 3, 5, 1, 6; Seth Nelson, Black Hills Corporation, 3, 5, 1, 6; - Jennifer Malon

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

William Steiner - Midwest Reliability Organization - 10

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Thomas Breene - WEC Energy Group, Inc. - 3

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Glen Farmer - Avista - Avista Corporation - 5

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Jesus Sammy Alcaraz - Imperial Irrigation District - 1

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

David Jendras - Ameren - Ameren Services - 3

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

James Baldwin - Lower Colorado River Authority - 1

Answer	Yes
---------------	-----

Document Name	
----------------------	--

Comment	
----------------	--

Likes	0
-------	---

Dislikes	0
----------	---

Response	
-----------------	--

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

Answer	Yes
---------------	-----

Document Name	
----------------------	--

Comment	
----------------	--

Likes	0
-------	---

Dislikes	0
----------	---

Response	
-----------------	--

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6

Answer	Yes
---------------	-----

Document Name	
----------------------	--

Comment	
----------------	--

Likes	0
-------	---

Dislikes	0
----------	---

Response	
-----------------	--

John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1

Answer	Yes
---------------	-----

Document Name	
----------------------	--

Comment	
----------------	--

Likes 0

Dislikes 0

Response

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

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

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Justin MacDonald - Midwest Energy, Inc. - 1

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

LaTroy Brumfield - American Transmission Company, LLC - 1

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Scott Kinney - Avista - Avista Corporation - 3

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

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

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Daniel Gacek - Exelon - 1

Answer

Document Name

Comment

Exelon will align with EEI in response to this question.

Likes 0

Dislikes 0

Response

Kinte Whitehead - Exelon - 3

Answer

Document Name

Comment

Exelon will align with EEI in response to this question.

Likes 0

Dislikes 0

Response

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

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

Answer No

Document Name

Comment

Recommend the following definition:

User-initiated access by a person using a Cyber Asset or VCA, not protected by any of the Responsible Entity's Electronic Security Perimeter(s) (ESP) and using a routable protocol To a Cyber System protected by an ESP.

Remove the following language: "That is converted to a non-routable protocol to a Cyber System not protected by an ESP; or To a Management Interface of Shared Cyber Infrastructure."

A management interface on a Shared cyber asset should reside within the registered entities ESP.

Assets that provide Serial conversion to downstream BES Cyber assets do not communicate to those assets using a routable communication protocol and should not be included in the definition of IRA.

In the proposed revised definition of Interactive Remote Access, the existing phrase "that is not an Intermediate System" would be removed. We are concerned that there is a possibility that an Intermediate System would be considered a Cyber Asset or VCA, not protected by any of the Responsible Entity's Electronic Security Perimeters, resulting in a "hall of mirrors" issue under CIP-005 R2.1. Accordingly we recommend either the phrase "that is not an Intermediate System" or the SDT provide clarity on how the proposed definition avoids compliance issues for Intermediate Systems vis-à-vis CIP-005 R2.1.

Likes 0

Dislikes 0

Response

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

Answer No

Document Name

Comment

Alliant Energy supports the comments submitted by the MRO NSRF.

Likes 0

Dislikes 0

Response

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

Answer No

Document Name

Comment

AEPCO is signing on to ACES comments below.

ACES Comments: The updated definition of Interactive Remote Access, removes the existing phrase “that is not an Intermediate System”. There could be an interpretation where an Intermediate System would be considered an Applicable System, not protected by an ESP. Thus the change appears to resulted in a “hall of mirrors”. We are suggesting the SDT provide clarity within the requirement or definition to avoid compliance issues for CIP-005 R2.1.

Likes 0

Dislikes 0

Response

Alison Mackellar - Constellation - 5

Answer No

Document Name

Comment

Constellation has elected to align with Exelon in response to this question.

Kim Turco, on behalf of Constellation Segments 5 and 6

Likes 0

Dislikes 0

Response

Kimberly Turco - Constellation - 6

Answer No

Document Name

Comment

Constellation has elected to align with Exelon in response to this question.

Kim Turco, on behalf of Constellation Segments 5 and 6

Likes 0

Dislikes 0

Response

Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC) 2016-02 Virtualization (Draft 3)

Answer

No

Document Name

Comment

The SRC does not agree with the proposed modification to the IRA definition. This type of change would require wholesale re-write of large parts of existing CIP standards to accommodate this change. The proposed change to existing standards would lead to re-interpretation and change in interpretation of currently effective requirements. This approach also puts a significant operational and financial burden on entities necessitating key program changes and re-investment in CIP tools and protections. The SRC recommends the drafting team consider simpler, lower-impact implementation guidance updates to address IRA which would be applicable to existing CIP requirements.

Additionally, the SRC believes that the proposed IRA definition change to require source of user-initiated routed traffic to come from outside the ESP may present concerns to entities leveraging EACMS outside ESP's. The SRC recommends that the SDT consider and document within the implementation guidance the use case of a management/monitoring network outside an ESP with EACMS implementations supporting reliability functions from such a network.

Likes 0

Dislikes 0

Response

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

Answer

No

Document Name

Comment

The updated definition of Interactive Remote Access, removes the existing phrase "that is not an Intermediate System". There could be an interpretation where an Intermediate System would be considered an Applicable System, not protected by an ESP. Thus the change appears to resulted in a "hall of mirrors". We are suggesting the SDT provide clarity within the requirement or definition to avoid compliance issues for CIP-005 R2.1.

Likes 0

Dislikes 0

Response

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

Answer No

Document Name

Comment

The proposed definition, specifically the third bullet, makes the MFA and the use of an Intermediate System in requirements in CIP-005 Part 2.1 and 2.3 a little confusing. At the end of the day, it seems as though the SDT is not intending to require MFA and an Intermediate System required for all SCI (only SCI and management interfaces supporting High and Medium Impact BCS and associated PCA) but because bullet #3 doesn't specify which SCI is being referred to, it could be interpreted that all interactive access to SCI requires the use of an Intermediate System and MFA. Recommend changing the third bullet to read:

“To a Management Interface of Shared Cyber Infrastructure protected by an ESP”

Likes 0

Dislikes 0

Response

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6

Answer No

Document Name

Comment

We do not agree with the removal of “that is not an Intermediate System.” With the current draft, an Intermediate System could be considered a “Cyber Asset or VCA not protected by any of the Responsible Entity’s ESPs.” Thus, an Intermediate System would be required for an Intermediate System.

Likes 0

Dislikes 0

Response

Nicolas Turcotte - Hydro-Quebec TransEnergie - 1

Answer No

Document Name

Comment

We support NPCC TFIST comments. Request clarification between CIP-005 Parts 2.1 and 2.2. Part 2.1 begins with “permit authorized Interactive Remote Access.” Part 2.2 begins with “for all IRA.” We suggest they should share the same beginning.

Likes 0

Dislikes 0

Response

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

Answer

No

Document Name

Comment

Request clarification between CIP-005 Parts 2.1 and 2.2. Part 2.1 begins with “permit authorized Interactive Remote Access.” Part 2.2 begins with “for all IRA.” We suggest they should share the same beginning.

Likes 0

Dislikes 0

Response

Thomas Breene - WEC Energy Group, Inc. - 3

Answer

No

Document Name

Comment

The definition for IRA clarifies the routable protocol to serial conversion scenario based on the rationale provided with the definition.

However, the removal of the following original clarifications used in the definitions is concerning:

"Remote access originates from a Cyber Asset that is not an Intermediate System..."

"Interactive remote access does not include system-to-system process communications."

Concerned without these referencable clarifying statements:

Intermediate Systems could be considered applicable to CIP-005 R2.1. (aligns with NSRF #4 response)

system to system process communications becomes a question again.

Likes 0

Dislikes 0

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer No

Document Name

Comment

IESO supports the comments provided by NPCC and IRC.

Likes 0

Dislikes 0

Response

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name SPP RTO

Answer No

Document Name

Comment

SPP is concerned that a wholesale re-write of large parts of the standards may lead to re-interpretation and substantive change in interpretation of requirements which could lead to significant program changes and re-investment in protections. Would the drafting team consider simpler, lower-impact implementation guidance with existing requirements instead? In this case, the change to IRA to require source of user-initiated routed traffic to come from outside the ESP may present concerns to entities leveraging EACMS outside ESP's.

Please also consider the use case of a management/monitoring network outside an ESP with EACMS implementations supporting reliability functions from such a network.

Likes 0

Dislikes 0

Response

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

Answer No

Document Name

Comment

The proposed language is not clear and confuses the issue.

Likes 0

Dislikes 0

Response

Lindsey Mannion - ReliabilityFirst - 10

Answer

No

Document Name

Comment

As written and presented, there is a gap between what is system-to-system and what is Interactive Remote Access (IRA) with the new IRA definition. Entities often rely on IRA ports for system-to-system communication but have not adequately enforced protections to ensure that malicious actors do not use the ports – regardless of whether a remote access client is available or used. Additional technical measures or controls should be added to the definition to ensure validity of communications to Applicable Systems. In addition, approval of CIP-005-8 would be conditional, based upon approval of the entire suite of new standards associated with virtualization and approval of SCI terminology and other definitions associated with virtualization. The SDT has not defined whether user-created scripts and programs that can be modified and scheduled to run independently are considered IRA – even though an unauthorized user could modify it to their benefit. Both scripts and programs can be user-initiated, and with no definition of system-to-system communications there is still lingering issues regarding what system-to-system communications is comprised of.

Likes 0

Dislikes 0

Response

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

Answer

No

Document Name

Comment

Should “or” be added to the end of the first bullet to more clearly define the need to continue dropping through the bullets like a decision tree to identify if any of the points are true instead of exiting after the first question?

Likes 0

Dislikes 0

Response

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

Answer	No
Document Name	
Comment	
<p>Comments: In the proposed revised definition of Interactive Remote Access, the existing phrase “that is not an Intermediate System” would be removed. We are concerned that there is a possibility that an Intermediate System would be considered a Cyber Asset or VCA, not protected by any of the Responsible Entity’s Electronic Security Perimeters, resulting in a “hall of mirrors” issue under CIP-005 R2.1. Accordingly we recommend either the phrase “that is not an Intermediate System” or the SDT provide clarity on how the proposed definition avoids compliance issues for Intermediate Systems vis-à-vis CIP-005 R2.1.</p>	
Likes	0
Dislikes	0
Response	
Carl Pineault - Hydro-Québec Production - 5	
Answer	No
Document Name	
Comment	
<p>Request clarification between CIP-005 Parts 2.1 and 2.2. Part 2.1 begins with “permit authorized Interactive Remote Access.” Part 2.2 begins with “for all IRA.” We suggest they should share the same beginning.</p>	
Likes	0
Dislikes	0
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
<p>NST sees no reason to change the existing definition's use of "remote access client or other remote access technology." The second part of the proposed definition would, as written, apply to any remote connection using a communications path that included routable to serial conversion, regardless of where that conversion took place (e.g., remote location vs. "local," or "inside the BES asset" location). NST is aware of concerns that using phrases such as "outside the asset" in this context might cause confusion about its relationship to electronic access control requirements for BES assets containing low impact BCS, but we nonetheless recommend using it to avoid overly broad application of "IRA" to communications using both routable and serial connections. Finally, NST believes the second bullet, "...That is converted to a non-routable protocol to a Cyber System not protected by an ESP" should apply only to a BES Cyber System not protected by an ESP.</p>	

Likes 0

Dislikes 0

Response

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

Answer

No

Document Name

Comment

Conversion to non-routable protocol in conjunction with authentication break should be sufficient and the subsequent bullets can be simplified in the IRA definition.

Language in the proposed definition is unclear due to the use of "or" in the bullet point "That is converted to a nonroutable protocol to a Cyber System not protected by an ESP; or". The use of "or" indicates a choice of only one of the two options, and choosing both options is not available. BC Hydro recommends clarifying the definition to allow the choice of both options.

The text "To a Cyber System protected by an ESP" should reside before the colon, and then add language that includes the additional qualifiers (the two subsequent bullets).

BCH requests clarity and pertinent use case examples of the newly defined term of 'IRA'

Likes 0

Dislikes 0

Response

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

Answer

No

Document Name

Comment

PNMR is concerned about IRA definition bullet point #2. This may get rid of the protocol break where IP to serial for a SCADA port was fine, but a user could initiate a session technically. The definition needs to result in user access not just user initiated. This seems to imply IRA can be between devices "not protected by an esp". Is that really IRA? Overall, the definition is confusing.

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	
Request clarification between CIP-005 Parts 2.1 and 2.2. Part 2.1 begins with “permit authorized Interactive Remote Access.” Part 2.2 begins with “for all IRA.” We suggest they should share the same beginning	
Likes 0	
Dislikes 0	
Response	
JT Kuehne - AEP - 6	
Answer	No
Document Name	
Comment	
The revised definition of IRA provides more clarity than the earlier version. With that said, AEP does not support the proposed changes made to the definition of IRA because we believe additional clarification is needed on the new term “Management Interface” which is used in the revised definition of IRA. In addition, AEP recommends adding “of a BCS” to the end of the last bullet, so it would read “ <i>To a Management Interface of Shared Cyber Infrastructure of a BCS.</i> ”	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Dwanique Spiller On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	No
Document Name	
Comment	
We do not agree with the removal of “that is not an Intermediate System.” With the current draft, an Intermediate System could be considered a “Cyber Asset or VCA not protected by any of the Responsible Entity’s ESPs.” Thus, an Intermediate System would be required for an Intermediate System.	
Likes 0	
Dislikes 0	
Response	

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

Answer No

Document Name

Comment

AZPS would like clarification on the proposed IRA definition, specifically we would like to understand the use cases which the 2nd bullet is intended to cover.

Likes 0

Dislikes 0

Response

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

Answer No

Document Name

Comment

- **Interactive Remote Access (IRA)** – Please clarify “user initiated” if it is limited to a person at a screen and keyboard or includes scheduled activities from EACMS outside the ESP into clients, agents or ssh into the ESP to SCI, MI, BCA, PCA, or VCA to run privileged application or command that use a protocol that is consider for “interactive user”.
- Please include the applicable definitions in CIP-002-7, CIP-005-7, CIP-007-7, and CIP-010-5 for orientation especially for those new to NERC CIP.

Likes 0

Dislikes 0

Response

Joseph Amato - Joseph Amato On Behalf of: Darnez Gresham, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Joseph Amato

Answer No

Document Name

Comment

We do not agree with the removal of “that is not an Intermediate System.” With the current draft, an Intermediate System could be considered a “Cyber Asset or VCA not protected by any of the Responsible Entity’s ESPs.” Thus, an Intermediate System would be required for an Intermediate System.

Likes 0

Dislikes 0

Response

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

Answer No

Document Name

Comment

CHPD appreciates the SDT's efforts for the modified definition of IRA. However, the definition remains cumbersome with the extra language needed to support SCI, which does not need to be within an ESP. Additionally, because Active Directory and the multi-factor authentication systems are part of the scheme to restrict access to IRA, they implicitly become Intermediate Systems, which is undesirable. CHPD suggests the following revisions:

IRA - User-initiated interactive access by a person from one Cyber Asset or Virtual Cyber Asset to another.

This makes IRA exist everywhere where any access from one (Virtual) Cyber Asset to another (Virtual) Cyber Asset is IRA. We scope what IRA is to be protected in the requirement, not in the definition.

Intermediate System - One or more Electronic Access Control or Monitoring Systems that are used to perform Interactive Remote Access to another Cyber Asset or Virtual Cyber Asset.

The requirement that the Intermediate System be outside the ESP is below in CIP-005 R2.1; Interactive Remote Access and Intermediate System exist, but there are currently no requirements on them.

CIP-005 R2.1

Applicable Systems:

High Impact BCS and their associated:

- PCA; or
- SCI

Medium Impact BCS and their associated:

- PCA; or
- SCI

Requirement:

Permit IRA, if any, only from:

- A Cyber Asset or Virtual Cyber Asset within a Responsible Entity's ESP
- An Intermediate System outside any ESP

This provides the scope for the requirement to only allow IRA connecting to Applicable Systems from a system protected by the ESP or from the Intermediate System outside the ESP. This also catches serial communications, since IRA is completely agnostic to communication protocol. If a device can connect to a BCA via serial, then it is IRA and that connection is only permitted if the source device is inside the ESP or if it is an Intermediate System.

CIP-005 R2.2

Applicable Systems:

Intermediate Systems used to access Applicable System of Part 2.1

Requirement:

Protect the Confidentiality and Integrity of all IRA connecting to the Intermediate System.

CHPD recommends the following rewording, which puts the verb first.

CIP-005 R2.3

Applicable Systems:

Intermediate Systems used to access Applicable System of Part 2.1

Requirement:

Require multi-factor authentication for all IRA connecting to the Intermediate System.

This is a minor change, as it would technically allow a connection from the Intermediate System to the ESP without MFA if one logs in locally to the Intermediate System. However, this does not seem to be a problem, the Intermediate System is required to be within the Physical Security Perimeter, so it is protected by that layer of protection.

R2.4 through R2.5 can remain as is, as they are not impacted by the suggested change to IRA. R2.6 should be deleted as it is covered by R2.1 now.

Likes 0

Dislikes 0

Response

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

Answer

No

Document Name

Comment

We do not agree with the removal of "that is not an Intermediate System." With the current draft, an Intermediate System could be considered a "Cyber Asset or VCA not protected by any of the Responsible Entity's ESPs." Thus, an Intermediate System would be required for an Intermediate System.

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).

Likes 0

Dislikes 0

Response

George Brown - Acciona Energy North America - 5

Answer

No

Document Name

Comment

Acciona Energy supports Midwest Reliability Organization's (MRO) NERC Standards Review Forum's (NSRF) comments on this question.

Likes 0

Dislikes 0

Response

Ryan Strom - Buckeye Power, Inc. - 5

Answer

No

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer

No

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 Hirschak, 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

See EEI comment.

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

ITC supports the comments submitted by EEI

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

We support NPCC RSC's comments.

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

EEl supports the proposed simplified definition of IRA.

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 simplified IRA definition.

Likes 0

Dislikes 0

Response

Maggy Powell - Amazon Web Services - 7

Answer Yes

Document Name

Comment

N/A

Likes 0

Dislikes 0

Response

patricia ireland - DTE Energy - 4

Answer Yes

Document Name	
Comment	
Patty Ireland on behalf of DTE Energy, Segments 3 and 4	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - SERC,RF	
Answer	Yes
Document Name	
Comment	
We agree with the proposed change.	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
<p>While the IRA definition is usable, BPA suggests making the following alterations to correct an apparent omission, ensure that scope is clearly limited to BCS, and ensure that grammar is less open to interpretation:</p> <p>User-initiated access by a person using routable protocol and a Cyber Asset or VCA not protected by any of the Responsible Entity's Electronic Security Perimeter(s) (ESP) that is:</p> <ul style="list-style-type: none"> &bull; To a cyber system protected by an ESP; or &bull; Converted to a non-routable protocol to a BCS not protected by an ESP; or &bull; To a Management Interface of Shared Cyber Infrastructure. 	
Likes 0	
Dislikes 0	

Response

Joni Jones - Wabash Valley Power Association - 1

Answer Yes

Document Name

Comment

While we agree, one risk with this definition and CIP-005 is that it is ambiguous where a software defined networking management plane would fall into the control environment.

Likes 0

Dislikes 0

Response

Scott Kinney - Avista - Avista Corporation - 3

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

Justin MacDonald - Midwest Energy, Inc. - 1

Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Likes	0

Dislikes 0

Response

James Baldwin - Lower Colorado River Authority - 1

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

David Jendras - Ameren - Ameren Services - 3

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Jesus Sammy Alcaraz - Imperial Irrigation District - 1

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Glen Farmer - Avista - Avista Corporation - 5

Answer

Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster	
Answer	Yes
Document Name	
Comment	
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	
William Steiner - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0

Response

Jennifer Malon - Jennifer Malon On Behalf of: Brooke Voorhees, Black Hills Corporation, 3, 5, 1, 6; Derek Silbaugh, Black Hills Corporation, 3, 5, 1, 6; Don Stahl, Black Hills Corporation, 3, 5, 1, 6; Seth Nelson, Black Hills Corporation, 3, 5, 1, 6; - Jennifer Malon

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Hien Ho - Tacoma Public Utilities (Tacoma, WA) - 4

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Donald Lock - Talen Generation, LLC - 5

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

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

Dislikes 0

Response

Bryan Koyle - Southern Indiana Gas and Electric Co. - 3,5,6 - RF

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Josh Johnson - Lincoln Electric System - 1

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer

Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Marshall - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Patricia Lynch - NRG - NRG Energy, 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

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

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,5 - RF

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Kinte Whitehead - Exelon - 3

Answer

Document Name

Comment

Exelon will align with EEI in response to this question.

Likes 0

Dislikes 0

Response

Daniel Gacek - Exelon - 1

Answer

Document Name

Comment

Exelon will align with EEI in response to this question.

Likes 0

Dislikes 0

Response

5. The SDT modified the VCA definition primarily to include the ability to host them on numerous asset types other than SCI. This allows for current state, where entities consider hypervisors as BCA, EACMS, etc. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

Joni Jones - Wabash Valley Power Association - 1

Answer No

Document Name

Comment

The phrase “excluding logical instances that are being actively remediated” does not accurately communicate the intent and provides no clear indication what actively remediated means. Further, this provides an incredible amount of ambiguity for enforcement on timing, and understanding of remediation. We agree with the remainder of the definition.

Likes 0

Dislikes 0

Response

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

Answer No

Document Name

Comment

SRP would like clarification on the last sentence “excluding logical instance that are being actively remediated”.

Likes 0

Dislikes 0

Response

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

Answer No

Document Name

Comment

This is a very confusing definition. Please add context to "actively remediated".

Likes 0

Dislikes 0

Response	
Justin Welty - NextEra Energy - Florida Power and Light Co. - 6	
Answer	No
Document Name	
Comment	
<p>Virtual Cyber Asset (VCA) New Definition –The definition does not address the possibility of containers. Consider adding language “including containers with operating system, firmware or isolated process”.</p>	
Likes	0
Dislikes	0
Response	
Amy Wesselkamper - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	No
Document Name	
Comment	
<p>“Non-dormant” and “excluding logical instances that are being actively remediated” feel redundand and sumwhat like a double negative. PNMR recommends the following modification. “A logical instance of an operating system or firmware, on a virtual machine hosted on a BES Cyber Asset; Electronic Access Control or Monitoring System; Physical Access Control System; Protected Cyber Asset; or Shared Cyber Infrastructure; excluding logical instances that are being actively remediated or dormant instances.)</p>	
Likes	0
Dislikes	0
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
<p>NST believes the proposed definition should more closely resemble the existing definition of "Cyber Asset" or, better still, be eliminated altogether. The existing definition of "Cyber Asset" could be easily "unbound" from "hardware" with this or a similar modification:</p>	

Change from, "Programmable electronic devices, including the hardware, software, and data in those devices" to, "Hardware-based or virtual programmable electronic devices, including the software and data in those devices."

Likes 0

Dislikes 0

Response

William Steiner - Midwest Reliability Organization - 10

Answer

No

Document Name

Comment

- Virtual Cyber Asset

- The scoping of VCA to include only those virtual machines hosted on BCA, EACMS, PACS, PCA, or SCI appears to exclude other virtual machines. This is a noticeable difference from CA, which includes all programmable assets regardless of classification.
 - We think the expectation may be that the underlying hardware would still be a Cyber Asset, which is clear for individual hypervisors, but is not as clear for clusters, which really aren't addressed outside of the SCI definition. If that was the intent, we recommend adding clarity at least to the rationale.
 - An example where this matters would be on a corporate cluster that hosts no BCA, EACMS, PACS, PCA, and therefore is a cluster that is not SCI. Any virtual machine hosted by that cluster would not be considered a VCA. The scoping in CIP-003 R2 Attachment 1, Section 3.1.i does not include non-VCA virtual machines, so controls may not be in place for that communication. Similarly, in CIP-005 R2, the IRA definition does not include virtual machines that are not VCAs, so they may not be required to go through an Intermediate System
 - MRO recommends that the Virtual Cyber Asset definition not be limited to virtual machines hosted on specific classifications of CAs/SCI, but rather include all virtual machines (similar to how CA includes all programmable electronic devices)
- MRO also observed that the VCA and SCI definitions are circular. SCI may be identified by its hosting of VCA, but VCA may be identified by being hosted on SCI.

Likes 0

Dislikes 0

Response

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

Answer

No

Document Name

Comment

The language "on a virtual machine" implies that a VCA is separate and distinct than a virtual machine since it resides "on a virtual machine". Should the language be something like logical instance of an operating system or firmware **of** a virtual machine...? This may lead to confusion of what requirements are necessary for a VCA vs a VM.

What does actively remediated mean? could be worded better than instances being actively remediated...today we have virtual firmware and OS...non-dormant seems to mean an image not started yet. Clarity needed for “on” what does “on” mean. Should it be changed to “of”?

Likes 0

Dislikes 0

Response

Lindsey Mannion - ReliabilityFirst - 10

Answer

No

Document Name

Comment

While the definition is specific with regards to dormancy, according to publications from the Cloud Security Alliance (see [*Best Practices for Mitigating Risks Virtual Environments April2015_4-1-15_GLM5.pdf*](#)), many issues need to be identified and secured in a virtualized environment when dealing with dormant VMs. VM sprawl can create uncontrolled proliferation of dormant VMs and can lead to an unmanageable condition of unpatched and unaccounted-for machines. Further, dormant, and offline VMs can deviate so far from a current security baseline that simply powering them on introduces massive security vulnerabilities (this is specifically mentioned in NIST publication [*NIST.SP.800-125Ar1.pdf*](#)). In addition, inadvertent initiation of a dormant VM that is part of an identified BCS within the ESP would be considered at least a PCA by definition of its connection via a routable protocol within a defined ESP. As stated above, a dormant VM may quickly move out of compliance with respect to security patches or updates that could be a security risk via multiple vulnerabilities for all other BCS within the associated ESP. Active remediation as implied in the new definition of VCA allows a “loophole” as there is no reference for what “active remediation” is. Using “Remediation VLANs” introduce new risks as the VCA may still be required to acquire an IP address (DHCP, if it is not hard-coded) and is required to initiate connections to authorize and authenticate itself prior to determining by policy if the Cyber Asset requires remediation. Poorly constructed, managed, and implemented policies to determine a VCA’s remediation status could allow persistent connections of VCA without proper updates until such time that the VCA is isolated with the other remediated support system (patches, updates, malicious code updates, etc.). By this action alone, a compromised system that is initiated could create security issues prior to the “remediation mode” or maintenance mode being invoked. Finally, there is no NERC definition of “Remediation VLAN” or “actively remediated” so there may be ongoing issues associated with differences of interpretation between Responsible Entities and the ERO Enterprise. Use of currently available tools to transfer VM Guests from a test or QA environment would allow complete patching, antivirus, updates, etc. prior to introduction of a dormant or new VM Guest into a production environment and keep the proliferation of dormant VM Guests to a minimum.

Likes 0

Dislikes 0

Response

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

Answer

No

Document Name

Comment

The proposed definition is too ambiguous. Please provide more context around “non-dormant”.

Likes 0

Dislikes 0

Response

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name SPP RTO

Answer No

Document Name

Comment

SPP has concerns for the definition of Virtual Cyber Asset(VCA) describes a “non-dormant logical instance.” What does the SDT mean by non-dormant in regards to a VCA? If a virtual machine is not in use, would that be classified as dormant and then once it is needed it becomes a VCA? Would a Golden Image be classified as dormant? Is the term “non-dormant” a permanent state? To help with interpretation, SPP would appreciate the SDT providing examples of what is meant by “Non-Dormant.”

Likes 0

Dislikes 0

Response

Maggy Powell - Amazon Web Services - 7

Answer No

Document Name

Comment

As noted by the drafting team in the *Technical Rationale, Project 2016-02 Modifications to CIP Standards New and Modified Terms, and Exemption Language Used in NERC Reliability Standards*, the “one-to- one relationship between a Cyber Asset and its underlying hardware is what virtualization intentionally breaks to increase reliability and resiliency.” Breaking the one-to-one relationship introduces new concepts like containerization that have security implications.

Applications can be containerized, including critical applications that could pose a direct impact to the grid, just as a physical on-prem BCA. We suggest revising the definition to “...logical instance of an operating system, firmware, or containerized application, on a virtual machine...”

Additionally, page 8 of the *Technical Rationale, Project 2016-02 Modifications to CIP Standards New and Modified Terms, and Exemption Language Used in NERC Reliability Standards* that states that “the phrase ‘excluding logical instances that are being actively remediated’ excludes those that are instantiated but are being remediated in an isolated environment before they are moved to production networks and begin providing their function or service” could be interpreted to mean that test environments or isolated environments are necessary for VCAs regardless of Impact Rating or device classification. The proposed CIP-010-5 R1, Part 1.2 is the only Requirement that discusses test environments, and only requires changes to be tested in a test environment prior to being deployed to production for High Impact BCS..

We suggest clarifying the VCA definition and/or technical rationale to state what is meant by “being actively remediated.” Standard Drafting team should clarify their intention by stating whether the term “being actively remediated” is mean to address both the configuration of a new VCA prior to it being moved to a production environment to perform its function, or if the intention spans to change management activities such as patching and configuration

changes. Implementation guidance for remediating logical instances such as requiring the VCA to be in an environment isolated from production at the time of remediation would also be beneficial.

Likes 0

Dislikes 0

Response

David Jendras - Ameren - Ameren Services - 3

Answer

No

Document Name

Comment

Non-dormant logical instance needs to be defined, the phrase actively remediated needs to be clarified.

Likes 0

Dislikes 0

Response

Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC) 2016-02 Virtualization (Draft 3)

Answer

No

Document Name

Comment

The SRC does not agree with the proposed modification to the VCA definition as it does not consider all use cases. The SRC highlights the use case of “active logical instance of an operating system” as a virtual machine running on a Cyber Asset.”

Additionally, the SRC requests further clarification be provided regarding the VCA definition in the following areas:

- *exclusion involving remediation and how the how the VCA definition may change during remediation efforts*
- *the feasibility and the level of detail required to list all categories of possible applicability as potential hypervisors for a given VCA*

The SRC also notes that there is distinction between a label (applicable system) and a transition process (non-dormant vs. dormant). However, SRC notes that some definitions seem to incorporate aspects of both, which may lead to confusion with interpretation of the definition. The SRC recommends the SDT to modify the term “non-dormant” as follows: If a VM is powered off (dormant), it is not a VCA. Likewise, the tail end of the definition is to prevent an entity from being in violation simply for powering up a VM. As long as that VM is moved to a remediation vlan (like a build network) and remediated it is not a VCA. Once remediated and back into production, it is a VCA again.

Likes 0

Dislikes 0

Response

George Brown - Acciona Energy North America - 5

Answer Yes

Document Name

Comment

Acciona Energy supports Midwest Reliability Organization's (MRO) NERC Standards Review Forum's (NSRF) comments on this question.

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

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

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

The definition is clear and possibly unnecessary given the intent is to simply provide an equivalent virtualized term for a Cyber Asset.

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

AZPS agrees with the proposed definition but would like the SDT to provide more clarity on the following:

What does actively remediate mean?

What constitutes dormant vs. non-dormant?

Likes 0

Dislikes 0

Response

Ellese Murphy - Duke Energy - 1,3,5,6 - SERC,RF

Answer Yes

Document Name

Comment

We agree with the proposed change.

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

CEHE agrees with the proposed VCA definition.

Likes 0

Dislikes 0

Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
<p>Although we agree with the proposed change, it is not explicitly clear that a hypervisor environment hosting VCAs must be categorized as a BCA, EACMS, etc. To avoid confusion the definition for SCI could state that a hypervisor environment hosting virtual cyber assets of the same classification must be categorized as the same type of cyber asset</p>	
Likes	0
Dislikes	0

Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes
Document Name	
Comment	
<p>The direction of the drafting team and new definition address the concern for SCI hosted on multiple classifications of Cyber Assets. The TCA classification was missing. The definition contains a term "Virtual Machine" that is technology specific and does not necessarily apply to all virtualization technologies such as the use of virtualization on a Cisco network switch implementing "Virtual Device Context" (VDC) to run independent instances of the switch on the same hardware. The following is proposed:</p> <p>A non-dormant logical instance of an operating system or firmware, hosted on a BCA,</p> <p>EACMS, PACS, PCA, TCA or SCI THAT SUPPORTS RUNNING MULTIPLE LOGICAL INSTANCES OF AN OPERATING SYSTEM OR FIRMWARE, excluding logical instances that are being actively remediated</p>	
Likes	0
Dislikes	0

Response	
JT Kuehne - AEP - 6	
Answer	Yes
Document Name	

Comment

AEP supports the definition of new term VCA.

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

No comment

Likes 0

Dislikes 0

Response

patricia ireland - DTE Energy - 4

Answer

Yes

Document Name

Comment

Patty Ireland on behalf of DTE Energy, Segments 3 and 4

Likes 0

Dislikes 0

Response

Carl Pineault - Hydro-Quebec Production - 5

Answer

Yes

Document Name

Comment

No comment

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

Comments: We request clarification on the exclusion involving remediation (“excluding logical instances that are being actively remediated). Does the status of the VCA change during remediation efforts?

What is the distinction between a label (applicable system) and a transition process (non-dormant vs. dormant)? Some definitions seem to incorporate aspects of both, which may lead to confusion with interpretation of the definition.

We believe there needs to be some language somewhere that addresses the phrase “non-dormant” in the definition. While we acknowledge that, at face value, it seems self-explanatory, in practice it’s possible there may be some instances of interpretation. We are not seeking a definition but just some clarity, perhaps in the Technical Guide, that addresses the topic further.

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 modified definition of VCA and the ability to host them on numerous asset types other than SCI.

Likes 0

Dislikes 0

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	Yes
Document Name	
Comment	
No comment	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI supports the proposed change.	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
We support NPCC RSC's comments.	
Request that guidance be added on the meaning of "remediated" as it is used in the VCA definition and the Technical Guidance and Rationale. Please differentiate between "active remediation" and some other form of remediation.	
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 comments submitted by EEI

Likes 0

Dislikes 0

Response

Kimberly Turco - Constellation - 6

Answer Yes

Document Name

Comment

Constellation has elected to align with Exelon in response to this question.

Kim Turco, on behalf of Constellation Segments 5 and 6

Likes 0

Dislikes 0

Response

Alison Mackellar - Constellation - 5

Answer Yes

Document Name

Comment

Constellation has elected to align with Exelon in response to this question.

Kim Turco, on behalf of Constellation Segments 5 and 6

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 Hirschak, 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

See EEI comment.

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Alliant Energy supports the comments submitted by the MRO NSRF.

Likes 0

Dislikes 0

Response

Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,5 - RF

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Mike Marshall - IDACORP - Idaho Power Company - 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	
Ryan Strom - Buckeye Power, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy 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

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Joseph Amato - Joseph Amato On Behalf of: Darnez Gresham, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Joseph Amato

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

Josh Johnson - Lincoln Electric System - 1

Answer Yes

Document Name

Comment	
Likes 0	
Dislikes 0	
Response	
Bryan Koyle - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Dwanique Spiller On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bridget Silvia - Sempra - San Diego Gas and Electric - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Donald Lock - Talen Generation, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Hien Ho - Tacoma Public Utilities (Tacoma, WA) - 4	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Jennifer Malon - Jennifer Malon On Behalf of: Brooke Voorhees, Black Hills Corporation, 3, 5, 1, 6; Derek Silbaugh, Black Hills Corporation, 3, 5, 1, 6; Don Stahl, Black Hills Corporation, 3, 5, 1, 6; Seth Nelson, Black Hills Corporation, 3, 5, 1, 6; - Jennifer Malon	
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	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Glen Farmer - Avista - Avista Corporation - 5

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Jesus Sammy Alcaraz - Imperial Irrigation District - 1

Answer Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response

John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

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

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

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Justin MacDonald - Midwest Energy, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Kinney - Avista - Avista Corporation - 3	
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

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

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Daniel Gacek - Exelon - 1

Answer

Document Name

Comment

Exelon will align with EEI in response to this question.

Likes 0

Dislikes 0

Response

Kinte Whitehead - Exelon - 3

Answer	
Document Name	
Comment	
Exelon will align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	

6. The SDT modified numerous other glossary terms. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

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

Answer No

Document Name

Comment

While largely in agreement with the proposed changes, we have issues with some of the proposed definitions.

First, we are concerned with the revised definition of Electronic Access Point, specifically with the term “to and from a BES Cyber System.” This could result in every BES Cyber System being considered an EAP, with additional requirements of an EAP. We suggest using second part of the existing definition: An electronic policy enforcement point or a Cyber Asset interface that controls routable communication between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter.

Further, the SDT may wish to address how host-based firewalls are treated under the proposed EAP definition (for example, is each host firewall a separate EAP or may be grouped together as one EAP).

Also, we are concerned that the revised definition of Protected Cyber Asset is contradictory to the new definition of Shared Cyber Infrastructure. The second bullet in the PCA definition states that it is a “Cyber Asset or Virtual Cyber Asset that shares CPU or memory with any part of the BES Cyber System...” This description seems to elevate the PCA to the higher watermark level than a BES Cyber Asset, and also seems to fit the definition of SCI. We suggest deleting the second bullet in the proposed PCA definition.

Likes 0

Dislikes 0

Response

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

Answer No

Document Name

Comment

Alliant Energy supports the comments submitted by the MRO NSRF.

Likes 0

Dislikes 0

Response

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

Answer No

Document Name	
Comment	
<p>AEPCO is signing on to ACES comments below.</p> <p>ACES Comments: We agree with most of the modifications to the proposed changes with minor exceptions:</p> <p>Within an ESP in a Zero Trust environment a network can be configured to restrict network traffic via policy enforcement all the way down to the switch port. In this case it is not clear if the policy protecting the BCS is the EAP or is each and every Cyber Asset interface within the Zero Trust environment with an enforcement policy is an EACMS/EAP as each Cyber Asset with a policy pushed from a Zero Trust policy server is an enforcement point. This would significantly increase the number of EACMS/EAP within a BCS. We feel there needs to be clarification or exclusions within the definition unless this is the intent of the modifications.</p>	
Likes 0	
Dislikes 0	
Response	
<p>Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirschak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker</p>	
Answer	No
Document Name	
Comment	
<p>See EEI comment.</p>	
Likes 0	
Dislikes 0	
Response	
<p>Alison Mackellar - Constellation - 5</p>	
Answer	No
Document Name	
Comment	
<p>Constellation has elected to align with Exelon in response to this question.</p> <p>Kim Turco, on behalf of Constellation Segments 5 and 6</p>	
Likes 0	

Dislikes 0

Response

Kimberly Turco - Constellation - 6

Answer

No

Document Name

Comment

Constellation has elected to align with Exelon in response to this question.

Kim Turco, on behalf of Constellation Segments 5 and 6

Likes 0

Dislikes 0

Response

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

Answer

No

Document Name

Comment

For this question, ITC supports the NSRF response

Likes 0

Dislikes 0

Response

Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC) 2016-02 Virtualization (Draft 3)

Answer

No

Document Name

Comment

The SRC does not agree with the proposed changes. Specifically, the PCA definition has become significantly more complicated as the current definition is much more straightforward distinguishing only the presence of the PCA network interface(s) in an ESP. Additionally, the SRC believes the mixture of label (applicable system) and process (remediation) does present opportunity for different interpretations of this definition (second bullet).

Furthermore, the addition of CPU/memory sharing as a criterion for categorizing a Cyber Asset as a PCA does increase the required program coverage of such boundaries as part of CIP-002 process.

SRC requests further clarification be provided regarding the new definition for BCS. In particular, the SRC requests that SDT clarify whether "Acronym only" be revised to include the original language for BCS Or does whether the current proposed redline change indicates that the original text stays and the only change is to the definition term field to include the acronym specifically.

Likes 0

Dislikes 0

Response

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

Answer

No

Document Name

Comment

The term Cyber System is not needed since it seems to be only used in CIP-010 R3.3 and IRA definition. The use in the CIP-010 R3.3 requirement is confusing since Cyber System includes PACS and TCAs and the CIP-010 R3.3 Applicable Systems does not.

Likes 0

Dislikes 0

Response

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

Answer

No

Document Name

Comment

We agree with most of the modifications to the proposed changes with minor exceptions:

Within an ESP in a Zero Trust environment a network can be configured to restrict network traffic via policy enforcement all the way down to the switch port. In this case it is not clear if the policy protecting the BCS is the EAP or is each and every Cyber Asset interface within the Zero Trust environment with an enforcement policy is an EACMS/EAP as each Cyber Asset with a policy pushed from a Zero Trust policy server is an enforcement point. This would significantly increase the number of EACMS/EAP within a BCS. We feel there needs to be clarification or exclusions within the definition unless this is the intent of the modifications.

Likes 0

Dislikes 0

Response

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6

Answer No

Document Name

Comment

Electronic Access Point: BHE does not agree with the revised definition of Electronic Access Point, specifically with the term “to and from a BES Cyber System.” This could result in every BES Cyber System being considered an EAP, with additional requirements of an EAP. Suggest using second part of the existing definition: An electronic policy enforcement point or a Cyber Asset interface that controls routable communication between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter.”

Protected Cyber Asset: BHE does not agree with the revised definition of PCA because it is contradictory to the new definition of Shared Cyber Infrastructure. The second bullet in the PCA definition states it is a “Cyber Asset or Virtual Cyber Asset that shares CPU or memory with any part of the BES Cyber System...” This description seems to elevate the PCA to the higher watermark level of the BCA, and also seems to fit the definition of SCI. Suggest deleting the second bullet in the PCA definition.

Likes 0

Dislikes 0

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1

Answer No

Document Name

Comment

We support NPCC TFIST comments.

Request clarification. Does the SDT intend CIP-008 Reportable Cyber Incident to include SCI but not PCA?

Likes 0

Dislikes 0

Response

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

Answer No

Document Name

Comment

Request clarification. Does the SDT intend CIP-008 Reportable Cyber Incident to include SCI but not PCA?

Likes 0

Dislikes 0

Response

Thomas Breene - WEC Energy Group, Inc. - 3

Answer No

Document Name

Comment

As written, the new definition for Management Interface is unclear of its intended description. Based on the rationale, it is understood why the need to define these interfaces. However, this definition differs from the virtual machine concept and extends to application functionality tools. Thus bringing additional devices into scope even for those entities that are not using virtual machines. Proposing the 2nd and 3rd bullet are removed from the definition.

Likes 0

Dislikes 0

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer No

Document Name

Comment

IESO supports the comments provided by NPCC and IRC

Likes 0

Dislikes 0

Response

Maggy Powell - Amazon Web Services - 7

Answer No

Document Name

Comment

Management Interface: The new language attempts to simplify the definition by describing what Lightsout Management (LOM) is in the definition itself but may limit an Entity's ability to clearly identify and appropriately classify all possible management interfaces. LOM is industry accepted terminology and we recommend reverting to the previous iteration of the definition.

Transient Cyber Asset (TCA):

The modification to the Transient Cyber Asset definition that allows virtual machines running on a physical TCA to be treated as software on the device should be reconsidered. As written, an entity may not apply the appropriate security controls to the virtual machines running on physical TCAs. Entities should be monitoring the state of the virtual machines running on their physical hardware for security issues.

We propose removing the language "Virtual machines hosted on a physical TCA can be treated as software on that physical TCA" from the TCA definition. By removing this language, entities would be required to apply security controls to the virtual machines hosted on their physical TCAs in alignment with CIP-010 R4.

Virtual Cyber Asset:

As noted by the drafting team in the *Technical Rationale, Project 2016-02 Modifications to CIP Standards New and Modified Terms, and Exemption Language Used in NERC Reliability Standards*, the "one-to-one relationship between a Cyber Asset and its underlying hardware is what virtualization intentionally breaks to increase reliability and resiliency." Breaking the one-to-one relationship introduces new concepts like containerization that have security implications.

Applications can be containerized, including critical applications that could pose a direct impact to the grid, just as a physical on-prem BCA. We suggest revising the definition to "...logical instance of an operating system, firmware, or containerized application, on a virtual machine...".

Additionally, page 8 of the *Technical Rationale, Project 2016-02 Modifications to CIP Standards New and Modified Terms, and Exemption Language Used in NERC Reliability Standards* states that "the phrase 'excluding logical instances that are being actively remediated' excludes those that are instantiated but are being remediated in an isolated environment before they are moved to production networks and begin providing their function or service" could be interpreted to mean that test environments or isolated environments are necessary for VCAs regardless of Impact Rating or device classification. The proposed CIP-010-5 R1, Part 1.2 is the only Requirement that discusses test environments, and only requires changes to be tested in a test environment prior to being deployed to production for High Impact BCS..

We suggest clarifying the VCA definition and/or technical rationale to state what is meant by "being actively remediated." Standard Drafting team should clarify their intention by stating whether the term "being actively remediated" is meant to address both the configuration of a new VCA prior to it being moved to a production environment to perform its function, or if the intention spans to change management activities such as patching and configuration changes. Implementation guidance for remediating logical instances such as requiring the VCA to be in an environment isolated from production at the time of remediation would also be beneficial.

Likes 0

Dislikes 0

Response

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name SPP RTO

Answer No

Document Name

Comment

SPP has the following comments on the proposals for glossary terms.

- SPP is concerned that the SDT has revised the definition of BES Cyber System as an “Acronym Only” while still including the term in the other definitions. SPP recommends the definition be added back to the term or removed from all of the standards where it is still included. “Cyber System” should also reference “BES Cyber System” to show their continuity.
- Intermediate System has been removed from the ESP, thereby lessening the security of an Intermediate System. The PCA definition has become significantly more complicated.
- The previous definition was much more straightforward with the only distinction being presence of the PCA network interface(s) in an ESP.
- The mixture of label (applicable system) and process (remediation) does present opportunity for different interpretations of this definition (second bullet).
- The addition of CPU/memory sharing as a criterion for categorizing a Cyber Asset as a PCA does increase the required program coverage of such boundaries as part of CIP-002 process.

Likes 0

Dislikes 0

Response

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

Answer

No

Document Name

Comment

BES Cyber Asset – Dominion does not agree with the proposed VCA definition.

Cyber System – Dominion found this definition to be confusing. A Cyber System is not defined by being part of the BES. Was the intent behind this to expand Cyber System beyond BES Cyber System? Please clarify.

Electronic Access Point (EAP) – Please provide more clarification on what electronic policy enforcement point means.

Management Interface – Does this definition include all power management devices? For example, does it include UPSs regardless of the access controls on the device?

Protected Cyber Aset (PCA) – Please provide clarity around what is included in “actively remediating prior to introduction to an ESP” (second bullet).

Removable Media – Dominion thinks the examples are necessary and suggests adding examples of virtual removable media.

Likes 0

Dislikes 0

Response

Lindsey Mannion - ReliabilityFirst - 10

Answer	No
Document Name	
Comment	
<p>Since the Glossary modifications are the foundation to all Standard changes, NERC should seek approval of the new terms prior to any changes being introduced in the Standards to reduce potential misunderstanding or misinterpretation of both the new definitions and modified Standards. This will also allow NERC, and industry, time to determine additional courses of action, reduce confusion, and reduce additional risk associated with such wholesale changes.</p>	
Likes 0	
Dislikes 0	
Response	
Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	
<p>Comments: We are concerned that the revised definition of Protected Cyber Asset is contradictory to the new definition of Shared Cyber Infrastructure. The second bullet in the PCA definition states that it is a “Cyber Asset or Virtual Cyber Asset that shares CPU or memory with any part of the BES Cyber System...” This description seems to elevate the PCA to the higher watermark level than a BES Cyber Asset, and also seems to fit the definition of SCI. We suggest deleting the second bullet in the proposed PCA definition. Further, the SDT may wish to address how host-based firewalls are treated under the proposed EAP definition (for example, is each host firewall a separate EAP or may be grouped together as one EAP?).</p>	
Likes 0	
Dislikes 0	
Response	
William Steiner - Midwest Reliability Organization - 10	
Answer	No
Document Name	
Comment	
<p>Management Interface</p> <p>- Management Interface</p> <ul style="list-style-type: none"> olt is still unclear if Management Interface includes software that resides on a different CA from the SCI. 	

- The first bullet in the definition appears to include vCenter and the third bullet appears that it would include firewall orchestration implementations. Both are typically on a separate CA or virtual machine, rather than being integrated into the hypervisor cluster or firewall appliances.
- MRO is concerned that the only required controls of the Management Interfaces are network access in CIP-005 Part 1.3 (no CIP-004, CIP-007, CIP-010, etc. controls are applicable to Management Interfaces).

Likes 0

Dislikes 0

Response

Carl Pineault - Hydro-Qu?bec Production - 5

Answer

No

Document Name

Comment

Request clarification. Does the SDT intend CIP-008 Reportable Cyber Incident to include SCI but not PCA?

Likes 0

Dislikes 0

Response

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

Answer

No

Document Name

Comment

NST considers the statement in the proposed definition of TCA, " Virtual machines hosted on a physical TCA are treated as software on that physical TCA" to be oddly inconsistent with the proposed definition of VCA. Furthermore, we disagree with the SDT's opinion that if a physical TCA hosts multiple virtual TCAs, there should be no need to track and manage each individual physical and virtual device.

Likes 0

Dislikes 0

Response

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

Answer

No

Document Name

Comment

Management Interfaces: Why is it restricted to SCI and EACMS? The new definition excludes most of BC Hydro's BCS.

TCA definition: It includes VCAs, however, VCAs are defined as being hosted on BCAs, EACMS, PACS and SCI. A TCA is by definition not part of any of those and is connected for less than 30 days. The qualifiers for VCAs and VMs being TCAs are unclear. There is an implication that VCA can be a BCS; however, a BCS cannot be a TCA since a TCA is connected for less than 30 days.

PACS: Are VCA and SCI not Cyber Assets already? Is the differentiation necessary? Please clarify and provide some examples or use cases.

PCA: The new definition requires clarification. "Share CPU or memory" needs clarification, as does the exclusion "are being actively remediated prior to introduction to an ESP."

BC Hydro requests additional clarity on the use of the above definitions, with pertinent examples as appropriate.

Likes 0

Dislikes 0

Response

Jennifer Malon - Jennifer Malon On Behalf of: Brooke Voorhees, Black Hills Corporation, 3, 5, 1, 6; Derek Silbaugh, Black Hills Corporation, 3, 5, 1, 6; Don Stahl, Black Hills Corporation, 3, 5, 1, 6; Seth Nelson, Black Hills Corporation, 3, 5, 1, 6; - Jennifer Malon

Answer

No

Document Name

Comment

In the EACMS definition, "cyber asset" should be replaced with "Cyber System" since a cyber system can be a single asset. Alternatively, it seems that "Cyber System" is used in only one other location. Does the "Cyber System" definition really need to exist?

In the "Reportable BES Cyber Security Incident" definition, the 1st bullet could be removed since it is the definition of a BES Cyber System if that definition remains.

In the "Removable Media" definition, BHP recommends keeping the examples removed which serve to help less technical individuals understand the intent of related requirements.

For the BCSI definition, BHP is OK with the changes. However, BHP would encourage a review of the BCSI definition to make it more objective in the determination of what is or is not BCSI.

For the TCA definition, BHP is concerned that by removing the removable media section it could create confusion regarding the classification of removable media as a TCA.

In the "Cyber Assets" definition, BHP recommends expanding the exclusion of SCI

In the Intermediate System definition, BHP believes clarification is needed for the removal of "The Intermediate System must not be located inside the Electronic Security Perimeter".

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

Request clarification. Does the SDT intend CIP-008 Reportable Cyber Incident to include SCI but not PCA?

Likes 0

Dislikes 0

Response

Donald Lock - Talen Generation, LLC - 5

Answer No

Document Name

Comment

The sea change being attempted in NERC's CIP definitions makes the success of the virtualization initiative highly dependent on clear communications, making significantly expanded explanations (with examples) appropriate, including clarifying that the new term, "Shared Cyber Infrastructure," applies to hypervisors and not GO-TO communications systems

Likes 0

Dislikes 0

Response

JT Kuehne - AEP - 6

Answer No

Document Name

Comment

AEP does not support the proposed definitions of the following terms and offers suggestions below:

- Electronic Access Point (EAP): The existing definition of EAP describes the access point as "on an ESP". The proposed definition of EAP expands the definition to indicate any Cyber Asset interface that controls routable communication, and not just the one on the ESP interface. This could lead to the expectation of designating multiple inline EAPs (where multiple devices that control routable communication exist in series). AEP recommends adding additional language "*on an Electronic Security Perimeter*" from the existing definition to the proposed definition. As such, the revised definition should read "*An electronic policy enforcement point or a Cyber Asset interface on an Electronic Security Perimeter that controls routable communication to and from a BES Cyber System.*"
- External Routable Connectivity (ERC) – See response to Question #3 above

- Electronic Security Perimeter (ESP) – See response to Question #2 above
- Interactive Remote Access (IRA) – See response to Question #4 above
- Intermediate Systems – Upon review of proposed new Requirement 2.6 in CIP-005-8, we believe the new requirement is not clear, and recommend SDT to consider keeping the existing definition and eliminate CIP-005-8 R2.6.
- Management Interface – AEP recommends SDT to further define “touch panel” in its definition. For example, one may consider touch panel as physical hardware such as on/off switches while another person may consider “touch panel” as a fully developed Human Machine Interface in a logical sense.

Likes 0

Dislikes 0

Response

Dwanique Spiller - Dwanique Spiller On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Berkshire Hathaway - NV Energy - 5 - WECC

Answer

No

Document Name

Comment

Electronic Access Point: NVE does not agree with the revised definition of Electronic Access Point, specifically with the term “to and from a BES Cyber System.” This could result in every BES Cyber System being considered an EAP, with additional requirements of an EAP. Suggest using second part of the existing definition: An electronic policy enforcement point or a Cyber Asset interface that controls routable communication between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter.”

Protected Cyber Asset: NVE does not agree with the revised definition of PCA because it is contradictory to the new definition of Shared Cyber Infrastructure. The second bullet in the PCA definition states it is a “Cyber Asset or Virtual Cyber Asset that shares CPU or memory with any part of the BES Cyber System...” This description seems to elevate the PCA to the higher watermark level of the BCA, and also seems to fit the definition of SCI. Suggest deleting the second bullet in the PCA definition.

Likes 0

Dislikes 0

Response

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

Answer

No

Document Name

Comment

The modified term Transient Cyber Asset (TCA) is not consistent with the new term VCA. The standards treat a VCA as an independent Cyber Asset in inventory and not as software. The removal of the following statement is suggested“Virtual machines hosted on a physical TCA are treated as software on that physical TCA.”, instead modifying the definition of VCA to also include that TCA may host a VCA.

Likes 0

Dislikes 0

Response

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

Answer No

Document Name

Comment

AZPS agrees with a majority of the modified glossary terms, but has questions regarding:

TCA Definition - How is a VCA that's a TCA work? Circular definition, can this be clarified or additional guidance provided in technical guidance?

Likes 0

Dislikes 0

Response

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

Answer No

Document Name

Comment

- Please add acronyms to all CIP definitions to aid in documentation alignment.
- **Management Interface (MI) New Definition**

Configures an Electronic Security Perimeter should also include Electronic Access Points and Access Control Lists. Recommend: "Configures an Electronic Security Perimeter(s), Electronic Access Point(s), Access Control List(s) or configurations for physical and logical networks." 3. Please add the acronym of (MI) to Management Interface to allow Entities to apply to documentation. Does Management Interface (MI) include a Bluetooth configuration interface by a tablet or smartphone on an SCI that is capable of rebooting the SCI or uploading new Firmware to the SCI that may impact the SCI and/or container VCAs or configurations?

Likes 0

Dislikes 0

Response

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

Answer No

Document Name

Comment

Reclamation recommends the Transient Cyber Asset (TCA) definition should include examples of Virtual Cyber Assets that may be considered TCAs.

Likes 0

Dislikes 0

Response

Joseph Amato - Joseph Amato On Behalf of: Darnez Gresham, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Joseph Amato

Answer

No

Document Name

Comment

Electronic Access Point: BHE does not agree with the revised definition of Electronic Access Point, specifically with the term “to and from a BES Cyber System.” This could result in every BES Cyber System being considered an EAP, with additional requirements of an EAP. Suggest using second part of the existing definition: An electronic policy enforcement point or a Cyber Asset interface that controls routable communication between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter.”

Protected Cyber Asset: BHE does not agree with the revised definition of PCA because it is contradictory to the new definition of Shared Cyber Infrastructure. The second bullet in the PCA definition states it is a “Cyber Asset or Virtual Cyber Asset that shares CPU or memory with any part of the BES Cyber System...” This description seems to elevate the PCA to the higher watermark level of the BCA, and also seems to fit the definition of SCI. Suggest deleting the second bullet in the PCA definition.

Likes 0

Dislikes 0

Response

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

Answer

No

Document Name

Comment

PCA definition - CHPD firmly believes there still has been no demonstrated risk of hardware-based virtualization attacks that warrant this definition or requirement. CISA's [Known Exploited Vulnerabilities Catalog | CISA](#) only lists a single VM escape vulnerability, which was patched before it was disclosed, and is disputed by the vendor as being in the wild. While a number of VM escape techniques have been disclosed, all have been patched and saw no confirmed exploitation in the wild.

Even speculative execution vulnerabilities like Spectre and Meltdown have not seen any confirmed exploitation in the wild and are effectively patched. Future vulnerabilities can be effectively managed by a Responsible Entity's CIP-007 R2 patching program (or mitigated by a mitigation plan if patching is not possible) and CIP-010 R3 Vulnerability Assessment program. This requirement only serves to restrict entities on architectures and to increase the cost of virtualization to make it untenable.

We can also look to NIST 800-125A, Security Recommendations for Server-based Hypervisor Platforms. While VM Process Isolation is considered the first and possibly most important of the baseline functions, preventing VMs from sharing CPU or memory is not listed as any of the security recommendations to secure hypervisor baseline functions.

Looking to the technical aspects, this 'requirement' abuses the functionality of DRS (or similar for non-VMware vendors) in ways that were not intended. DRS affinity rules were not intended as a cyber security tool to prevent side channel attacks, but are intended to ensure availability and performance of VMs, as DRS is fundamentally a tool to allocate distributed resources. There are typically three types of rules; VM-to-VM affinity rules which ensure VM stay together for performance reasons, VM-to-VM anti-affinity rules which ensure that VMs stay apart for redundancy reasons incase a host fails, and VM-to-host rules, which ensure that VMs either stay connected to a specific physical resource. Since DRS rulesets were not intended for security, affinity rules do not generally allow you to specify groups of VMs and cannot share CPU with another group of VMs. That means, for example, an EACMS VM would need to have a rule for every VM that it cannot share CPU and memory with it to comply with this requirement. On an infrastructure that hosts both EACMS and non-CIP devices, this could result in hundreds of DRS rules. If a Responsible Entity were to do this, this would create a massive web of affinity rules that would be unmanageable and potentially create a reliability issue in the event of a hardware failure, where critical VMs might not be able to find a suitable host to run on given affinity restrictions.

Likes 0

Dislikes 0

Response

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

Answer No

Document Name

Comment

Electronic Access Point: BHE does not agree with the revised definition of Electronic Access Point, specifically with the term "to and from a BES Cyber System." This could result in every BES Cyber System being considered an EAP, with additional requirements of an EAP. Suggest using second part of the existing definition: An electronic policy enforcement point or a Cyber Asset interface that controls routable communication between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter."

Protected Cyber Asset: BHE does not agree with the revised definition of PCA because it is contradictory to the new definition of Shared Cyber Infrastructure. The second bullet in the PCA definition states it is a "Cyber Asset or Virtual Cyber Asset that shares CPU or memory with any part of the BES Cyber System..." This description seems to elevate the PCA to the higher watermark level of the BCA, and also seems to fit the definition of SCI. Suggest deleting the second bullet in the PCA definition.

Likes 0

Dislikes 0

Response

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

Answer No

Document Name

Comment

Definitions such as VCA is not clear and confusing.

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).

Likes 0

Dislikes 0

Response

George Brown - Acciona Energy North America - 5

Answer

No

Document Name

Comment

Acciona Energy supports Midwest Reliability Organization's (MRO) NERC Standards Review Forum's (NSRF) comments on this question.

Likes 0

Dislikes 0

Response

Joni Jones - Wabash Valley Power Association - 1

Answer

No

Document Name

Comment

Definition of TCA: In a VDI based environment, it will be common for VCAs to not be connected for 30 consecutive days. Example, A VDI based operator workstation may only be online for one shift. Under the definition, this could be considered by a entity as a TCA not included in a BES Cyber System. Consider the impact of the definition in this environment for both full function operator workstations and read only operator workstations.

Likes 0

Dislikes 0

Response

Ryan Strom - Buckeye Power, Inc. - 5

Answer

No

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

PCA – EEI supports the proposed modified glossary terms but asks for clarification regarding the phrase “prior to the introduction to an ESP” with the second bullet. Additionally, we offer suggested bolded minor edits to the balance of the definition:

Are protected by an ESP but are not part of the highest impact BES Cyber System protected by the same ESP; or

A shared CPU or memory within any part of the BCS, excluding Virtual Cyber Assets that are being actively remediated prior to introduction to an ESP.

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 EEI's suggestion on clarifying the phrase in PCA; "prior to the introduction to an ESP" and their suggested edits to the phrase.

Likes 0

Dislikes 0

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

Answer

Yes

Document Name

Comment

Although we agree with the glossary term changes, there needs to be a separate ballot for definition changes in the future.

Likes 0

Dislikes 0

Response**patricia ireland - DTE Energy - 4**

Answer

Yes

Document Name

Comment

Patty Ireland on behalf of DTE Energy, Segments 3 and 4

Likes 0

Dislikes 0

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

Answer

Yes

Document Name

Comment

CEHE agrees with the proposed definitions.

Likes 0

Dislikes 0

Response

Ellese Murphy - Duke Energy - 1,3,5,6 - SERC,RF

Answer

Yes

Document Name

Comment

We agree with the proposed changes.

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

WECC supports the proposed revisions to the terms, but has a question for consideration.

In the Protected Cyber Asset definition was it the intent of the SDT to negate the language 'highest rated' in the second bullet of the definition considering it is included in the first bullet of the definition?

Likes 0

Dislikes 0

Response

Scott Kinney - Avista - Avista Corporation - 3

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

Justin MacDonald - Midwest Energy, Inc. - 1

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

James Baldwin - Lower Colorado River Authority - 1

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

David Jendras - Ameren - Ameren Services - 3

Answer Yes

Document Name

Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Hien Ho - Tacoma Public Utilities (Tacoma, WA) - 4

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Bryan Koyle - Southern Indiana Gas and Electric Co. - 3,5,6 - RF

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Josh Johnson - Lincoln Electric System - 1

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Mike Marshall - IDACORP - Idaho Power Company - 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

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Patricia Lynch - NRG - NRG Energy, 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

Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,5 - RF

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Kinte Whitehead - Exelon - 3

Answer

Document Name

Comment

Exelon will align with EEI in response to this question.

Likes 0

Dislikes 0

Response

Daniel Gacek - Exelon - 1

Answer

Document Name

Comment

Exelon will align with EEI in response to this question.

Likes 0

Dislikes 0

Response

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

Answer

Document Name

Comment

SDG&E Supports EEI's Comments on this question.

Likes 0

Dislikes 0

Response

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

Joni Jones - Wabash Valley Power Association - 1

Answer No

Document Name

Comment

In 1.2, The phrase “through and ESP” should be written “through an EAP”. An EAP is the policy enforcement point or interface, not the ESP.

In 2.4. Would a SAN vendor that provides continuing monitoring using data pushed from the SAN with no inbound capability be classified as a vendor remote access session. Industry clarity is needed associated with this requirement

In the applicability section of 2.6, spell out the applicability for the requirement rather than referencing a separate requirement. Language needs to say EAP, not ESP. An EAP is the policy enforcement point or interface, not the ESP.

Likes 0

Dislikes 0

Response

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

Answer No

Document Name

Comment

Please provide the technical guidelines within the standard document. Can NERC provide an example of what an authenticated vendor initiated remote connection is? What is the definition of an authenticated vendor initiated remote connection?

Likes 0

Dislikes 0

Response

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

Answer No

Document Name

Comment

Definitions such as SCI is not clear and confusing.

Likes 0

Dislikes 0

Response

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

Answer No

Document Name

Comment

For 2.1, change to: "Permit Interactive Remote Access (IRA) only through an Intermediate System." (Delete "authorized" and "if any.") The term "authorized" could be interpreted by auditors to mean that authorization evidence just for the IRA is required for each person having IRA, which we don't believe was the SDT's intent. "if any" is not needed.

Likes 0

Dislikes 0

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer No

Document Name

Comment

The effective language in the currently approved CIP-005-6 R1.3 has been moved to CIP-005 R1.2. In this move the applicability column has removed EAPs for medium/high impact BCS to being directly applicable to high/medium impact BCS with ERC and their associated PCAs. Texas RE recommends this requirement to remain applicable to the EAPs of medium/high impact BCS.

Texas RE is concerned that the Part 1.4 addresses confidentiality, but excludes integrity from the compliance examples provided. Texas RE notes that there are attacks that involve re-writing ciphertext to alter the contents of the encrypted message/file. The attacker will not be able to gain access to the contents of the message/file, however they will have successfully compromised the integrity of the file/message by altering the eventual output once the message/file is decrypted by the intended audience. Encryption does not provide integrity assurance unless it is accompanied by an integrity control, such as GCM (Galois/Counter Mode).

Texas RE understands this to mean that an entity securing communications with AES-256 would be noncompliant with CIP-005 R1.4 and CIP-005 R2.2 as written, as they would have implemented an encryption control but would not have implemented an integrity control.

An entity securing communications with AES-GCM would be compliant, as both encryption and integrity are addressed via AES-GCM. Is this the SDT's intent? Texas RE recommends it could be clearer by adding an example of an integrity control along with the example of encryption as the confidentiality control to clarify that both confidentiality and integrity are necessary CIP-005 compliance elements.

Likes 0

Dislikes 0

Response

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

Answer

No

Document Name

Comment

CHPD agrees with the proposed changes to CIP-005 Requirement R1, however, CHPD does not agree with the proposed changes to Requirement R2 and have identified areas of concern.

Requirement R2.6 as written is not possible to comply with in regards to SCI. SCI are not ESP assets, but R2.6 requires IRA to pass through the ESP. Secondly, often times the hypervisors and management interface will reside on the same network. It is therefore not possible to isolate those devices from each other to prevent IRA from one to another. CHPD recommends removing R2.6 in its entirety.

CHPD appreciates the SDT's efforts and believes the SDT is moving in the right direction however additional modifications are needed. As it is currently proposed, the definition remains cumbersome with the extra language needed to support SCI, which does not need to be within an ESP. Additionally, because Active Directory and the multi-factor authentication systems are part of the scheme to restrict access to IRA, they implicitly become Intermediate Systems, which is undesirable. CHPD suggests the following revisions:

IRA - User-initiated interactive access by a person from one Cyber Asset or Virtual Cyber Asset to another.

This makes IRA exist everywhere where any access from one (Virtual) Cyber Asset to another (Virtual) Cyber Asset is IRA. We scope what IRA is to be protected in the requirement, not in the definition.

Intermediate System - One or more Electronic Access Control or Monitoring Systems that are used to perform Interactive Remote Access to another Cyber Asset or Virtual Cyber Asset.

The requirement that the Intermediate System be outside the ESP is below in CIP-005 R2.1. As stated previously, Interactive Remote Access and Intermediate System exist but there are currently no requirements on them.

CIP-005 R2.1

Applicable Systems:

High Impact BCS and their associated:

- PCA; or
- SCI

Medium Impact BCS and their associated:

- PCA; or

- SCI

Requirement:

Permit IRA, if any, only from:

- A Cyber Asset or Virtual Cyber Asset within a Responsible Entity's ESP;
- SCI; or
- An Intermediate System outside any ESP

This scopes the requirement to only allow IRA connecting to Applicable Systems from a system protected by the ESP or from the Intermediate System outside the ESP. This also catches serial communications, since IRA is completely agnostic to communication protocol. If a device can connect to a BCA via serial, then it is IRA and that connection is only permitted if the source device is inside the ESP or if it is an Intermediate System.

CIP-005 R2.2

Applicable Systems:

Intermediate Systems used to access Applicable System of Part 2.1

Requirement:

Protect the Confidentiality and Integrity of all IRA connecting to the Intermediate System.

CHPD recommends the following rewording, which puts the verb first.

CIP-007 R2.3

Applicable Systems:

Intermediate Systems used to access Applicable System of Part 2.1

Requirement:

Require multi-factor authentication for all IRA connecting to the Intermediate System.

This is a minor change, as it would technically allow a connection from the Intermediate System to the ESP without MFA if one logs in locally to the Intermediate System. However, this does not seem to be a problem, the Intermediate System is required to be within the Physical Security Perimeter, so it is protected by that layer of protection.

CHPD does not have any comments regarding R2.4 through R2.5 as they are not impacted to the suggested change to IRA. As stated above, R2.6 should be deleted as it is covered by R2.1 now.

Likes 0

Dislikes 0

Response

Joseph Amato - Joseph Amato On Behalf of: Darnez Gresham, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Joseph Amato

Answer

No

Document Name	
Comment	
For 2.1, change to: "Permit Interactive Remote Access (IRA) only through an Intermediate System." (Delete "authorized" and "if any.") The term "authorized" could be interpreted by auditors to mean that authorization evidence just for the IRA is required for each person having IRA, which we don't believe was the SDT's intent. "if any" is not needed.	
Likes	0
Dislikes	0
Response	
Justin Welty - NextEra Energy - Florida Power and Light Co. - 6	
Answer	No
Document Name	
Comment	
<ul style="list-style-type: none"> • NEE Supports NPCC comments: • Request clarification of the combination of 1) the definition of Management Interface and 2) CIP-005 R1 Part 1.3 Requirement. That Requirement says, "Permit only needed routable protocol communications to and from Management Interfaces, and deny all other routable protocol communications, per system capability." This combination implies new CIP-002 categorizations for assets with SCI and/or Management Interface. If this conclusion is not correct, please explain why this conclusion is incorrect. If this conclusion is correct, should CIP-002 explicitly state this Requirement? • Request an update to the Requirement for Part 1.4. The first bullet says, "Confidentiality and integrity controls (such as encryption), or." Requirement should what to accomplish. Measures should be how to accomplish. Requirements should be technically agnostic. We recommend moving encryption to these Measures. • Request an update to the Requirement for Part 2.2. The first bullet says, "For all Interactive Remote Access IRA, protect the confidentiality and integrity (e.g., encryption) of communications between the initiating Cyber Asset or Virtual Cyber Asset and the Intermediate System." Requirement should what to accomplish. Measures should be how to accomplish. Requirements should be technically agnostic. We recommend moving encryption to these Measures. • Request clarification between Parts 2.1 and 2.2. Part 2.1 begins with "permit authorized Interactive Remote Access." Part 2.2 begins with "for all IRA." We suggest they should share the same beginning. 	
Likes	0
Dislikes	0
Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	No

Document Name	
Comment	
<p>Manitoba Hydro agrees with the direction of the SDT to leave existing requiremts intact and add additional requirements to support SCI. The addition of a requirement to restrict routable communication access to management interfaces of SCI and EACMS that enforce an ESP is a sound security practice. The standard should leave open the option of creating an out of band management zone so that routable protocol access can be restricted for a group of Cyber Assets instead of requiring this be administered for every single Cyber Asset. This would also remove the per system capability restriction. The following wording is proposed:</p> <p>Permit only needed routable protocol communications to and from Management Interfaces, and deny all other routable protocol communications OR permit only needed routable protocol communication through a logical border surrounding a network to which only EACMS or SCI are connected and deny all other routable protocol communication.</p> <p>The scope of applicable systems for part 2.4 and 2.5 is unclear for SCI, it would seem to leave a gap where the requirement is NOT applicable to vendor remote access to SCI located in an ESP if there is no vendor remote access to BCS. Manitoba Hydro suggest the wording match part 2.1</p> <p>High Impact BCS and their associated:</p> <ul style="list-style-type: none"> PCA <p>Medium Impact BCS and their associated :</p> <ul style="list-style-type: none"> PCA <p>SCI supporting an Applicable System in this Part</p> <p>To limit the scope to system where vendor remote access has been implemented, the following wording is suggested:</p> <p>Where vendor remote access is implemented, have one or more methods for determining active vendor remote access sessions (including IRA and system-to-system remote access).</p>	
Likes	0
Dislikes	0
Response	
<p>Dwanique Spiller - Dwanique Spiller On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Berkshire Hathaway - NV Energy - 5 - WECC</p>	
Answer	No
Document Name	
Comment	
<p>For 2.1, change to: "Permit Interactive Remote Access (IRA) only through an Intermediate System." (Delete "authorized" and "if any.") The term "authorized" could be interpreted by auditors to mean that authorization evidence just for the IRA is required for each person having IRA, which we don't believe was the SDT's intent. "if any" is not needed.</p>	
Likes	0

Dislikes 0

Response

JT Kuehne - AEP - 6

Answer

No

Document Name

Comment

While AEP agrees with most of the proposed revisions in CIP-005-8, the new Requirement R2 Part 2.6 may not be sufficiently clear where it specifies that communications must be **through an ESP** (i.e., “*Routable protocol communications between Intermediate Systems and Applicable Systems of Part 2.1 must be through an ESP.*”). AEP recommends SDT to consider keeping the existing definition of “Intermediate Systems” unchanged and eliminating proposed CIP-005-8 R2.6.

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

Request clarification of the combination of 1) the definition of Management Interface and 2) CIP-005 R1 Part 1.3 Requirement. That Requirement says, “Permit only needed routable protocol communications to and from Management Interfaces, and deny all other routable protocol communications, per system capability.” This combination implies new CIP-002 categorizations for assets with SCI and/or Management Interface. If this conclusion is not correct, please explain why this conclusion is incorrect. If this conclusion is correct, should CIP-002 explicitly state this Requirement?

Recommend an update to the Requirement for CIP-005 Part 1.4. The first bullet says, “Confidentiality and integrity controls (such as encryption), or.” Requirement should what to accomplish. Measures should be how to accomplish. Requirements should be technically agnostic. We recommend moving encryption to these Measures.

Recommend an update to the Requirement for CIP-005 Part 2.2. The first bullet says, “For all Interactive Remote Access IRA, protect the confidentiality and integrity (e.g., encryption) of communications between the initiating Cyber Asset or Virtual Cyber Asset and the Intermediate System.” Requirement should what to accomplish. Measures should be how to accomplish. Requirements should be technically agnostic. We recommend moving encryption to these Measures.

Request clarification between CIP-005 Parts 2.1 and 2.2. Part 2.1 begins with “permit authorized Interactive Remote Access.” Part 2.2 begins with “for all IRA.” We suggest they should share the same beginning.

Likes 0

Dislikes 0

Response

Hien Ho - Tacoma Public Utilities (Tacoma, WA) - 4

Answer No

Document Name

Comment

Tacoma Power suggests moving the proposed CIP-005-7 R1 Part 1.4 (Super ESP Control) to 1.6 to maintain the current numbering of the Dial-up (CIP-005-7 R1.4) & malicious communication (CIP-005-7 R1.5) controls. Additionally, Tacoma Power is concerned with the proposed R1 Part 1.4 language and the inclusion of PSPs. By including PSPs, CIP-005 now relies on physical boundaries within what was previously a Standard which required only logical boundaries. Tacoma Power suggests reinstating a modification version of CIP-006 R1 Part 1.10 to exclude the Super ESP concepts, and include only those within CIP-005, referring to more than one geographical location to reflect the language of Exemption 4.2.3.3.

Suggested CIP-006 R1.10 modification:

“Restrict physical access to cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same geographic location and Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter.”

Suggested CIP-005 R1 Part 1.4 (or 1.6 if moved) modification:

“Protect the data traversing communication networks and data communication links used in extending an ESP to one or more geographic locations through the use of confidentiality and integrity controls (such as encryption), Excluding...”

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 CIP-005 R1.2 it is not clear on the use of the phrase "through the ESP"? Use of the term "through" could imply a requirement to perform intra-ESP electronic access controls when the intent is to apply electronic access controls to routable protocol network traffic entering and leaving the ESP. Suggest the SDT consider the language used in R1.6 (entering or leaving an ESP). As EAP acts as a policy enforcement point, should the language referene an EAP instead of an ESP here?

BC Hydro requests clarity on the use of the above referenced terms with pertinent examples as appropriate.

Likes 0

Dislikes 0

Response

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

Answer

No

Document Name

Comment

NST notes there is no explicit requirement to protect an SCI with an ESP in R1, while it is clearly implied in R2. This inconsistency should be addressed. NST believes the use of the word, "through" in R1.2 is inappropriate and that "through the ESP" should be replaced with "through an ESP boundary or access point" (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'").

Likes 0

Dislikes 0

Response

Carl Pineault - Hydro-Qu?bec Production - 5

Answer

No

Document Name

Comment

Request clarification of the combination of 1) the definition of Management Interface and 2) CIP-005 R1 Part 1.3 Requirement. That Requirement says, "Permit only needed routable protocol communications to and from Management Interfaces, and deny all other routable protocol communications, per system capability." This combination implies new CIP-002 categorizations for assets with SCI and/or Management Interface. If this conclusion is not correct, please explain why this conclusion is incorrect. If this conclusion is correct, should CIP-002 explicitly state this Requirement?

Recommend an update to the Requirement for CIP-005 Part 1.4. The first bullet says, "Confidentiality and integrity controls (such as encryption), or." Requirement should what to accomplish. Measures should be how to accomplish. Requirements should be technically agnostic. We recommend moving encryption to these Measures.

Recommend an update to the Requirement for CIP-005 Part 2.2. The first bullet says, "For all Interactive Remote Access IRA, protect the confidentiality and integrity (e.g., encryption) of communications between the initiating Cyber Asset or Virtual Cyber Asset and the Intermediate System." Requirement should what to accomplish. Measures should be how to accomplish. Requirements should be technically agnostic. We recommend moving encryption to these Measures.

Request clarification between CIP-005 Parts 2.1 and 2.2. Part 2.1 begins with “permit authorized Interactive Remote Access.” Part 2.2 begins with “for all IRA.” We suggest they should share the same beginning.

Likes 0

Dislikes 0

Response

William Steiner - Midwest Reliability Organization - 10

Answer

No

Document Name

Comment

- Part 1.3 – The inclusion of ‘per system capability’ with no additional mitigations, could allow an Entity to use implementations that inherently allows unneeded routable protocol communication to and from Management Interfaces. Routable protocol controls to Management Interfaces should be the same as required controls to BCS because of the inherent risk of Management Interfaces. An alternate proposal would be to remove the ‘per system capability’ from CIP-005-8 R1.3, which matches the CIP-005-8 R1.2 controls to a BCS.
- Part 1.5 – The applicable systems are high/medium impact BES Cyber Systems with dial-up and their associated PCAs and supporting SCI. The “with dial-up” qualifier is only applied to the BCS. A PCA or SCI with dial-up connectivity would not be applicable if the associated high/medium impact BCS or supported Applicable System does not have dial-up. An alternate proposal could be to update the “with dial-up” qualifier in the applicable systems column to apply to the intended applicable systems.
- Part 1.6 – Including the ‘Internet Protocol’ qualification in the requirement could inhibit malicious communication detection for future technologies and implementations that may not use a traditional firewall and IP routing. In particular with the change from firewalls as the outer perimeter to a zero-trust implementation, there will likely be more configuration points that aren't also acting as routers, so the inherent protection from non-IP protocols offered by the separation of subnets will no longer be there and other protocols could pass. Furthermore the use of the word ‘or’ between ‘entering’ and ‘leaving’ could allow an entity to only have methods for one direction. Also, SCI and Management Interfaces are not included in the applicable systems. The inherent risk of Management Interfaces should require the same protections as the BCS.
- R2 – The replacement of ‘where technically feasible’ with ‘per system capability’ statement could allow implementations that bypass the controls of an IS, encryption, and/or multi-factor authentication without the additional mitigations that are currently required by a TFE.
- Part 2.3 - The changed language now states 'require multi-factor authentication to the Intermediate System'. Does the 'to' indicate that the authentication has to happen at that IS? The language before was scoped to the IRA session, which allowed for that to occur somewhere along the session. The Technical Rationale says this was intentional to define 'where the requirement for multifactor authentication should be applied'.
 - This could make current implementations noncompliant where multi-factor authentication occurs along the session, but not on the Intermediate System.
- Part 2.4, 3.1, 3.2 – The applicability column qualifier, “with vendor remote access”, is only applied against the BCS, but not the associated PCA or supporting SCI. This could allow SCI with vendor remote access no controls if the supporting BCS does not have vendor remote access. An alternate proposal could be to update the “with vendor remote access” qualifier in the applicable systems column to apply to the intended applicable systems.
- Part 2.6 Similar to the comment in Part 1.6, with the potential move from perimeter-based security to zero-trust, the inherent protections against non-routable protocols provided by the firewall may not necessarily be there. Limiting this to routable protocols, leaves potential for non-routable protocols to access BCAs, etc. from the IS unfettered.
- Part 2.6 requires communications between Intermediate System and SCI go through an ESP, however that is not possible (see reasoning below):

- R1.3 Requires that routable access to SCI Management Interfaces be controlled, but does not require the SCI to be in an ESP. 2.6 requires that access to the SCI from an IS go through an ESP. Definition of ESP, which is dependent upon the definition of EAP – EAP states “controls routable communication to and from a BES Cyber System”. BES Cyber System is one or more BCAs. BCAs by definition exclude SCI. Intermediate Systems cannot be inside and therefore cannot be a BCA. Therefore communication between an Intermediate System and SCI cannot go through an ESP.
- Part 2.6 – The rationale states that an Intermediate System that shares CPU/memory with a BCS would then be a PCA by PCA definition. It then states that R1.1 requires that since it is a PCA that it be protected by an ESP. We understand that the conclusions intended by the drafting team is that the IS could then not be a PCA because of Part 2.6 requiring it to go through an ESP to access BCS. However, in the case of many small ESPs, the IS could be a PCA to one BCS, but only access other BCS by going through an ESP. As long as it doesn't access the BCS that made it a PCA, it would be compliant. This could allow an IS that is a VCA to be hosted on the same SCI (hypervisor) as a BCA. An alternate proposal could be to update the requirement to include CPU and Memory affinity controls or update the IS definition to include such CPU and Memory affinity controls.

Likes 0

Dislikes 0

Response

Lindsey Mannion - ReliabilityFirst - 10

Answer

No

Document Name

Comment

There is still a gap between what is system-to-system and what is Interactive Remote Access (IRA) with the new IRA definition. Entities often rely on IRA ports for system-to-system communication but have not adequately enforced protections to ensure that malicious actors do not use the ports – regardless of whether a remote access client is available or used. Additional technical measures or controls should be added to ensure validity of communications to Applicable Systems.

CIP-005 Requirement R1 Part1.3 to protect the confidentiality and integrity of data traversing communication links that span multiple Physical Security Perimeters, but no minimum level of encryption is required which could result in older less secure methods being used leaving the data at risk.

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

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

Further, introducing Shared Cyber Infrastructure (SCI) increases the number of Requirements and Parts that a Responsible Entity needs to track compared to simply identifying the hypervisor and associated hardware and “high-water-marking” them with the highest identified impact rating and creating a BCS. Allowing “mixed-trust” environments within the same SCI (hypervisor) increases the

complexity and management of the environment as the SDT relaxes the “high-water-marking” required to this point (exceptions being EACMS and PACS – but only with the understanding that the hypervisor and associated SCI is protected as an EACMS or PACS).

Finally, there is no NERC definition of “Remediation VLAN” so therefore the Responsible Entity could keep VMs spun up and within the Remediation network for extended periods of time – without the benefit of protections from the other CIP Standards.

Likes 0

Dislikes 0

Response

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name SPP RTO

Answer No

Document Name

Comment

Is the intent at the actual Management Interface itself for R1.3 for communications to and from or can we have a management network that that all of management interfaces are on and control access that way?

Except for the comments regarding the definitions for VCA, SCI, EAP, PCA, and ERC as noted above in Question 1-6, SPP supports the changes the SDT has made to the Requirements for CIP-005.

Likes 0

Dislikes 0

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer No

Document Name

Comment

IESO supports the comments provided by NPCC and IRC

Likes 0

Dislikes 0

Response

Thomas Breene - WEC Energy Group, Inc. - 3

Answer No

Document Name

Comment

We have concerns with the SCI, IRA and Management Interface definitions. These terms are used throughout the Standard.

Likes 0

Dislikes 0

Response

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

Answer No

Document Name

Comment

Request clarification of the combination of 1) the definition of Management Interface and 2) CIP-005 R1 Part 1.3 Requirement. That Requirement says, "Permit only needed routable protocol communications to and from Management Interfaces, and deny all other routable protocol communications, per system capability." This combination implies new CIP-002 categorizations for assets with SCI and/or Management Interface. If this conclusion is not correct, please explain why this conclusion is incorrect. If this conclusion is correct, should CIP-002 explicitly state this Requirement?

Recommend an update to the Requirement for CIP-005 Part 1.4. The first bullet says, "Confidentiality and integrity controls (such as encryption), or." The requirement should be what to accomplish. Measures should be how accomplished. Requirements should be technology agnostic. We recommend moving encryption to these Measures.

Recommend an update to the Requirement for CIP-005 Part 2.2. The first bullet says, "For all Interactive Remote Access IRA, protect the confidentiality and integrity (e.g., encryption) of communications between the initiating Cyber Asset or Virtual Cyber Asset and the Intermediate System." The requirement should be what to accomplish. Measures should be how accomplished. Requirements should be technology agnostic. We recommend moving encryption to these Measures.

Request clarification between CIP-005 Parts 2.1 and 2.2. Part 2.1 begins with "permit authorized Interactive Remote Access." Part 2.2 begins with "for all IRA." We suggest they should share the same beginning.

Likes 0

Dislikes 0

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1

Answer No

Document Name

Comment

We support NPCC TFIST comments.

Request clarification of the combination of 1) the definition of Management Interface and 2) CIP-005 R1 Part 1.3 Requirement. That Requirement says, "Permit only needed routable protocol communications to and from Management Interfaces, and deny all other routable protocol communications, per system capability." This combination implies new CIP-002 categorizations for assets with SCI and/or Management Interface. If this conclusion is not correct, please explain why this conclusion is incorrect. If this conclusion is correct, should CIP-002 explicitly state this Requirement?

Recommend an update to the Requirement for CIP-005 Part 1.4. The first bullet says, “Confidentiality and integrity controls (such as encryption), or.” Requirement should what to accomplish. Measures should be how to accomplish. Requirements should be technically agnostic. We recommend moving encryption to these Measures.

Recommend an update to the Requirement for CIP-005 Part 2.2. The first bullet says, “For all Interactive Remote Access IRA, protect the confidentiality and integrity (e.g., encryption) of communications between the initiating Cyber Asset or Virtual Cyber Asset and the Intermediate System.” Requirement should what to accomplish. Measures should be how to accomplish. Requirements should be technically agnostic. We recommend moving encryption to these Measures.

Request clarification between CIP-005 Parts 2.1 and 2.2. Part 2.1 begins with “permit authorized Interactive Remote Access.” Part 2.2 begins with “for all IRA.” We suggest they should share the same beginning.

Likes 0

Dislikes 0

Response

Glen Farmer - Avista - Avista Corporation - 5

Answer

No

Document Name

Comment

New requirement to deny access to the Management Interface from BCS and associated PCAs (R1.3). – This would require significant effort for us if approved. As written, the proposed changes appear to require significant modification to our current network architecture without clearly indicating even how this can be accomplished in a compliant fashion or how that improves upon the existing security posture.

Likes 0

Dislikes 0

Response

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6

Answer

No

Document Name

Comment

For 2.1, change to: “Permit Interactive Remote Access (IRA) only through an Intermediate System.” (Delete “authorized” and “if any.”) The term “authorized” could be interpreted by auditors to mean that authorization evidence just for the IRA is required for each person having IRA, which we don’t believe was the SDT’s intent. “if any” is not needed.

Likes 0

Dislikes 0

Response

John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1

Answer No

Document Name

Comment

Tacoma Power suggests moving the proposed CIP-005-7 R1 Part 1.4 (Super ESP Control) to 1.6 to maintain the current numbering of the Dial-up (CIP-005-7 R1.4) & malicious communication (CIP-005-7 R1.5) controls.

Additionally, Tacoma Power is concerned with the proposed R1 Part 1.4 language and the inclusion of PSPs. By including PSPs, CIP-005 now relies on physical boundaries within what was previously a Standard which required only logical boundaries. Tacoma Power suggests reinstating a modification version of CIP-006 R1 Part 1.10 to exclude the Super ESP concepts, and include only those within CIP-005, referring to more than one geographical location to reflect the language of Exemption 4.2.3.3.

Suggested CIP-006 R1.10 modification:

“Restrict physical access to cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same geographic location and Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter.”

Suggested CIP-005 R1 Part 1.4 (or 1.6 if moved) modification:

“Protect the data traversing communication networks and data communication links used in extending an ESP to one or more geographic locations through the use of confidentiality and integrity controls (such as encryption),

Excluding...”

Likes 0

Dislikes 0

Response

Mike Magruder - Avista - Avista Corporation - 1

Answer No

Document Name

Comment

New requirement to deny access to the Management Interface from BCS and associated PCAs (R1.3). – This would require significant effort for us if approved. As written, the proposed changes appear to require significant modification to our current network architecture without clearly indicating even how this can be accomplished in a compliant fashion or how that improves upon the existing security posture.

Likes 0

Dislikes 0

Response

Kimberly Turco - Constellation - 6

Answer No

Document Name

Comment

Constellation has elected to align with Exelon in response to this question.

Kim Turco, on behalf of Constellation Segments 5 and 6

Likes 0

Dislikes 0

Response

Alison Mackellar - Constellation - 5

Answer No

Document Name

Comment

Constellation has elected to align with Exelon in response to this question.

Kim Turco, on behalf of Constellation Segments 5 and 6

Likes 0

Dislikes 0

Response

Scott Kinney - Avista - Avista Corporation - 3

Answer No

Document Name

Comment

Comments: New requirement to deny access to the Management Interface from BCS and associated PCAs (R1.3). – This would require significant effort for us if approved. As written, the proposed changes appear to require significant modification to our current network architecture without clearly indicating even how this can be accomplished in a compliant fashion or how that improves upon the existing security posture.

Likes 0

Dislikes 0

Response

George Brown - Acciona Energy North America - 5

Answer

Yes

Document Name

Comment

Acciona Energy supports Midwest Reliability Organization's (MRO) NERC Standards Review Forum's (NSRF) comments on this question.

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

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

Likes 0

Dislikes 0

Response

Josh Johnson - Lincoln Electric System - 1

Answer

Yes

Document Name

Comment

LES agrees with the majority of proposed changes regarding CIP-005 but has concerns with the 'Technical Feasibility' conforming change which is further detailed in the Question 11 response.

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

AZPS agrees with the revised proposed changes to the CIP-005 standard.

Likes 0

Dislikes 0

Response

Ellese Murphy - Duke Energy - 1,3,5,6 - SERC,RF

Answer

Yes

Document Name

Comment

We agree with the proposed changes.

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

CEHE agrees with the proposed revisions in CIP-005.

Likes 0

Dislikes 0

Response

patricia ireland - DTE Energy - 4

Answer Yes

Document Name

Comment

Patty Ireland on behalf of DTE Energy, Segments 3 and 4

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Comments: For Requirement 2 Part 2.1, change the language to read: "Permit Interactive Remote Access (IRA) only through an Intermediate System." (Deleting "authorized" and "if any.") The term "authorized" could be interpreted by auditors to mean that authorization evidence just for the IRA is required for each person having IRA, which we don't believe was the SDT's intent. "if any" is not needed.

Likes 0

Dislikes 0

Response

Maggy Powell - Amazon Web Services - 7

Answer Yes

Document Name

Comment

N/A

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Southern supports the proposed changes to CIP-005.

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

EI supports the proposed changes.

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Request clarification of the combination of 1) the definition of Management Interface and 2) CIP-005 R1 Part 1.3 Requirement. That Requirement says, "Permit only needed routable protocol communications to and from Management Interfaces, and deny all other routable protocol communications, per system capability." This combination implies new CIP-002 categorizations for assets with SCI and/or Management Interface. If this conclusion is not correct, please explain why this conclusion is incorrect. If this conclusion is correct, should CIP-002 explicitly state this Requirement?

Likes 0

Dislikes 0

Response

Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC) 2016-02 Virtualization (Draft 3)

Answer Yes

Document Name

Comment

The SRC agrees with the proposed changes to CIP-005. In particular, SRC agrees with the proposed change to R1.2 from a security objective but finds the exclusion for time-sensitive Protection System traffic questionable. The SRC entities do not generally work with such systems in scope. Additionally, the SRC agrees with the proposed change to R1.3 from a security perspective and believes that this is good practice to restrict access to such management interfaces. The SRC also appreciates the exclusions to prevent situations of double-jeopardy regarding other standards as referenced in R1.4. Furthermore, the SRC finds no concerns with the proposed changes to the remaining CIP-005 sub requirements and believes that the proposed change to R1.6 is consistent with good practice.

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 comments submitted by EEI

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

See EEI comment.

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Alliant Energy supports the comments submitted by the MRO NSRF.

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

For Requirement 2 Part 2.1, change the language to read: "Permit Interactive Remote Access (IRA) only through an Intermediate System." (Deleting "authorized" and "if any.") The term "authorized" could be interpreted by auditors to mean that authorization evidence just for the IRA is required for each person having IRA, which we don't believe was the SDT's intent. "if any" is not needed.

Likes 0

Dislikes 0

Response

Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,5 - RF

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Mike Marshall - IDACORP - Idaho Power Company - 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

Ryan Strom - Buckeye Power, Inc. - 5

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Bryan Koyle - Southern Indiana Gas and Electric Co. - 3,5,6 - RF

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Donald Lock - Talen Generation, LLC - 5

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Jennifer Malon - Jennifer Malon On Behalf of: Brooke Voorhees, Black Hills Corporation, 3, 5, 1, 6; Derek Silbaugh, Black Hills Corporation, 3, 5, 1, 6; Don Stahl, Black Hills Corporation, 3, 5, 1, 6; Seth Nelson, Black Hills Corporation, 3, 5, 1, 6; - Jennifer Malon

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Jesus Sammy Alcaraz - Imperial Irrigation District - 1

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

David Jendras - Ameren - Ameren Services - 3

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

James Baldwin - Lower Colorado River Authority - 1

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

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

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Justin MacDonald - Midwest Energy, Inc. - 1

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

LaTroy Brumfield - American Transmission Company, LLC - 1

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Daniel Gacek - Exelon - 1

Answer

Document Name

Comment

Referencing Part 2.6, if the definition of IRA is changing to potentially include "...that is converted to a non-routable protocol, to a Cyber System not protected by an Electronic Security Perimeter" but the Part 2.6 requirement states that communication between IS and applicable systems must be through an ESP, that complicates this. It's not clear where the ESP would be if the applicable system isn't in an ESP, but where there is routable communication between the IS and the protocol converter. This would potentially lead to some "Creative" network architectures, which provide limited value.

Likes 0

Dislikes 0

Response

Kinte Whitehead - Exelon - 3

Answer

Document Name

Comment

Referencing Part 2.6, if the definition of IRA is changing to potentially include "...that is converted to a non-routable protocol, to a Cyber System not protected by an Electronic Security Perimeter" but the Part 2.6 requirement states that communication between IS and applicable systems must be through an ESP, that complicates this. It's not clear where the ESP would be if the applicable system isn't in an ESP, but where there is routable communication between the IS and the protocol converter. This would potentially lead to some "Creative" network architectures, which provide limited value.

Likes 0

Dislikes 0

Response

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

Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC) 2016-02 Virtualization (Draft 3)

Answer No

Document Name

Comment

The SRC does not agree with several of the key proposed changes to CIP-007. In particular, SRC believes the proposed change will necessitate additional requirements to define accessibility in order to determine what controls are necessary and this may lead to disputes in interpretation. In regards to R1.3, The SRC recommends that SDT modify that requirement to read "by mitigating the risk of sharing CPU resources, show how you detect, deter or prevent risk of shared CPU or memory resources." The SRC believes that, as written, this requirement seems too prescriptive. The SRC agrees with the minor proposed changes to the remaining sub-requirements.

Likes 0

Dislikes 0

Response

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

Answer No

Document Name

Comment

SMUD is not sure why requirements for R1.1 changed or why the measures now include the need to document both port and service instead of logical accessible port or service. From a security objective point of view, there is nothing to gain by changing the requirement or measure here, it's only adding a new layer of confusion based on the new requirement language.

It is not clear how the changes being made are needed to support virtualization. SMUD's recommendation is to leave the requirements as they are unless there is a specific need to address a requirement in support of virtualization technology - this does not appear to be the case.

Likes 0

Dislikes 0

Response

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

Answer No

Document Name	Affinity Rules - Eversource comments.pdf
Comment	
<p>Request clarification of CIP-007, Part 1.3. It appears that applications operating on a SCI platform where memory and CPU hardware devices are shared MUST all be classified at the same impact level. Is this a correct interpretation? If not, please explain. Memory and CPU are both implemented in hardware devices which are naturally shared across multiple processes and system functions. There is no known method to prevent the physical sharing of memory and CPU hardware devices in a virtual platform (SCI) based on the application and operating system processes that share these hardware devices.</p> <p>Request clarification of CIP-007, Part 1.3 since there are two scenarios. In the first scenario there is one SCI for everything - BES Cyber Assets, PCAs, EACMS, PACS, potentially non-CIP VMs. In the second scenario there are two SCIs. The first SCI includes BES Cyber Assets and PCAs (within the ESP). The second SCI includes assets outside the ESP, like EACMS, PACS, potentially non-CIP VMs. These two SCIs do not have the same risk. Should we expect different Requirements for these two SCIs?</p> <p>See attached file for the different scenarios mentioned in the narrative.</p>	
Likes	0
Dislikes	0
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
<p>"System hardening" may belong in CIP-010, R1.3: Does risk regarding memory sharing need to be mitigated or completely eliminated, do you need a dedicated host per asset clarification? R2.2: Need more clarity on the frequency of evaluation (35 days from the source or 35 days from the last evaluation?). R4 and R5: Will TFEs still apply by removing the technical feasibility language and replacing it with per system capability? Applicable Systems needs to be defined.</p>	
Likes	0
Dislikes	0
Response	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	No
Document Name	
Comment	

We support NPCC TFIST comments.

Request clarification of CIP-007, Part 1.3. It appears that applications operating on a SCI platform where memory and CPU hardware devices are shared MUST all be classified at the same impact level. Is this a correct interpretation? If not, please explain. Memory and CPU are both implemented in hardware devices which are naturally shared across multiple processes and system functions. There is no known method to prevent the physical sharing of memory and CPU hardware devices in a virtual platform (SCI) based on the application and operating system processes that share these hardware devices.

Request clarification of CIP-007, Part 1.3 since there are two scenarios. In the first scenario there is one SCI for everything - BES Cyber Assets, PCAs, EACMS, PACS, potentially non-CIP VMs. In the second scenario there are two SCIs. The first SCI includes BES Cyber Assets and PCAs (within the ESP). The second SCI includes assets outside the ESP, like EACMS, PACS, potentially non-CIP VMs. These two SCIs do not have the same risk. Should we expect different Requirements for these two SCIs?

Likes 0

Dislikes 0

Response

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

Answer

No

Document Name

Comment

Request clarification of CIP-007, Part 1.3. It appears that applications operating on an SCI platform where memory and CPU hardware devices are shared MUST all be classified at the same impact level. Is this a correct interpretation? If not, please explain. Memory and CPU are both implemented in hardware devices which are naturally shared across multiple processes and system functions. There is no known method to prevent the physical sharing of memory and CPU hardware devices in a virtual platform (SCI) based on the application and operating system processes that share these hardware devices.

Request clarification of CIP-007, Part 1.3 since there are two scenarios. In the first scenario, there is one SCI for everything - BES Cyber Assets, PCAs, EACMS, PACS, and potentially non-CIP VMs. In the second scenario, there are two SCIs. The first SCI includes BES Cyber Assets and PCAs (within the ESP). The second SCI includes assets outside the ESP, like EACMS, PACS, and potentially non-CIP VMs. These two SCIs do not have the same risk. Should we expect different Requirements for these two SCIs?

Likes 0

Dislikes 0

Response

Thomas Breene - WEC Energy Group, Inc. - 3

Answer

No

Document Name

Comment

We have concerns with the SCI definition and it potentially bringing additional devices into scope. This term is used throughout the Standard. Additionally, the recategorization of R1 from “Ports and Services” to a broader term of “System Hardening” raises potential differences in interpretations during an audit.

Likes 0

Dislikes 0

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer

No

Document Name

Comment

IESO supports the comments provided by NPCC and IRC

Likes 0

Dislikes 0

Response

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name SPP RTO

Answer

No

Document Name

Comment

SPP requests that guidance is needed to define what is meant by “System Hardening.”

Except for the comments regarding the definitions for VCA, SCI, EAP, PCA, and ERC as noted above in Question 1-6, SPP supports the changes the SDT has made to the Requirements for CIP-007.

Likes 0

Dislikes 0

Response

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

Answer

No

Document Name

Comment

If a firewall has VLANs on it for medium and low, or high and low, does that pull low impact network connection into scope because it shares the same firewall? More clarity is needed.

Likes 0

Dislikes 0

Response**William Steiner - Midwest Reliability Organization - 10**

Answer

No

Document Name

Comment

Part 5.1 – The replacement of 'where technically feasible' with 'per system capability' could potentially introduce risk. TFEs require additional mitigations to address the risk posed by not requiring authentication - per system capability does not have this requirement.

Likes 0

Dislikes 0

Response**Carl Pineault - Hydro-Quebec Production - 5**

Answer

No

Document Name

Comment

Request clarification of CIP-007, Part 1.3. It appears that applications operating on a SCI platform where memory and CPU hardware devices are shared MUST all be classified at the same impact level. Is this a correct interpretation? If not, please explain. Memory and CPU are both implemented in hardware devices which are naturally shared across multiple processes and system functions. There is no known method to prevent the physical sharing of memory and CPU hardware devices in a virtual platform (SCI) based on the application and operating system processes that share these hardware devices.

Request clarification of CIP-007, Part 1.3 since there are two scenarios. In the first scenario there is one SCI for everything - BES Cyber Assets, PCAs, EACMS, PACS, potentially non-CIP VMs. In the second scenario there are two SCIs. The first SCI includes BES Cyber Assets and PCAs (within the ESP). The second SCI includes assets outside the ESP, like EACMS, PACS, potentially non-CIP VMs. These two SCIs do not have the same risk. Should we expect different Requirements for these two SCIs?

Likes 0

Dislikes 0

Response

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

Answer No

Document Name

Comment

While NST endorses replacing "where technically feasible" with "per system capability" in R.1.1, we believe the proposed new language in R1.1 ("Disable or prevent unneeded routable protocol network accessibility") subtracts rather than adds clarity, and we therefore recommend retaining the existing and familiar "enable only logical network accessible ports." If the SDT wants to explicitly allow for the use of host-based firewalls or similar, per device controls as an alternative, R1.1 could be modified to say, "enable only logical network accessible ports... or prevent access to unnecessary logical network accessible ports using host-based firewalls or other, per device controls."

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

Request clarification of CIP-007, Part 1.3. It appears that applications operating on a SCI platform where memory and CPU hardware devices are shared MUST all be classified at the same impact level. Is this a correct interpretation? If not, please explain. Memory and CPU are both implemented in hardware devices which are naturally shared across multiple processes and system functions. There is no known method to prevent the physical sharing of memory and CPU hardware devices in a virtual platform (SCI) based on the application and operating system processes that share these hardware devices.

Request clarification of CIP-007, Part 1.3 since there are two scenarios. In the first scenario there is one SCI for everything - BES Cyber Assets, PCAs, EACMS, PACS, potentially non-CIP VMs. In the second scenario there are two SCIs. The first SCI includes BES Cyber Assets and PCAs (within the ESP). The second SCI includes assets outside the ESP, like EACMS, PACS, potentially non-CIP VMs. These two SCIs do not have the same risk. Should we expect different Requirements for these two SCIs?

Likes 0

Dislikes 0

Response

JT Kuehne - AEP - 6

Answer No

Document Name

Comment

While AEP agrees with most of the proposed revisions in CIP-007-7, we recommend adding languages to Requirement R1 Part 1.3 to provide more clarity. Requirement R1 Part 1.3 would then read “Mitigate the risk of CPU or memory vulnerabilities by (1) preventing the sharing of CPU and memory resources between VCAs or (2) **protecting all VCA on SCI with the highest impact BCS rating that are not of, or associated with, the same impact categorization.**”

Likes 0

Dislikes 0

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

No

Document Name**Comment**

- NEE supports the NPCC Comments:
- Request clarification of CIP-007, Part 1.3. It appears that applications operating on a SCI platform where memory and CPU hardware devices are shared MUST all be classified at the same impact level. Is this a correct interpretation? If not, please explain. Memory and CPU are both implemented in hardware devices which are naturally shared across multiple processes and system functions. There is no known method to prevent the physical sharing of memory and CPU hardware devices in a virtual platform (SCI) based on the application and operating system processes that share these hardware devices.
- Request clarification of CIP-007, Part 1.3 since there are two scenarios. In the first scenario there is one SCI for everything - BES Cyber Assets, PCAs, EACMS, PACS, potentially non-CIP VMs. In the second scenario there are two SCIs. The first SCI includes BES Cyber Assets and PCAs (within the ESP). The second SCI includes assets outside the ESP, like EACMS, PACS, potentially non-CIP VMs. These two SCIs do not have the same risk. Should we expect different Requirements for these two SCIs?

Likes 0

Dislikes 0

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

No

Document Name**Comment**

CHPD agrees with the proposed changes to Requirement R1.1 however, CHPD does not agree with the proposed changes to Requirement R1.3.

Regarding Requirement R1.3, CHPD firmly believes there has been no demonstrated risk of hardware-based virtualization attacks that warrant this requirement. CISA's [Known Exploited Vulnerabilities Catalog | CISA](#) only lists a single VM escape vulnerability, which was patched before it was disclosed, and is disputed by the vendor as being in the wild. While a number of VM escape techniques have been disclosed, all have been patched and saw no confirmed exploitation in the wild.

Even speculative execution vulnerabilities like Spectre and Meltdown have not seen any confirmed exploitation in the wild and are effectively patched. Future vulnerabilities can be effectively managed by a Responsible Entity's CIP-007 R2 patching program (or mitigated by a mitigation plan if patching is not possible) and CIP-010 R3 Vulnerability Assessment program. This requirement only serves to restrict entities on architectures and to increase the cost of virtualization which would make it untenable.

We can also look to NIST 800-125A, Security Recommendations for Server-based Hypervisor Platforms. While VM Process Isolation is considered the first and possibly most important of the baseline functions, preventing VMs from sharing CPU or memory is not listed as any of the security recommendations to secure hypervisor baseline functions.

Looking to the technical aspects, this requirement misuses the functionality of DRS (or similar for non-VMware vendors) in ways that were not intended. DRS affinity rules were not intended as a cyber security tool to prevent side channel attacks, but are intended to ensure availability and performance of VMs, as DRS is fundamentally a tool to allocate distributed resources. There are typically three types of rules; VM-to-VM affinity rules which ensure VM stay together for performance reasons, VM-to-VM anti-affinity rules which ensure that VMs stay apart for redundancy reasons in case a host fails, and VM-to-host rules, which ensure that VMs either stay connected to a specific physical resource. Because DRS rulesets were not intended for security, affinity rules do not generally allow you to specify groups of VMs and cannot share CPU with another group of VMs. That means, for example, an EACMS VM would need to have a rule for every VM that it cannot share CPU and memory with to comply with this requirement. If a Responsible Entity were to do this, this would create a massive web of affinity rules that would be unmanageable and potentially create a reliability issue in the event of a hardware failure, where critical VMs might not be able to find a suitable host to run on given affinity restrictions.

Setting aside the security and technical problems, the requirement itself is not clear in what it allows. It is possible to interpret the requirement as contradicting the definition of SCI. There is a very fine line drawn with the terminology in the definition of SCI ("cluster") and the wording of CIP-007 R1.3 (sharing of CPU and memory). Some might interpret the specific hosts allowed to host CIP devices (according to the affinity ruleset) as the "cluster", meaning that R1.3 essentially contradicts the definition of SCI. There is also the question of if a high watermarked BCA still counts as its Medium Impact self. Even though you must treat it as a high impact PCA, it is still fundamentally a medium impact BCA and according to the requirement, it cannot coexist on the same CPU and memory as it is of a different impact classification. The language of R1.3 combined with the definition of SCI creates too vague of a security control to implement without significant compliance risk.

Likes 0

Dislikes 0

Response

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

Answer

No

Document Name

Comment

Definitions such as VCA is not clear and confusing.

Likes 0

Dislikes 0

Response

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

Answer No

Document Name

Comment

Please provide the technical guidelines within the standard document. SRP feels they are necessary to understand this requirement in more detail. Regarding R1.3 please clarify the expectation around not sharing CPU and Memory and it still be SCI and definition for SCI. What role does storage play?

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

For Requirement R1.3, consider if there is a better verb than “preventing” when discussing mitigation of risk (in order to avoid potential overly prescriptive interpretations and enforcement).

Further, we are concerned about the last phrase in Requirement R1.3, “between VCAs that are not of, or associated with, the same impact categorization.” We question whether this phrase is needed in the requirement language and, if included, whether it could force Entities to “cluster” virtual assets by impact level (high, medium, low) which would be inefficient. We are supportive of operating to the “high water” level; we are simply concerned about the categorization level. We recommend re-wording the proposed requirement text to read, “Mitigate the risk of CPU or memory vulnerabilities by preventing the sharing of CPU and memory resources between unassociated VCAs that are not of, or associated with, the same SCI (clustered configuration).” [changes underlined]

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Alliant Energy supports the comments submitted by the MRO NSRF.

Likes 0

Dislikes 0

Response

Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirschak, 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

See EEI comment.

Likes 0

Dislikes 0

Response

Alison Mackellar - Constellation - 5

Answer

Yes

Document Name

Comment

Constellation has elected to align with Exelon in response to this question.

Kim Turco, on behalf of Constellation Segments 5 and 6

Likes 0

Dislikes 0

Response

Kimberly Turco - Constellation - 6

Answer

Yes

Document Name

Comment

Constellation has elected to align with Exelon in response to this question.

Kim Turco, on behalf of Constellation Segments 5 and 6

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 comments submitted by EEI

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

Request clarification of CIP-007, Part 1.3 since there are two scenarios. In the first scenario there is one SCI for everything - BES Cyber Assets, PCAs, EACMS, PACS, potentially non-CIP VMs. In the second scenario there are two SCIs. The first SCI includes BES Cyber Assets and PCAs (within the ESP). The second SCI includes assets outside the ESP, like EACMS, PACS, potentially non-CIP VMs. These two SCIs do not have the same risk. Should we expect different Requirements for these two SCIs?

Likes 0

Dislikes 0

Response

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

Answer	Yes
Document Name	
Comment	
EEl supports the proposed 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 supports the proposed changes to CIP-007.	
Likes 0	
Dislikes 0	
Response	
Maggy Powell - Amazon Web Services - 7	
Answer	Yes
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	

Comment

Comments: For Requirement R1.3, consider if there is a better verb than “preventing” when discussing mitigation of risk (in order to avoid potential overly prescriptive interpretations and enforcement).

Further, we are concerned about the last phrase in Requirement R1.3, “between VCAs that are not of, or associated with, the same impact categorization.” We question whether this phrase is needed in the requirement language and, if included, whether it could force Entities to “cluster” virtual assets by impact level (high, medium, low) which would be inefficient. We are supportive of operating to the “high water” level; we are simply concerned about the categorization level.

It is our understanding that if everything in an asset is operated or associated at the same impact level, then the asset does not meet the proposed definition of SCI. It is also our understanding that the proposed Requirement 1 Part 1.3 is intended to be backwards-compatible and to not require that present-day compliant network architecture change. However, we were not clear on these points just from reading the proposed revised text alone. We urge the SDT to issue additional clarity on these points, either through documented technical guidance or even clarifying changes to the proposed requirement text itself.

Likes	0
-------	---

Dislikes	0
----------	---

Response**patricia ireland - DTE Energy - 4****Answer**

Yes

Document Name**Comment**

Patty Ireland on behalf of DTE Energy, Segments 3 and 4

Likes	0
-------	---

Dislikes	0
----------	---

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

Yes

Document Name**Comment**

CEHE agrees with the proposed revisions in CIP-007.

Likes	0
-------	---

Dislikes	0
----------	---

Response

Ellese Murphy - Duke Energy - 1,3,5,6 - SERC,RF

Answer Yes

Document Name

Comment

While we agree with the changes as a whole, consider clarifying what memory means in CIP-007 R1.3. Does memory refer to RAM?

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

AZPS agrees with the revised proposed changes to the CIP-007 standard.

Likes 0

Dislikes 0

Response

Josh Johnson - Lincoln Electric System - 1

Answer Yes

Document Name

Comment

LES agrees with the majority of proposed changes regarding CIP-007 but has concerns with the 'Technical Feasibility' conforming change which is further detailed in the Question 11 response.

Likes 0

Dislikes 0

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer Yes

Document Name

Comment

Texas RE recommends removing the language “Mitigate the risk of CPU or memory vulnerabilities” in CIP-007 Part 1.3 as it is more appropriate for Technical Rationale.

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

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

Likes 0

Dislikes 0

Response

George Brown - Acciona Energy North America - 5

Answer Yes

Document Name

Comment

Acciona Energy supports Midwest Reliability Organization’s (MRO) NERC Standards Review Forum’s (NSRF) comments on this question.

Likes 0

Dislikes 0

Response

Joni Jones - Wabash Valley Power Association - 1

Answer Yes

Document Name	
Comment	
no further comments	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Kinney - Avista - Avista Corporation - 3	
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

Justin MacDonald - Midwest Energy, Inc. - 1

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Mike Magruder - Avista - Avista Corporation - 1

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1

Answer

Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response

Jesus Sammy Alcaraz - Imperial Irrigation District - 1

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Glen Farmer - Avista - Avista Corporation - 5

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

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	
Gail Golden - Entergy - Entergy Services, Inc. - 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	
Jennifer Malon - Jennifer Malon On Behalf of: Brooke Voorhees, Black Hills Corporation, 3, 5, 1, 6; Derek Silbaugh, Black Hills Corporation, 3, 5, 1, 6; Don Stahl, Black Hills Corporation, 3, 5, 1, 6; Seth Nelson, Black Hills Corporation, 3, 5, 1, 6; - Jennifer Malon	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Amy Wesselkamper - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Hien Ho - Tacoma Public Utilities (Tacoma, WA) - 4	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Donald Lock - Talen Generation, LLC - 5	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bridget Silvia - Sempra - San Diego Gas and Electric - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Dwanique Spiller On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Bryan Koyle - Southern Indiana Gas and Electric Co. - 3,5,6 - RF

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Joseph Amato - Joseph Amato On Behalf of: Darnez Gresham, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Joseph Amato

Answer Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ryan Strom - Buckeye Power, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response

Mike Marshall - IDACORP - Idaho Power Company - 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

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Patricia Lynch - NRG - NRG Energy, 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

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

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,5 - RF

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Kinte Whitehead - Exelon - 3

Answer

Document Name

Comment

Exelon will align with EEI in response to this question.

Likes 0

Dislikes 0

Response

Daniel Gacek - Exelon - 1

Answer

Document Name

Comment

Exelon will align with EEI in response to this question.

Likes 0

Dislikes 0

Response

9. The SDT revised CIP-010 R1 to focus on defining change, authorizing change, and verifying that CIP-005 and CIP-007 related security controls are not affected by changes. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

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

Answer No

Document Name

Comment

The verbiage pertaining to CIP-005 and CIP-007 controls within CIP-010 R1 is acceptable. However, the verbiage in CIP-010 R1.2.1 states, "Prior to implementing ANY change..." which is far too all-inclusive. Additionally, the verbiage in CIP-010 R2.1 states, "Methods to monitor for unauthorized changes..." which also implies that ANY change is included in this scenario. The verbiage in both R1.2.1 and R2.1 should be revised to include only those changes applicable to Part 1.1 of CIP-010, not ANY change, as it is currently stated/implied.

Likes 0

Dislikes 0

Response

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

Answer No

Document Name

Comment

The verbiage pertaining to CIP-005 and CIP-007 controls within CIP-010 R1 is acceptable. However, the verbiage in CIP-010 R1.2.1 states, "Prior to implementing ANY change..." which is far too all-inclusive. Additionally, the verbiage in CIP-010 R2.1 states, "Methods to monitor for unauthorized changes..." which also implies that ANY change is included in this scenario. The verbiage in both R1.2.1 and R2.1 should be revised to include only those changes applicable to Part 1.1 of CIP-010, not ANY change, as it is currently stated/implied.

Likes 0

Dislikes 0

Response

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

Answer No

Document Name

Comment

Please provide the technical guidelines within the standard document. On “The Measures”, they call out testing what used to be in “The Requirements”, does this mean for each type of change there needs to be a different set of cyber security controls tested.

Likes 0

Dislikes 0

Response

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

Answer

No

Document Name

Comment

By removing the baseline requirement would leave too much ambiguity in the standard versus the more prescriptive requirements that are there now. Ambiguous requirements rely on too much auditor interpretation. Can the SDT develop a practice or implementation guidance. Industry needs to understand what's acceptable and what's not.

Likes 0

Dislikes 0

Response

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

Answer

No

Document Name

Comment

There is concern that the revised CIP-010-5 is not backwards compatible. For instance even though the Technical Rationale for CIP-010-5 states on page 5:

'The items found in the CIP-010-4 “**baseline**” are now included in the Measures column within CIP-010-5. This maintains compatibility with current state but allows flexibility for virtualization technologies. This also ensures the focus is not on documenting past changes but the authorization of current or future changes, thus making the requirement forward looking with a clearer security objective'

The actual CIP-010-5 **only mentions baseline once in the Measures column, for R1.3**

Likes 0

Dislikes 0

Response

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

Answer No

Document Name

Comment

Definitions such as SCI is not clear and confusing.

Likes 0

Dislikes 0

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer No

Document Name

Comment

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

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

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

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

Likes 0

Dislikes 0

Response

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

Answer No

Document Name

Comment

CHPD approves of the approach, but finds several fundamental issues with this draft.

By including the previous baseline items in the Measure, the intended goal is not met. No Responsible Entity's compliance staff will be willing to risk doing any less than what is listed in the Measures. If the SDT wants to commit to allowing Responsible Entities to choose their own changes that CIP-010 R1 applies to, it should consider removing the configuration items from the Measures. It will then need to be up to NERC and the Regional Entities to ensure that Responsible Entities are appropriately determining the changes that apply.

Given that software is effectively being removed from R1.1, it does not make sense to perform verification of software integrity and source (R1.5) in CIP-010 R1. It should instead be moved to a different requirement (either a new requirement in CIP-010 or into CIP-013).

CHPD believes that the changes proposed to CIP-010 R1 creates problems to CIP-010 R2.1. A change is fundamentally a difference from what something was previously to what something is now. You fundamentally have to know what something was to tell if it has changed. Knowing the previous state of the system is fundamentally what a baseline configuration is, and that makes it impossible to detect a change without having a baseline configuration. A Responsible Entity might be able to configure events to detect when certain changes occur, but that alert needs to know what the previous state was to know if a change occurred.

If the SDT wishes to pursue the current language, it will need to either eliminate CIP-010 R2 or rewrite it, as it is not possible to comply with it without tracking a baseline configuration. In keeping with the actual security objective of CIP-010 R1 (ensuring changes do not impact security controls adversely) CHPD recommends looking to TOP-001-4 R21/R24 for guidance. Instead of detecting unauthorized changes, require that RE's perform a test of a subset of CIP-005 and CIP-007 cyber security controls on a periodic basis.

Alternatively, the SDT could keep the baseline configuration requirements, reordering the requirements and removing time frames, and eliminating the proscriptive list of configuration items and allowing Responsible Entities to determine the configuration items for themselves.

Likes 0

Dislikes 0

Response

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

Answer No

Document Name

Comment

Comments:

- CIP-010-5 R1 P1.1 Please add "per system capability". Proposed language: "Define types of changes that may impact CIP-005 or CIP-007 security controls per system capability. For those changes:" The reasoning is that most network CA or VCA could only "baseline" firmware and logically accessible network ports. The security patches will be part of the firmware.

- CIP-010-5 R1 P1.1.1 and P1.1.3 Please add “per system capability”.
- 1.1.1. Prior to change implementation, identify impacted security controls in CIP-005 and CIP-007 per system capability, except during CIP Exceptional Circumstances.
- 1.1.3. Verify cyber security controls from CIP-005 and CIP-007 per system capability are not adversely affected.
- CIP-010-5 R1 P1.1.3 Measure please include in bullet 2 “or baseline tool” to read as follows: “An output from cyber security testing tools such as a vulnerability scanner or baseline tool.”
- Removing baseline language and concept from the standard completely creates risks for Entities to demonstrate compliance through the transition. The addition of all CIP-005 and CIP-007 controls as potential baselines or monitoring may take entities more than 12-months and therefore supports a 36-month implementation plan to migrate a large number of cyber assets.
- CIP-010-7 R1 P1.1 is a migration toward objected focus for CIP-005 and CIP-007 security controls but clarity on the Entities’ definition or determination of impact based up technology will take time and tooling requiring more time than 12-month implementation period. Objectives should be clear and must be applied based per the system capability.

Likes 0

Dislikes 0

Response

Bryan Koyle - Southern Indiana Gas and Electric Co. - 3,5,6 - RF

Answer

No

Document Name

Comment

The revised CIP-010 R1.1 language is vague and allows each entity to choose different types of changes to manage. What if a change occurs that affects the security controls; however, this change was not previously defined as a type of change that may impact CIP-005 or CIP-007? The removal of the specific baseline requirements will lead to a broad interpretive field on what is actually required and what is not. This may lead to differing regional interpretations and each entity left unclear as to what they have to do and what is merely good practice or due diligence.

Likes 0

Dislikes 0

Response

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

Answer

No

Document Name

Comment

The revised CIP-010 R1.1 language is vague and allows each entity to choose different types of changes to manage. What if a change occurs that affects the security controls; however, this change was not previously defined as a type of change that may impact CIP-005 or CIP-007? The removal of the specific baseline requirements will lead to a broad interpretive field on what is actually required and what is not. This may lead to differing regional interpretations and each entity left unclear as to what they have to do and what is merely good practice or due diligence.

Likes 0

Dislikes 0

Response

JT Kuehne - AEP - 6

Answer

No

Document Name

Comment

AEP appreciates SDT's attempt in making CIP-010-5 Requirement 1 Part 1.1 less prescriptive by moving types of baseline changes from the Requirements column to the Measures column. However, AEP believes this proposed revision may have unintended consequences of broadening the scope by not providing a definitive list to the Registered Entities. Therefore, AEP recommends moving the bulleted items from the Measures column to the Requirements column. AEP also recommends not including "Any other configuration or setting determined by the Responsible Entity" as this introduces ambiguity.

The Requirement 1 Part 1.1 would read as follows:

"Types of changes that may impact CIP-005 or CIP-007 security controls shall include the following items:

- **Operating system (OS) software;**
- **Firmware, where no independent OS exists;**
- **Commercially available or opensource application software, including application containers;**
- **Custom software installed, including application containers;**
- **Configuration that modifies network accessible logical ports or network accessible services on an Applicable System;**
- **SCI configuration of host affinity control between systems with different impact ratings;**
- **Changes to configurations or settings for an ESP between systems with different impact ratings; or**
- **Changes to parent images from which individual child images are derived, such as in virtual desktop infrastructure (VDI) implementations.**

For those changes:

1.1.1. Prior to change implementation, identify impacted security controls in CIP-005 and CIP-007, except during CIP Exceptional Circumstances;

1.1.2. Authorize those changes; and

1.1.3. Verify cyber security controls from CIP-005 and CIP-007 are not adversely affected."

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

Recommend keeping the approved language (keeping baselining) instead of the proposed update because 1) the older language better improves reliability (security) and 2) the newer language introduces more uncertainty in tracking the baseline. We suggest the existing group approach addresses this overall concern. We understand the new language tries addressing the brief period where an entity moves from one baseline to another. Meaning the entity has two baselines during this transition. We suggest there are other, less impactful ways to address these transitions.

Also, removing baselining causes so many questions and complications. Suggest the proposed updates do not simplify, instead these updates 1) add complexity, 2) increase cost with questionable benefit and 3) increase uncertainty of audit interpretations. Suggest that the SDT address previous baseline concerns in other ways. The concern for baselining system operator virtual desktops could be addressed by baselining the underlying disk image. The concern of children VMs not updating when their parents are updated could be addressed by documenting those situations.

Recommend keeping the approved language because the changes are not backward compatible.

Request Supply Chain updates align with Supply Chain best practices (like NIST 800-161)

The following comments provide reasons to support returning the approved baselining language.

Recommend an update to CIP-010 R1. This proposed removes the approved language on custom software. Request written exclusion of custom software in R1. Making this change reduces the ripple effect on the sub-parts of R1. As written, the proposed language impacts change process and change documentation. The proposed R1.3 adds confusion on software vs firmware. In the proposed updates, R1.3 is the only Requirement for tracking *all* versions.

For CIP-010, Part 1,1, we 1) recommend an update to provide audit certainty as to who determines impactful changes. Recommend adding “as determined by entity” to the Requirement language - “Define types of changes that may impact CIP-005 or CIP-007 security controls. For those changes:” and 2) request clarification. If the SDT moves towards measurable objective based, where are the objectives? As written, CIP-010 could be a heavy lift when getting into the details.

Request clarification of CIP Exceptional Circumstances in CIP-010, Part 1.1.1. Is this exception intended to be specific (Part 1.1.1) or general (R1)?

In CIP-010 Part 1.3, we 1) recommend moving “(or firmware where no OS exists)” from Requirements to Measures because the proposed language is confusing; 2) request explicit clarification that firmware is software; and 3) request update to Measures. Since “baseline” was removed from the Requirements, the Measures should not include “baseline.”

Likes 0

Dislikes 0

Response

Hien Ho - Tacoma Public Utilities (Tacoma, WA) - 4

Answer No

Document Name

Comment

R1 Part 1.3: With the removal of the specific baseline references for which changes are relevant to R1 Part 1.3 (previously R1.6), Tacoma Power is concerned that custom software (scripts) could be identified as applicable.

Likes 0

Dislikes 0

Response

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

Answer

No

Document Name

Comment

NST believes proposed changes beyond those needed for conformance have little or nothing to do with virtualization, are unlikely to improve anyone's cyber security posture, are outside the scope of the original 2016 SAR, are not addressed in any relevant FERC Order, and would be an unnecessary and unwelcome distraction for entities trying to adjust their CIP programs and documentation to accommodate new virtualization-related requirements. NST remains unconvinced that the existing requirement to maintain configuration baselines would inhibit the use of virtualized environments or that it has somehow become an outmoded approach to change management. We note that the NIST Cyber Security Framework, which has some strong advocates among various bodies with electric utility industry and reliability standard oversight responsibilities, lists among its controls, "A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)." We note, further, an online glossary accessible on the vmware.com web site includes an entry that reads, "A Configuration management system allows the enterprise to define settings in a consistent manner, then to build and maintain them according to the established baselines."

Likes 0

Dislikes 0

Response

Carl Pineault - Hydro-Qu?bec Production - 5

Answer

No

Document Name

Comment

Recommend keeping the approved language (keeping baselining) instead of the proposed update because 1) the older language better improves reliability (security) and 2) the newer language introduces more uncertainty in tracking the baseline. We suggest the existing group approach addresses this overall concern. We understand the new language tries addressing the brief period where an entity moves from one baseline to another. Meaning the entity has two baselines during this transition. We suggest there are other, less impactful ways to address these transitions.

Also, removing baselining causes so many questions and complications. Suggest the proposed updates do not simplify, instead these updates 1) add complexity, 2) increase cost with questionable benefit and 3) increase uncertainty of audit interpretations. Suggest that the SDT address previous

baseline concerns in other ways. The concern for baselining system operator virtual desktops could be addressed by baselining the underlying disk image. The concern of children VMs not updating when their parents are updated could be addressed by documenting those situations.

Recommend keeping the approved language because the changes are not backward compatible.

Request Supply Chain updates align with Supply Chain best practices (like NIST 800-161)

The following comments provide reasons to support returning the approved baselining language.

Recommend an update to CIP-010 R1. This proposed removes the approved language on custom software. Request written exclusion of custom software in R1. Making this change reduces the ripple effect on the sub-parts of R1. As written, the proposed language impacts change process and change documentation. The proposed R1.3 adds confusion on software vs firmware. In the proposed updates, R1.3 is the only Requirement for tracking *all* versions.

For CIP-010, Part 1,1, we 1) recommend an update to provide audit certainty as to who determines impactful changes. Recommend adding “as determined by entity” to the Requirement language - “Define types of changes that may impact CIP-005 or CIP-007 security controls. For those changes:” and 2) request clarification. If the SDT moves towards measurable objective based, where are the objectives? As written, CIP-010 could be a heavy lift when getting into the details.

Request clarification of CIP Exceptional Circumstances in CIP-010, Part 1.1.1. Is this exception intended to be specific (Part 1.1.1) or general (R1)?

In CIP-010 Part 1.3, we 1) recommend moving “(or firmware where no OS exists)” from Requirements to Measures because the proposed language is confusing; 2) request explicit clarification that firmware is software; and 3) request update to Measures. Since “baseline” was removed from the Requirements, the Measures should not include “baseline.”

Likes 0

Dislikes 0

Response

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

Answer

No

Document Name

Comment

Do not agree with the proposed CIP-010 R1.2 which states “Prior to implementing any change in the production environment” security controls testing is required. The use of “any change” is overly inclusive and would require security controls testing and compliance documentation for changes that would not fall into scope of the required change review/testing/authorizations identified in the proposed CIP-010 R1.1. Propose including language for this requirement to tie back to the types of changes identified in CIP-010 R1.1.

Likes 0

Dislikes 0

Response

Lindsey Mannion - ReliabilityFirst - 10

Answer	No
Document Name	
Comment	
<p>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.</p> <ul style="list-style-type: none"> · 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	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
<p>R2.1 ties back to R1. Please specify which components we need at a minimum to monitor for the unauthorized changes? Otherwise, it is up to the auditor's discretion.</p>	
Likes	0
Dislikes	0
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name SPP RTO	
Answer	No
Document Name	
Comment	
<p>SPP does not agree with the proposed changes to CIP-010 R1. Specifically, SPP believes that the current language improves reliability (security) but that the proposed language introduces more uncertainty in tracking the baseline. As such, the SPP recommends retaining the currently approved language for CIP-010 and not moving the prior language to the measures.</p>	

Additionally, the changed proposed for R1.3 are confusing. The way the SDT has written R1.3 language, the requirement appears to only apply to changes to software or firmware versioning, rather than new software. Finally, the proposed measures for R1.3 do not match with the proposed R1.3 requirement language.

Likes 0

Dislikes 0

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer

No

Document Name

Comment

IESO supports the comments provided by NPCC and IRC

Likes 0

Dislikes 0

Response

Thomas Breene - WEC Energy Group, Inc. - 3

Answer

No

Document Name

Comment

We have concerns with the SCI definition and it potentially bringing additional devices into scope. Additionally WEC agrees with NSRF comments regarding R1:

The SDT needs to revisit the issue of discussing a baseline in the R1 language. While we appreciate the difficulty in maintaining a traditional baseline when employing virtualization, and while we approve more flexible requirement language, it appears from industry comments and questions that simply removing the phrase "baseline" has caused confusion. This implies that there will be confusion in the future in terms of auditing and enforcement. Perhaps the term "baseline" should be re-added to the Measure as it pertains to traditional, non-virtual systems and then provide additional Measures for virtual systems.

Likes 0

Dislikes 0

Response

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

Answer	No
Document Name	
Comment	
<p>Recommend keeping the approved language (keeping baselining) instead of the proposed update because 1) the older language better improves reliability (security) and 2) the newer language introduces more uncertainty in tracking the baseline. We suggest the existing group approach addresses this overall concern. We understand the new language tries addressing the brief period where an entity moves from one baseline to another. Meaning the entity has two baselines during this transition. We suggest there are other, less impactful ways to address these transitions.</p> <p>Also, removing baselining causes so many questions and complications. Suggest the proposed updates do not simplify, instead these updates 1) add complexity, 2) increase cost with questionable benefit, and 3) increase uncertainty of audit interpretations. Suggest that the SDT address previous baseline concerns in other ways. The concern for baselining system operator virtual desktops could be addressed by baselining the underlying disk image. The concern of children's VMs not updating when their parents are updated could be addressed by documenting those situations.</p> <p>Recommend keeping the approved language because the changes are not backward compatible.</p> <p>Request Supply Chain updates align with Supply Chain best practices (like NIST 800-161)</p> <p>The following comments provide reasons to support returning the approved baselining language.</p> <p>Recommend an update to CIP-010 R1. This proposed removes the approved language on custom software. Request written exclusion of custom software in R1. Making this change reduces the ripple effect on the sub-parts of R1. As written, the proposed language impacts the change process and change documentation. The proposed R1.3 adds confusion on software vs firmware. In the proposed updates, R1.3 is the only Requirement for tracking *all* versions.</p> <p>For CIP-010, Part 1,1, we 1) recommend an update to provide audit certainty as to who determines impactful changes. Recommend adding "as determined by entity" to the Requirement language - "Define types of changes that may impact CIP-005 or CIP-007 security controls. For those changes:" and 2) request clarification. If the SDT moves towards measurable objective-based, where are the objectives? As written, CIP-010 could be a heavy lift when getting into the details.</p> <p>Request clarification of CIP Exceptional Circumstances in CIP-010, Part 1.1.1. Is this exception intended to be specific (Part 1.1.1) or general (R1)?</p> <p>In CIP-010 Part 1.3, we 1) recommend moving "(or firmware where no OS exists)" from Requirements to Measures because the proposed language is confusing; 2) request explicit clarification that firmware is software, and 3) request an update to Measures. Since "baseline" was removed from the Requirements, the Measures should not include "baseline."</p>	
Likes	0
Dislikes	0
Response	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	No
Document Name	
Comment	

We support NPCC TFIST comments.

Recommend keeping the approved language (keeping baselining) instead of the proposed update because 1) the older language better improves reliability (security) and 2) the newer language introduces more uncertainty in tracking the baseline. We suggest the existing group approach addresses this overall concern. We understand the new language tries addressing the brief period where an entity moves from one baseline to another. Meaning the entity has two baselines during this transition. We suggest there are other, less impactful ways to address these transitions.

Also, removing baselining causes so many questions and complications. Suggest the proposed updates do not simplify, instead these updates 1) add complexity, 2) increase cost with questionable benefit and 3) increase uncertainty of audit interpretations. Suggest that the SDT address previous baseline concerns in other ways. The concern for baselining system operator virtual desktops could be addressed by baselining the underlying disk image. The concern of children VMs not updating when their parents are updated could be addressed by documenting those situations.

Recommend keeping the approved language because the changes are not backward compatible.

Request Supply Chain updates align with Supply Chain best practices (like NIST 800-161)

The following comments provide reasons to support returning the approved baselining language.

Recommend an update to CIP-010 R1. This proposed removes the approved language on custom software. Request written exclusion of custom software in R1. Making this change reduces the ripple effect on the sub-parts of R1. As written, the proposed language impacts change process and change documentation. The proposed R1.3 adds confusion on software vs firmware. In the proposed updates, R1.3 is the only Requirement for tracking *all* versions.

For CIP-010, Part 1.1, we 1) recommend an update to provide audit certainty as to who determines impactful changes. Recommend adding “as determined by entity” to the Requirement language - “Define types of changes that may impact CIP-005 or CIP-007 security controls. For those changes:” and 2) request clarification. If the SDT moves towards measurable objective based, where are the objectives? As written, CIP-010 could be a heavy lift when getting into the details.

Request clarification of CIP Exceptional Circumstances in CIP-010, Part 1.1.1. Is this exception intended to be specific (Part 1.1.1) or general (R1)?

In CIP-010 Part 1.3, we 1) recommend moving “(or firmware where no OS exists)” from Requirements to Measures because the proposed language is confusing; 2) request explicit clarification that firmware is software; and 3) request update to Measures. Since “baseline” was removed from the Requirements, the Measures should not include “baseline.”

Likes 0

Dislikes 0

Response

David Jendras - Ameren - Ameren Services - 3

Answer

No

Document Name

Comment

We are uncomfortable with the slight ambiguity of the language. To make us more comfortable with the language, please define more clearly CIP-005 and CIP-007 security controls (Example: CIP-007 R1: Logical vs physical ports).

Likes 0

Dislikes 0

Response

John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1

Answer No

Document Name

Comment

R1 Part 1.3: With the removal of the specific baseline references for which changes are relevant to R1 Part 1.3 (previously R1.6), Tacoma Power is concerned that custom software (scripts) could be identified as applicable.

Likes 0

Dislikes 0

Response

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

Answer No

Document Name

Comment

From a security perspective, it is not clear what the proposed wording in CIP-010 R1.1 is intended to accomplish. The proposed wording doesn't look like it belongs in a change control requirement. Having a baseline and monitoring a baseline is one of the strongest security controls that exist in the CIP Standards. The proposed language in the requirements does not provide much direction and without reading the measures, an entity would have no idea how to interpret the requirement or how it relates to security of configuration management. SMUD recommends reconsidering the objective being addressed for changing CIP-010 R1.1 as the new direction proposed seems to lack clarity on the intent.

It is not clear how the changes being made are needed to support virtualization. SMUD's recommendation is to leave the requirements as they are unless there is a specific need to address a requirement in support of virtualization technology - this does not appear to be the case.

Likes 0

Dislikes 0

Response

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

Answer No

Document Name

Comment

We support NPCC RSC's comments.

Propose changing software (or firmware where no OS exists) to software or firmware. Hardware that runs an OS also has firmware that can usually be updated

Likes 0

Dislikes 0

Response

Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC) 2016-02 Virtualization (Draft 3)

Answer

No

Document Name

Comment

The SRC does not agree with the proposed changes to CIP-010 R1. Specifically, the SRC believes that the current language better improves reliability (security) and the proposed language introduces more uncertainty in tracking the baseline. As such, the SRC recommends retaining the currently approved language.

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

WECC supports the proposed changes but has some minor suggestions for possible edits.

Minor suggest edit, but to be consistent with the language of R1, Part 1.1 consider changing the language in the Measure from:

'a documented process that defines changes that may impact security controls in CIP-005 and CIP-007, such as but not limited to:'

To:

a documented process that defines changes that may impact CIP-005 and CIP-007 security controls, such as but not limited to:

Likes 0

Dislikes 0

Response	
Joni Jones - Wabash Valley Power Association - 1	
Answer	Yes
Document Name	
Comment	
Recommend removing R1.1.1. As written, R1.1 says What do you think will happen, authorize, test what did happen (regardless of what you thought would happen). While advance thought is good practice, the document what you think will happen is nothing more than a checkbox requirement that does not improve security.	
Likes	0
Dislikes	0

Response	
George Brown - Acciona Energy North America - 5	
Answer	Yes
Document Name	
Comment	
Acciona Energy supports Midwest Reliability Organization’s (MRO) NERC Standards Review Forum’s (NSRF) comments on this question.	
Likes	0
Dislikes	0

Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
MPC supports comments submitted by the MRO NERC Standards Review Forum (NSRF).	
For the proposed CIP-010-5, R1, Part 1.1.1, the draft language clarifies that impacted security controls in CIP-005 and CIP-007 must be identified prior to the change. Does the inclusion of the “prior to change” language in part 1.1.1 imply that the authorization of changes in part 1.1.2 can occur before or after the change? If the intent is to require authorization prior to the change, then the requirements should clearly state this.	
Likes	0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

BPA believes removing the 30 day timeframe and baseline requirements gives the Change & Configuration Management Program greater flexibility.

Likes 0

Dislikes 0

Response

Josh Johnson - Lincoln Electric System - 1

Answer Yes

Document Name

Comment

While LES is in agreement with the flexibility offered through the proposed changes, the abrupt shift away from baselines could use additional clarity for entities continuing to utilize the existing baseline method such as including baselines as an existing measure.

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

AZPS agrees that changes to CIP-010 R1 help streamline changes that are routine and known to not impact security controls. Allows effort to be focused on risk-based changes.

Likes 0

Dislikes 0

Response

Ellese Murphy - Duke Energy - 1,3,5,6 - SERC,RF

Answer Yes

Document Name

Comment

We agree and are very favorable of the revisions made to CIP-010 R1. As a quick note, part 1.6 should say part 1.3 in R1.3.

Likes 0

Dislikes 0

Response

patricia ireland - DTE Energy - 4

Answer Yes

Document Name

Comment

Patty Ireland on behalf of DTE Energy, Segments 3 and 4

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 proposed changes. However, BC Hydro has some concerns on the understanding specific to CIP-010 R1.3 which should clearly indicate that only the identified impacted security controls from CIP-010 Part 1.1.1 should be verified. Additionally, it is not clear if the verification can be done on a test asset/system or if it is expected to be done on all production assets of a given system.

The new CIP-010 R1.2.1 implies that the verification for CIP-010 R1.1.3 can be done on a representative test asset/system instead of all production assets for the given system. Testing on all production assets could have huge resourcing impacts.

BC Hydro seeks clarification on the above points and suggest adding an explanation in the technical rationale of the revised CIP-010 standard.

Likes	0
Dislikes	0
Response	
Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
<p>Comments: The SDT needs to revisit the issue of discussing a baseline in the R1 language. While we appreciate the difficulty in maintaining a traditional baseline when employing virtualization, and while we approve more flexible requirement language, it appears from industry comments and questions that simply removing the phrase "baseline" has caused confusion. This implies that there will be confusion in the future in terms of auditing and enforcement. Perhaps the term "baseline" should be re-added to the Measure as it pertains to traditional, non-virtual systems and then provide additional Measures for virtual systems.</p>	
Likes	0
Dislikes	0
Response	
Maggy Powell - Amazon Web Services - 7	
Answer	Yes
Document Name	
Comment	
N/A	
Likes	0
Dislikes	0
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern supports the revision of CIP-010 R1 to focus on CIP-005 and CIP-007 related security controls are not affected by changes.	

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

EEl supports the proposed changes.

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 comments submitted by EEI

Likes 0

Dislikes 0

Response

Kimberly Turco - Constellation - 6

Answer

Yes

Document Name

Comment

Constellation has elected to align with Exelon in response to this question.

Kim Turco, on behalf of Constellation Segments 5 and 6

Likes 0

Dislikes 0

Response

Alison Mackellar - Constellation - 5

Answer

Yes

Document Name

Comment

Constellation has elected to align with Exelon in response to this question.

Kim Turco, on behalf of Constellation Segments 5 and 6

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 Hirschak, 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

See EEI comment.

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

Alliant Energy supports the comments submitted by the MRO NSRF.

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

The SDT needs to revisit the issue of discussing a baseline in the R1 language. While we appreciate the difficulty in maintaining a traditional baseline when employing virtualization, and while we approve more flexible requirement language, it's evidence from industry comments and questions that simply removing the phrase "baseline" out completely has caused confusion. This implies that there will be confusion in the future in terms of auditing and enforcement. Perhaps the term "baseline" should be re-added to the Measure as it pertains to traditional, non-virtual systems and then provide additional Measures for virtual systems.

Likes 0

Dislikes 0

Response

Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,5 - RF

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Mike Marshall - IDACORP - Idaho Power Company - 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

Ryan Strom - Buckeye Power, Inc. - 5

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Joseph Amato - Joseph Amato On Behalf of: Darnez Gresham, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Joseph Amato	
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	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes	0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Dwanique Spiller - Dwanique Spiller On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Berkshire Hathaway - NV Energy - 5 - WECC

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Donald Lock - Talen Generation, LLC - 5

Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Amy Wesselkamper - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Jennifer Malon - Jennifer Malon On Behalf of: Brooke Voorhees, Black Hills Corporation, 3, 5, 1, 6; Derek Silbaugh, Black Hills Corporation, 3, 5, 1, 6; Don Stahl, Black Hills Corporation, 3, 5, 1, 6; Seth Nelson, Black Hills Corporation, 3, 5, 1, 6; - Jennifer Malon	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
William Steiner - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Glen Farmer - Avista - Avista Corporation - 5

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Jesus Sammy Alcaraz - Imperial Irrigation District - 1

Answer	Yes
---------------	-----

Document Name	
----------------------	--

Comment	
----------------	--

Likes	0
-------	---

Dislikes	0
----------	---

Response	
-----------------	--

James Baldwin - Lower Colorado River Authority - 1

Answer	Yes
---------------	-----

Document Name	
----------------------	--

Comment	
----------------	--

Likes	0
-------	---

Dislikes	0
----------	---

Response	
-----------------	--

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

Answer	Yes
---------------	-----

Document Name	
----------------------	--

Comment	
----------------	--

Likes	0
-------	---

Dislikes	0
----------	---

Response	
-----------------	--

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6

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

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

Justin MacDonald - Midwest Energy, Inc. - 1

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	
Scott Kinney - Avista - Avista Corporation - 3	
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	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	
Exelon will align with EEI in response to this question.	

Likes 0

Dislikes 0

Response

Kinte Whitehead - Exelon - 3

Answer

Document Name

Comment

Exelon will align with EEI in response to this question.

Likes 0

Dislikes 0

Response

10. The SDT made other revisions 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.

Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC) 2016-02 Virtualization (Draft 3)

Answer No

Document Name

Comment

The SRC does not agree with the other key proposed changes to CIP-010. Specifically, the SRC believes that within R2, the term "Unauthorized changes" is too broad and does not include "per system capability." The SRC recommends for the SDT to consider adding "monitor for changes identified in R1.1." The SRC also requests further clarification regarding the proposed change to R3.3 in regards to when a system becomes an "Applicable System." The SRC recommends that STD clarify whether this occurs before / after engaging service provision. The SRC agrees with the proposed changes to the remaining sub-requirements.

Likes 0

Dislikes 0

Response

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

Answer No

Document Name

Comment

We support NPCC RSC's comments.

In R2.1 The use of the term "for unauthorized changes" without the reference to a defined set of changes like the previous baseline, could imply that the entity authorize all changes on the system. This could include addition of data to existing or new files. Changing of file dates. Configuration of windows layouts on a display.....

In R3.3, make "Cyber System" singular for both uses in the first bullet or better yet, use Applicable Sytem since the defintion of Cyber Sytem includes PACS and the Applicable Systems do not

Likes 0

Dislikes 0

Response

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

6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Tim Kelley

Answer No

Document Name

Comment

Given the ambiguity of CIP-010 R1.1 it is difficult to understand why the other sub-requirements were either removed or updated. It also makes no sense to modify R1.1 in the way that it was modified, yet keep R2.1 relatively unchanged. Does R2.1 now mean that the entire system and all apps need to be monitored for unauthorized changes? It is unclear what unauthorized changes are to be monitored in the new version. The current version of the standard makes it clear what needs to be monitored.

SMUD does not agree with putting the requirements in the measures which seems to be what is happening here. We recommend rolling CIP-010 R1.1 back to what it was as these changes do not support virtualization.

Likes 0

Dislikes 0

Response

John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1

Answer No

Document Name

Comment

Tacoma Power is concerned that the scope of change associated to CIP-010-5 R2 part 2.1 is no longer bounded. The current version of CIP-010 R2 Part 2.1 is scoped to only those “changes to baseline configuration (as described in Requirement R1, Part 1.1).”

Tacoma Power suggests the following modification to the proposed language of CIP-010-5 R2 Part 2.1:
“Methods to monitor for unauthorized changes that may impact CIP-005 or CIP-007 security controls (as described in Requirement R1, Part 1.1) at least once every 35 calendar days. Document and investigate detected unauthorized changes.”

Likes 0

Dislikes 0

Response

David Jendras - Ameren - Ameren Services - 3

Answer No

Document Name

Comment

R1.1: We are uncomfortable with the slight ambiguity of the language. To make us more comfortable with the language, please define more clearly CIP-005 and CIP-007 security controls (Example: CIP-007 R1: Logical vs physical ports). R1.2: Like the clear documentation and the ability to use CIP exceptional circumstances. R2.1: Why did they add the word methods (under requirements)?. We are comfortable with the rest of the requirements.

Likes 0

Dislikes 0

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1

Answer

No

Document Name

Comment

We support NPCC TFIST comments.

In CIP-010, Part 2.1, request clarification of the SDT's intent. Does the new language pertain to 1) version changes in 1.3, 2) changes for CIP-005 & CIP-007 or 3) both?

In CIP-010, Part 3.3, Request clarification on when "Applicable System" starts. Suggest changing the beginning of Requirement from "Prior to becoming a new Applicable System" to "Prior to becoming a new, production Applicable System"

In CIP-010, Attachment 1, 1.3 we recommend removing two bullets because they are not software vulnerability mitigation which is the title of 1.3. The new bullet which is "Controls that maintain the state of the operating system and software such that it is in a known state prior to execution." The second bullet is "System hardening." Also, the new bullet preserves the vulnerability which is contrary to good security. The last bullet should remain since it covers alternatives.

In CIP-010, Attachment 1, 1.4 we recommend removing two bullets because they are not mitigating the introduction of malicious code which is the title of 1.4. The new bullet which is "Controls that maintain the state of the operating system and software such that it is in a known state prior to execution that mitigates the risk of introduction of malicious code." This new bullet preserves the vulnerability which is contrary to good security. The second bullet is "Application whitelisting;" The last bullet should remain since it covers alternatives.

Since CIP-010, Attachment 2 is the Measures for CIP-010, Attachment 1, we request updates to Attachment 2 per our Attachment 1 comments

Likes 0

Dislikes 0

Response

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

Answer

No

Document Name

Comment

In CIP-010, Part 2.1, request clarification of the SDT's intent. Does the new language pertain to 1) version changes in 1.3, 2) changes for CIP-005 & CIP-007 or 3) both?

In CIP-010, Part 3.3, Request clarification on when "Applicable System" starts. Suggest changing the beginning of Requirement from "Prior to becoming a new Applicable System" to "Prior to becoming a new, production Applicable System"

In CIP-010, Attachment 1, 1.3 we recommend removing two bullets because they are not software vulnerability mitigation which is the title of 1.3. The new bullet is "Controls that maintain the state of the operating system and software such that it is in a known state prior to execution." The second bullet is "System hardening." Also, the new bullet preserves the vulnerability which is contrary to good security. The last bullet should remain since it covers alternatives.

In CIP-010, Attachment 1, 1.4 we recommend removing two bullets because they are not mitigating the introduction of malicious code which is the title of 1.4. The new bullet is "Controls that maintain the state of the operating system and software such that it is in a known state prior to execution that mitigates the risk of introduction of malicious code." This new bullet preserves the vulnerability which is contrary to good security. The second bullet is "Application whitelisting;" The last bullet should remain since it covers alternatives.

Since CIP-010, Attachment 2 is the Measures for CIP-010, Attachment 1, we request updates to Attachment 2 per our Attachment 1 comments.

Likes 0

Dislikes 0

Response

Thomas Breene - WEC Energy Group, Inc. - 3

Answer

No

Document Name

Comment

Please refer to the response to question #9.

Likes 0

Dislikes 0

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer

No

Document Name

Comment

IESO supports the comments provided by NPCC and IRC

Likes 0

Dislikes 0

Response

Maggy Powell - Amazon Web Services - 7

Answer No

Document Name

Comment

AWS agrees with changes to CIP-010 R1, R2, and R3. AWS is concerned that CIP-010 R4 does not address security risk associated with virtual machines hosted on physical Transient Cyber Assets because the standard language states that a VM running on a physical TCA can be treated as software. The Standard allows an entity to choose one or a combination of security controls that may not extend cyber security protections to the VM itself leaving VMs potentially vulnerable to security threats undetected by the physical host.

We propose removing the language "Virtual machines hosted on a physical TCA can be treated as software on that physical TCA" from the TCA definition. By removing this language, entities would be required to apply security controls to the virtual machines hosted on their physical TCAs in alignment with CIP-010 R4.

Likes 0

Dislikes 0

Response

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name SPP RTO

Answer No

Document Name

Comment

The wording for CIP-010 R2.1 is very broad. For example, "changes" could be interpreted multiple ways and should be narrowed down. SPP suggests wording such as: "Security Controls identified in R1.1 should be monitored every 35 days for any unauthorized changes." Also when the same requirement was applied to R1.1, examples were included in the implementation guidance (e.g., examples of "replacement").

Likes 0

Dislikes 0

Response

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

Answer No

Document Name

Comment

A proposed administrative fix is: In the Applicable Systems column under "Note:" for Part 1.3 there is an old reference to Part 1.6 that should be updated to Part 1.3.

In Part 3.3 there is confusion over the language being used. The Applicable Systems column references BCS and the Requirements column references both Applicable Systems and Cyber System. The current approved version references Cyber Asset. Can you please clarify if the requirement is for an Applicable System or a Cyber Asset?

Likes 0

Dislikes 0

Response

Lindsey Mannion - ReliabilityFirst - 10

Answer

No

Document Name

Comment

R3- The concern is that Remediation VLANs should be properly defined in the technical rational or Glossary as it may introduce situations where an entity could inadvertently place production Cyber Assets in this VLAN.

Likes 0

Dislikes 0

Response

Carl Pineault - Hydro-Quebec Production - 5

Answer

No

Document Name

Comment

In CIP-010, Part 2.1, request clarification of the SDT's intent. Does the new language pertain to 1) version changes in 1.3, 2) changes for CIP-005 & CIP-007 or 3) both?

In CIP-010, Part 3.3, Request clarification on when "Applicable System" starts. Suggest changing the beginning of Requirement from "Prior to becoming a new Applicable System" to "Prior to becoming a new, production Applicable System"

In CIP-010, Attachment 1, 1.3 we recommend removing two bullets because they are not software vulnerability mitigation which is the title of 1.3. The new bullet which is "Controls that maintain the state of the operating system and software such that it is in a known state prior to execution." The second bullet is "System hardening." Also, the new bullet preserves the vulnerability which is contrary to good security. The last bullet should remain since it covers alternatives.

In CIP-010, Attachment 1, 1.4 we recommend removing two bullets because they are not mitigating the introduction of malicious code which is the title of 1.4. The new bullet which is "Controls that maintain the state of the operating system and software such that it is in a known state prior to execution"

that mitigates the risk of introduction of malicious code.” This new bullet preserves the vulnerability which is contrary to good security. The second bullet is “Application whitelisting;” The last bullet should remain since it covers alternatives.

Since CIP-010, Attachment 2 is the Measures for CIP-010, Attachment 1, we request updates to Attachment 2 per our Attachment 1 comments

Likes 0

Dislikes 0

Response

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

Answer

No

Document Name

Comment

Per our comments above on R1, NST disagrees with proposed changes that strike references to baselines.

Likes 0

Dislikes 0

Response

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

Answer

No

Document Name

Comment

The new TCA definition includes the use of Virtual Cyber Assets (VCA) as TCAs. This definition is problematic as the definition of a Virtual Cyber Asset includes only logical instances of an operating system or firmware hosted on BCAs, EACMS, PACS, PCAs, or SCI. The Cyber Asset acting as a TCA doesn't fall into any of these categories, so the VCA should not be referenced in the TCA definition. The new TCA definition implies that each VM on a Cyber Asset is a potential individual TCA.

Likes 0

Dislikes 0

Response

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

Answer

No

Document Name

Comment

R2.1 should address unauthorized changes to CIP-005 and CIP-007 controls. PNMR suggests the following modification to CIP-010 R2.1. “Methods to monitor for unauthorized changes to CIP-005 and CIP-007 controls at least once every 35 calendar days. Document and investigate detected unauthorized changes.”

Likes 0

Dislikes 0

Response**Hien Ho - Tacoma Public Utilities (Tacoma, WA) - 4**

Answer

No

Document Name

Comment

Tacoma Power is concerned that the scope of change associated to CIP-010-5 R2 part 2.1 is no longer bounded. The current version of CIP-010 R2 Part 2.1 is scoped to only those “changes to baseline configuration (as described in Requirement R1, Part 1.1).”

Tacoma Power suggests the following modification to the proposed language of CIP-010-5 R2 Part 2.1:

“Methods to monitor for unauthorized changes that may impact CIP-005 or CIP-007 security controls (as described in Requirement R1, Part 1.1) at least once every 35 calendar days. Document and investigate detected unauthorized changes.”

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

In CIP-010, Part 2.1, request clarification of the SDT’s intent. Does the new language pertain to 1) version changes in 1.3, 2) changes for CIP-005 & CIP-007 or 3) both?

In CIP-010, Part 3.3, Request clarification on when “Applicable System” starts. Suggest changing the beginning of Requirement from “Prior to becoming a new Applicable System” to “Prior to becoming a new, production Applicable System”

In CIP-010, Attachment 1, 1.3 we recommend removing two bullets because they are not software vulnerability mitigation which is the title of 1.3. The new bullet which is “Controls that maintain the state of the operating system and software such that it is in a known state prior to execution.” The second bullet is “System hardening.” Also, the new bullet preserves the vulnerability which is contrary to good security. The last bullet should remain since it covers alternatives.

In CIP-010, Attachment 1, 1.4 we recommend removing two bullets because they are not mitigating the introduction of malicious code which is the title of 1.4. The new bullet which is “Controls that maintain the state of the operating system and software such that it is in a known state prior to execution that mitigates the risk of introduction of malicious code.” This new bullet preserves the vulnerability which is contrary to good security. The second bullet is “Application whitelisting;” The last bullet should remain since it covers alternatives.

Since CIP-010, Attachment 2 is the Measures for CIP-010, Attachment 1, we request updates to Attachment 2 per our Attachment 1 comments

Likes 0

Dislikes 0

Response

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

Answer

No

Document Name

Comment

CenterPoint Energy suggests revising the requirement language in CIP-010 R3.3, second bullet, to say “Like replacements **or clone** of the same type of Cyber Systems with a configuration of the previous or existing Cyber System; or ” This revision will include new systems that are added for the same type or clone of a Cyber System.

Likes 0

Dislikes 0

Response

Bryan Koyle - Southern Indiana Gas and Electric Co. - 3,5,6 - RF

Answer

No

Document Name

Comment

SIGE suggests revising the requirement language in CIP-010 R3.3, second bullet, to say “Like replacements **or clone** of the same type of Cyber Systems with a configuration of the previous or existing Cyber System; or ” This revision will include new systems that are added for the same type or clone of a Cyber System.

Likes 0

Dislikes 0

Response

Josh Johnson - Lincoln Electric System - 1

Answer	No
Document Name	
Comment	
<p>R2.1 as written broadens beyond the intended scope of requirement R1. LES recommends the following alternative phrasing 'At least once every 35 calendar days, methods to monitor for changes identified in Requirement R1, Part 1.1 that have not been authorized.'</p> <p>In addition, LES has concern with the 'Technical Feasibility' conforming changes further detailed in the Question 11 response.</p>	
Likes	0
Dislikes	0
Response	
Justin Welty - NextEra Energy - Florida Power and Light Co. - 6	
Answer	No
Document Name	
Comment	
<p>The CIP-010-5 Technical Rationale confuses the changes proposed especially around R1. The Technical Rationale includes baselines in R1 and R1 P1.1 that have been removed from the standards. Reference CIP-010-4 Baseline details further complicates and confuses the implementation and does not clearly align with the new CIP-010-5 standard as written. A dormant VM cannot have a baseline run against it that is the same as when it is operating. Yet a VM image file can have a file integrity baseline and then when activated have the operating baselines verified with alerting for deviation and an incident response plan for monitoring deviations.</p>	
Likes	0
Dislikes	0
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	No
Document Name	
Comment	
<p>CHPD does not agree with the proposed changes to CIP-010. CHPD believes the changes to CIP-010 R1 cause problems to CIP-010 R2.1. A change is fundamentally a difference from what something was previously to what something is now. You fundamentally have to know what something was to tell if it has changed. Knowing the previous state of the system is fundamentally what a baseline configuration is, and that makes it impossible to detect a change without having a baseline configuration. A Responsible Entity might be able to configure events to detect when certain changes occur, but that alert needs to know what the previous state was to know if a change occurred.</p>	

If the SDT wishes to pursue the current language, it will need to either eliminate CIP-010 R2 or rewrite it, as it is not possible to comply with it without tracking a baseline configuration. In keeping with the actual security objective of CIP-010 R1 (ensuring changes do not impact security controls adversely) CHPD recommends looking to TOP-001-4 R21/R24 for guidance. Instead of detecting unauthorized changes, require that RE's perform a test of a subset of CIP-005 and CIP-007 cyber security controls on a periodic basis.

Alternatively, the SDT could keep the baseline configuration requirements, reordering the requirements and removing time frames, and eliminating the proscriptive list of configuration items and allowing Responsible Entities to determine the configuration items for themselves.

Likes 0

Dislikes 0

Response

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

Answer No

Document Name

Comment

Definitions such as SCI is not clear and confusing.

Likes 0

Dislikes 0

Response

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

Answer No

Document Name

Comment

The phrase "prior to becoming a new Applicable System" is confusing and open to multiple interpretations. BPA recommends adding language to clearly scope the Part to the device level.

Prior to adding new applicable Cyber Assets or a new Applicable System, perform an active vulnerability assessment of the new Cyber Assets or Applicable System, except for:

• Like replacements of the same type of Cyber Assets or Applicable Systems with a configuration of the previous or other existing Cyber Assets or Applicable System; or

• CIP Exceptional Circumstances.

Likes 0

Dislikes 0

Response

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

Answer No

Document Name

Comment

What, if any, impacts will the virtualization modifications have on what is required in a vulnerability assessments that is currently outlined in the Guidelines and Technical Basis?

Also note Attachment 1 was modified starting on page 31 for TCA's and RM. This seems vague and Attachment 2 doesn't really help. IE: what is a valid control?

a. "Live operating system and software executable only from read only media" was eliminated. But, in 1.3 "Controls that maintain the state of the operating system and software such that it is in a known state prior to execution;" was added. Also in 1.4 "Controls that maintain the state of the operating system and software such that it is in a known state prior to execution that mitigates the risk of introduction of malicious code"

Please provide the technical guidelines within the standard document. We would like more details for what needs to be performed for a VA.

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Consider re-writing R2.1 to read, "Methods to monitor at least once every 35 calendar days for changes that were not authorized per Requirement R1. Document and investigate any such detected unauthorized changes." While potentially minor, this change in language provides more stricture around the term "unauthorized change," explicitly tying it to the processes established under Requirement R1.

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Alliant Energy supports the comments submitted by the MRO NSRF.

Likes 0

Dislikes 0

Response

Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirschak, 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

See EEI comment.

Likes 0

Dislikes 0

Response

Alison Mackellar - Constellation - 5

Answer

Yes

Document Name

Comment

Constellation has elected to align with Exelon in response to this question.

Kim Turco, on behalf of Constellation Segments 5 and 6

Likes 0

Dislikes 0

Response

Kimberly Turco - Constellation - 6

Answer

Yes

Document Name	
Comment	
Constellation has elected to align with Exelon in response to this question.	
Kim Turco, on behalf of Constellation Segments 5 and 6	
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 comments 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.	
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 revisions to CIP-010.	
Likes 0	
Dislikes 0	
Response	
Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Comments: Consider re-writing R2.1 to read, "Methods to monitor at least once every 35 calendar days for changes that were not authorized per Requirement R1. Document and investigate any such detected unauthorized changes." While potentially minor, this change in language provides more stricture around the term "unauthorized change," explicitly tying it to the processes established under Requirement R1.	
Likes 0	
Dislikes 0	
Response	
Jennifer Malon - Jennifer Malon On Behalf of: Brooke Voorhees, Black Hills Corporation, 3, 5, 1, 6; Derek Silbaugh, Black Hills Corporation, 3, 5, 1, 6; Don Stahl, Black Hills Corporation, 3, 5, 1, 6; Seth Nelson, Black Hills Corporation, 3, 5, 1, 6; - Jennifer Malon	
Answer	Yes
Document Name	
Comment	
Black Hills Corporation agrees with the proposed changes, but has concerns that the new 1.3 language is less clear. As written, it appears a utility could install new software and not check the source.	
Likes 0	
Dislikes 0	
Response	
patricia ireland - DTE Energy - 4	
Answer	Yes

Document Name

Comment

Patty Ireland on behalf of DTE Energy, Segments 3 and 4

Likes 0

Dislikes 0

Response

JT Kuehne - AEP - 6

Answer

Yes

Document Name

Comment

AEP supports the proposed changes in CIP-010-5, Requirements R2, R3 and R4.

Likes 0

Dislikes 0

Response

Ellese Murphy - Duke Energy - 1,3,5,6 - SERC,RF

Answer

Yes

Document Name

Comment

We agree with the proposed changes.

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

AZPS agrees that the revisions to CIP-010 helps clarify the risk based approach to change management.

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

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

Likes 0

Dislikes 0

Response

George Brown - Acciona Energy North America - 5

Answer

Yes

Document Name

Comment

Acciona Energy supports Midwest Reliability Organization's (MRO) NERC Standards Review Forum's (NSRF) comments on this question.

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

All other proposed changes to CIP-010 are acceptable, except for some potential confusion around CIP-010, R4. In R4, the language, “for its high and medium impact BCS and associated PCA AND SCI” could be misinterpreted and viewed as all inclusive. NRG proposes to change the AND in “associated PCA AND SCI” to OR.

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

All other proposed changes to CIP-010 are acceptable, except for some potential confusion around CIP-010, R4. In R4, the language, “for its high and medium impact BCS and associated PCA AND SCI” could be misinterpreted and viewed as all inclusive. NRG proposes to change the AND in “associated PCA AND SCI” to OR.

Likes 0

Dislikes 0

Response

Joni Jones - Wabash Valley Power Association - 1

Answer

Yes

Document Name

Comment

no further comments

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Scott Kinney - Avista - Avista Corporation - 3

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

Justin MacDonald - Midwest Energy, Inc. - 1

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Mike Magruder - Avista - Avista Corporation - 1

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

James Baldwin - Lower Colorado River Authority - 1

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Jesus Sammy Alcaraz - Imperial Irrigation District - 1

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Glen Farmer - Avista - Avista Corporation - 5

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

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

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

William Steiner - Midwest Reliability Organization - 10

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Donald Lock - Talen Generation, LLC - 5

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Dwanique Spiller - Dwanique Spiller On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Berkshire Hathaway - NV Energy - 5 - WECC

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Joseph Amato - Joseph Amato On Behalf of: Darnez Gresham, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Joseph Amato

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

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

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Ryan Strom - Buckeye Power, Inc. - 5

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Mike Marshall - IDACORP - Idaho Power Company - 1

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,5 - RF

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Kinte Whitehead - Exelon - 3

Answer	
Document Name	
Comment	
Exelon will align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	
Exelon will align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	

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

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

Answer No

Document Name

Comment

CIP-009 R1 does not require a Recovery Plan for SCI, yet CIP-009 R1.5 requires data preservation for SCI during recovery. There is not a mechanism (i.e., a Recovery Plan) in which to document the data preservation requirement if there is Recovery Plan requirement for SCI.

Likes 0

Dislikes 0

Response

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

Answer No

Document Name

Comment

CIP-009 R1 does not require a Recovery Plan for SCI, yet CIP-009 R1.5 requires data preservation for SCI during recovery. There is not a mechanism (i.e., a Recovery Plan) in which to document the data preservation requirement if there is Recovery Plan requirement for SCI.

Likes 0

Dislikes 0

Response

Mike Marshall - IDACORP - Idaho Power Company - 1

Answer No

Document Name

Comment

The Supplemental Guidelines section of the written standard were helpful in creating applicable controls however with the removal of these technical explanations of new controls should be included with the proposed changes.

Likes 0

Dislikes 0

Response

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

Answer No

Document Name

Comment

Definitions such as SCI is not clear and confusing.

Likes 0

Dislikes 0

Response

Josh Johnson - Lincoln Electric System - 1

Answer No

Document Name

Comment

LES recognizes and appreciates the work put into the conforming changes. LES agrees with the vast majority, however, the alternative to the 'Technical Feasibility Exception (TFE)' process should incorporate the full range of circumstances currently available to entities. As written, 'per system capability' would obligate entities to implement the requirements based solely on whether the Cyber Asset or Cyber System is technically capable whereas the TFE process currently allows entities to apply for exceptions based on operational feasibility, reliability feasibility, resource limitations, safety risks, separate regulatory requirements, and associated costs in addition to the prescribed technical limitations.

LES suggests replacing the phrase 'per system capability' with 'per System Feasibility'. This would require a new term, '**System Feasibility**' which would include the 6 identified circumstances outlined within Appendix 4D of the NERC Rules of Procedure. (Page 2, Section 3.0)

System Feasibility:

Technical or operational circumstances of a Cyber System or Cyber Asset that consider;

- Technical limitations;
- Operational feasibility that could adversely affect reliability of the BES;
- Is technically possible or operationally feasible but has limitations due to scarce technical resources;
- Safety risks or issues that outweigh the benefits of compliance;
- Conflicts with separate statutory or regulatory requirements; or
- Incurrence of costs that far exceed the benefits to the reliability of the BES.

Likes 0

Dislikes 0

Response

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

Answer No

Document Name

Comment

Manitoba Hydro agrees with the direction of the SDT and all conforming changes to standards CIP-003, CIP-004, CIP-008, CIP-009, CIP-011 and CIP-013. For standard CIP-006 the applicability column does not include SCI. This could create confusion as a VCA designated as an applicable system (BCS for example) would need to be located in a Physical Security Perimeter (PSP), however the SCI physically hosting the VCA is not explicitly noted in the applicability column.

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

Request clarification of CIP-003 R2. Listing locations containing SCI outside of BES assets is a benefit. However, CIP-003 stipulates that an inventory (list) is not required. How to reconcile these two statements? Should CIP-002 require listing these locations?

Recommend update of CIP-003, Attachment 1, 3.1.i. Recommend new wording and no bullets for improved readability. "Between a low impact BCS or an SCI that supports any part of low BCS and a Cyber System outside the asset containing the low impact BCS(s) or the SCI that supports any part of the Low Impact BCS;"

Recommend update of CIP-003, Attachment 1, 5.1. We recommend removing the new (second) bullet which is consistent with our comments on CIP-010, Attachment 1, 1.3 and 1.4. We recommend removing the new bullet because it is not "malicious code mitigation" which is the title of Section 5. The new bullet which is "Controls that maintain the state of the operating system and software such that they are in a known state prior to execution that mitigates the risk of introduction of malicious code." The last bullet should remain since it covers alternatives.

Recommend update of CIP-003, Attachment 1, 5.2. We recommend removing the updated (fourth) bullet which is consistent with our comments on CIP-010, Attachment 1, 1.3 and 1.4. We recommend removing the new bullet because it is not "malicious code mitigation" which is the title of Section 5. The updated bullet which is "Review of controls that maintain the state of the operating system and software such that they are in a known state prior to execution that mitigates the risk of introduction of malicious code."

If the SDT believes CIP-006 implies physical security of the SCI, we request explicit language in this Standard.

Request correction to CIP-006 Part 1.2 from "Physical Access Control Systems" to "Protected Cyber Assets" for consistency with Part 1.3.

Request update to CIP-008 Part 2.3. For consistency, this Part should include SCI in the Applicable Systems.

Request update to the Parts of CIP-009 R1. If SCI is required for Applicable System recovery, SCI should be included in that recovery plan.

Request clarification on CIP-011 R2 Part 2.1. Is this focus on unauthorized retrieval of BCSI or the lifecycle question of decommissioning of the asset containing BCSI?

Request clarification on CIP-011 R2 Part 2.1. Why is PCA is a Part 2.1 Applicable System but not an Applicable System in Parts 1.1 and 1.2?

We suggest removing R2 to avoid double jeopardy because methods of protection (R1) should include destruction – making R1 sufficient. Plus, R2 is asset based while BCSI is information. This Standard and R1 are focused on information protection

Likes 0

Dislikes 0

Response

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

Answer No

Document Name

Comment

NST agrees with proposed changes to CIP-003, CIP-004, CIP-008, CIP-011, and CIP-013.

NST disagrees with proposed changes to CIP-006 and CIP-009.

CIP-006: NST understands the omission of SCI from any requirement part was intentional, but we disagree with this decision for two reasons. First, it would establish yet more “implied requirements,” as discussed in our comments on Question 1. Second, it is inconsistent with the proposed changes to CIP-004, which would establish explicit requirements to authorize, review and, when appropriate, revoke unescorted physical access to SCI.

CIP-009: NST understands the omission of SCI from any requirement part except for R1.5 (preservation of forensic data if possible) was intentional, but we disagree with this decision, as it would establish yet more “implied requirements,” as discussed in our comments on Question 1. NST acknowledges that in some recovery situations, it might only be necessary to recover a virtual BES Cyber System and not its supporting SCI. However, given the fact the failure or destruction of an SCI could, in some scenarios, wipe out an entire Control Center, NST believes that inclusion of SCI in a Responsible Entity’s recovery plan(s) should be mandatory rather than a suggested best practice.

Likes 0

Dislikes 0

Response

Carl Pineault - Hydro-Qu?bec Production - 5

Answer No

Document Name

Comment

Request clarification of CIP-003 R2. Listing locations containing SCI outside of BES assets is a benefit. However, CIP-003 stipulates that an inventory (list) is not required. How to reconcile these two statements? Should CIP-002 require listing these locations?

Recommend update of CIP-003, Attachment 1, 3.1.i. Recommend new wording and no bullets for improved readability. "Between a low impact BCS or an SCI that supports any part of low BCS and a Cyber System outside the asset containing the low impact BCS(s) or the SCI that supports any part of the Low Impact BCS;"

Recommend update of CIP-003, Attachment 1, 5.1. We recommend removing the new (second) bullet which is consistent with our comments on CIP-010, Attachment 1, 1.3 and 1.4. We recommend removing the new bullet because it is not "malicious code mitigation" which is the title of Section 5. The new bullet which is "Controls that maintain the state of the operating system and software such that they are in a known state prior to execution that mitigates the risk of introduction of malicious code." The last bullet should remain since it covers alternatives.

Recommend update of CIP-003, Attachment 1, 5.2. We recommend removing the updated (fourth) bullet which is consistent with our comments on CIP-010, Attachment 1, 1.3 and 1.4. We recommend removing the new bullet because it is not "malicious code mitigation" which is the title of Section 5. The updated bullet which is "Review of controls that maintain the state of the operating system and software such that they are in a known state prior to execution that mitigates the risk of introduction of malicious code."

If the SDT believes CIP-006 implies physical security of the SCI, we request explicit language in this Standard.

Request correction to CIP-006 Part 1.2 from "Physical Access Control Systems" to "Protected Cyber Assets" for consistency with Part 1.3.

Request update to CIP-008 Part 2.3. For consistency, this Part should include SCI in the Applicable Systems.

Request update to the Parts of CIP-009 R1. If SCI is required for Applicable System recovery, SCI should be included in that recovery plan.

Request clarification on CIP-011 R2 Part 2.1. Is this focus on unauthorized retrieval of BCSI or the lifecycle question of decommissioning of the asset containing BCSI?

Request clarification on CIP-011 R2 Part 2.1. Why is PCA is a Part 2.1 Applicable System but not an Applicable System in Parts 1.1 and 1.2?

We suggest removing R2 to avoid double jeopardy because methods of protection (R1) should include destruction – making R1 sufficient. Plus, R2 is asset based while BCSI is information. This Standard and R1 are focused on information protection

Likes 0

Dislikes 0

Response

William Steiner - Midwest Reliability Organization - 10

Answer

No

Document Name

Comment

CIP-003

- -Attachment 1, Section 2 - How do you control physical access to a VCA? SCI is not required to have protections. Is the expectation that only the specific nodes of the SCI cluster that are hosting the VCA are physically protected?
- Attachment 1, Section 3 – The applicability of requirements to SCI at assets containing low impact BCS is not well defined. CIP-002 does not require the identification of assets containing low impact SCI. If SCI supporting low-impact BCS is spread across multiple assets it is not clear if the protections need to be applied at those other assets as well. For example, some of nodes of an SCI cluster are at a substation and host low impact BCS containing VCAs, but other nodes of that same SCI cluster are located at another asset that does not contain any low impact BCS – it is not clear whether those controls need to be applied there, especially since that asset did not need to be identified in CIP-002.
- Formatting comment only: Attachment 1, Section 3 - the and/or formatting leaves room for confusion - it is not clear that the 'and a Cyber System(s) outside the asset containing:' is not part of the bullet 'An SCI that supports any part of a low BCS', but rather applies to both bullets or'd together.

CIP-006

- Part 1.2 - The applicability column does not include SCI, but does include VCAs (as part of BCS). Scoping the physical requirement to a logical instance could be misleading and allow physical protections to not be applied as necessary. Furthermore, the exclusion of SCI could allow a hypervisor/SCI(1) (hosting non-CIP VCA) that's part of the SCI cluster which is geographically dispersed from the SCI(2) hosting a BCS. The requirement infers that as soon as the SCI(1) hosts an applicable CIP VCA it would require PSP protections. But if the SCI(1) is not hosting an applicable system in CIP-006 R1.2 it would not require PSP protections. An alternate approach would be to include SCI as an applicable system.
- Part 1.3 – The change from “where technically feasible” to “per system capability” removes the requirement for mitigation of the risks posed by the feasibility exception. The requirement is not prescriptive to specific technical controls, this provides flexibility that should not be limited to technical infeasibility. For a PSP protecting high impact BCS, it seems unreasonable to allow for implementations that aren't capable of using two or more physical access controls without mitigation of the risk.

Likes 0

Dislikes 0

Response

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

Answer

No

Document Name

Comment

In CIP-003, concerned about the ambiguous language of “supports any part of the low impact BCS” and what exactly that means. This makes sense for SCI that directly supports a BROS function of the low impact BCS, but “[supporting] any part” may lead to misinterpretations. For example, does “support” include:

- Security controls an entity implements that are above and beyond the CIP-003 standards? e.g if an entity implements a virtualized configuration monitoring tool specific for low impact in their Data Center and it scans remote low impact BCS, am I required per CIP-003 to control inbound/outbound permissions or utilize a TCA program to the security tool SCI in the DC that otherwise doesn't fall under CIP scope?

- Operational tools an entity uses to run/manage the low impact BCS? E.g. if an entity implements a virtualized system monitoring tool that identifies system health (e.g. up/down status, processor utilization, memory utilization, bandwidth, etc) of the low impact BCS in their Data Center, am I

required per CIP-003 to control inbound/outbound permissions or utilize a TCA program to the health monitoring SCI in the DC that otherwise doesn't fall under CIP scope?

- Data aggregation tools that collect data not used in a real-time horizon as defined by NERC? E.g if an entity implements a data aggregation tool that collects system that is not used for real-time decision making or any other real-time horizon, but helps "support" the operation of the low impact BCS (e.g. configurations, set-points, fault tracking, historian, etc) in their Data Center, am I required per CIP-003 to control inbound/outbound permissions or utilize a TCA program to the data aggregation tool SCI in the DC that otherwise doesn't fall under CIP scope?

Concerned the ambiguous definition of "support" may bring assets/tools/SCI into scope that otherwise would not be. Recommend more descriptive language or a definition of "support" to ensure the proper scope is obtained.

Likes 0

Dislikes 0

Response

Lindsey Mannion - ReliabilityFirst - 10

Answer No

Document Name

Comment

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

Likes 0

Dislikes 0

Response

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name SPP RTO

Answer No

Document Name

Comment

Except for the comments regarding the definitions for VCA, SCI, EAP, PCA, and ERC as noted above in Question 1-6, SPP supports the changes the SDT has made to the Requirements for CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013.

If the SDT continues with another version of the standards, SPP suggests the SDT consider the following actions or clarifications:

- Should SCI be included as part of R1.1 for CIP-009?

- For CIP-008 R4,. add "..., or their successors" in the R4 requirement of the language after Cybersecurity & Infrastructure Security Agency (CISA).

Likes 0

Dislikes 0

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer

No

Document Name

Comment

IESO supports the comments provided by NPCC and IRC

Likes 0

Dislikes 0

Response

Thomas Breene - WEC Energy Group, Inc. - 3

Answer

No

Document Name

Comment

CIP-003 – *No, we have concerns with the SCI definition and it potentially bringing additional devices into scope. This term is used throughout the Standard.*

CIP-004 – *No, we have concerns with the SCI and IRS definitions. These terms are used throughout the Standard.*

CIP-006 – *Yes*

CIP-008 – *No, we have concerns with the SCI definition and it potentially bringing additional devices into scope. This term is used throughout the Standard.*

CIP-009 - *No, we have concerns with the SCI definition and it potentially bringing additional devices into scope. This term is used throughout the Standard.*

CIP-011 - *No, we have concerns with the SCI definition and it potentially bringing additional devices into scope. This term is used throughout the Standard.*

CIP-013 - No, we have concerns with the SCI definition and it potentially bringing additional devices into scope. This term is used throughout the Standard.

Likes 0

Dislikes 0

Response

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

Answer

No

Document Name

Comment

Request clarification of CIP-003 R2. Listing locations containing SCI outside of BES assets is a benefit. However, CIP-003 stipulates that an inventory (list) is not required. How do you reconcile these two statements? Should CIP-002 require listing these locations?

Recommend update of CIP-003, Attachment 1, 3.1.i. Recommend new wording and no bullets for improved readability. "Between a low impact BCS or an SCI that supports any part of low BCS and a Cyber System outside the asset containing the low impact BCS(s) or the SCI that supports any part of the Low Impact BCS;"

Recommend update of CIP-003, Attachment 1, 5.1. We recommend removing the new (second) bullet which is consistent with our comments on CIP-010, Attachment 1, 1.3, and 1.4. We recommend removing the new bullet because it is not "malicious code mitigation" which is the title of Section 5. The new bullet is "Controls that maintain the state of the operating system and software such that they are in a known state prior to execution that mitigates the risk of introduction of malicious code." The last bullet should remain since it covers alternatives.

Recommend update of CIP-003, Attachment 1, 5.2. We recommend removing the updated (fourth) bullet which is consistent with our comments on CIP-010, Attachment 1, 1.3, and 1.4. We recommend removing the new bullet because it is not "malicious code mitigation" which is the title of Section 5. The updated bullet is a "Review of controls that maintain the state of the operating system and software such that they are in a known state prior to execution that mitigates the risk of introduction of malicious code."

If the SDT believes CIP-006 implies the physical security of the SCI, we request explicit language in this Standard.

Request correction to CIP-006 Part 1.2 from "Physical Access Control Systems" to "Protected Cyber Assets" for consistency with Part 1.3.

Request update to CIP-008 Part 2.3. For consistency, this Part should include SCI in the Applicable Systems.

Request update to the Parts of CIP-009 R1. If SCI is required for Applicable System recovery, SCI should be included in that recovery plan.

Request clarification on CIP-011 R2 Part 2.1. Is this focus on unauthorized retrieval of BCSI or the lifecycle question of decommissioning the asset containing BCSI?

Request clarification on CIP-011 R2 Part 2.1. Why is PCA a Part 2.1 Applicable System but not an Applicable System in Parts 1.1 and 1.2?

We suggest removing R2 to avoid double jeopardy because methods of protection (R1) should include destruction – making R1 sufficient. Plus, R2 is asset-based while BCSI is information. This Standard and R1 are focused on information protection.

Likes 0

Dislikes 0

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1

Answer No

Document Name

Comment

We support NPCC TFIST comments.

Request clarification of CIP-003 R2. Listing locations containing SCI outside of BES assets is a benefit. However, CIP-003 stipulates that an inventory (list) is not required. How to reconcile these two statements? Should CIP-002 require listing these locations?

Recommend update of CIP-003, Attachment 1, 3.1.i. Recommend new wording and no bullets for improved readability. "Between a low impact BCS or an SCI that supports any part of low BCS and a Cyber System outside the asset containing the low impact BCS(s) or the SCI that supports any part of the Low Impact BCS;"

Recommend update of CIP-003, Attachment 1, 5.1. We recommend removing the new (second) bullet which is consistent with our comments on CIP-010, Attachment 1, 1.3 and 1.4. We recommend removing the new bullet because it is not "malicious code mitigation" which is the title of Section 5. The new bullet which is "Controls that maintain the state of the operating system and software such that they are in a known state prior to execution that mitigates the risk of introduction of malicious code." The last bullet should remain since it covers alternatives.

Recommend update of CIP-003, Attachment 1, 5.2. We recommend removing the updated (fourth) bullet which is consistent with our comments on CIP-010, Attachment 1, 1.3 and 1.4. We recommend removing the new bullet because it is not "malicious code mitigation" which is the title of Section 5. The updated bullet which is "Review of controls that maintain the state of the operating system and software such that they are in a known state prior to execution that mitigates the risk of introduction of malicious code."

If the SDT believes CIP-006 implies physical security of the SCI, we request explicit language in this Standard.

Request correction to CIP-006 Part 1.2 from "Physical Access Control Systems" to "Protected Cyber Assets" for consistency with Part 1.3.

Request update to CIP-008 Part 2.3. For consistency, this Part should include SCI in the Applicable Systems.

Request update to the Parts of CIP-009 R1. If SCI is required for Applicable System recovery, SCI should be included in that recovery plan.

Request clarification on CIP-011 R2 Part 2.1. Is this focus on unauthorized retrieval of BCSI or the lifecycle question of decommissioning of the asset containing BCSI?

Request clarification on CIP-011 R2 Part 2.1. Why is PCA is a Part 2.1 Applicable System but not an Applicable System in Parts 1.1 and 1.2?

We suggest removing R2 to avoid double jeopardy because methods of protection (R1) should include destruction – making R1 sufficient. Plus, R2 is asset based while BCSI is information. This Standard and R1 are focused on information protection

Likes 0

Dislikes 0

Response

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

Answer	No
Document Name	
Comment	
<p>Suggest adding SCI to the Note for CIP-003 R2</p> <p>Request clarification of CIP-003 R2. Listing locations containing SCI outside of BES assets is a benefit. However, CIP-003 stipulates that an inventory (list) is not required. How to reconcile these two statements? Should CIP-002 require listing these locations?</p> <p>If the SDT believes CIP-006 implies physical security of the SCI, we request explicit language in this Standard.</p> <p>Request update to CIP-008 Part 2.3. For consistency, this Part should include SCI in the Applicable Systems.</p> <p>Request update to the Parts of CIP-009 R1. If SCI is required for Applicable System recovery, SCI should be included in that recovery plan.</p> <p>Request clarification on CIP-011 R2 Part 2.1. Why is PCA a Part 2.1 Applicable System but not an Applicable System in Parts 1.1 and 1.2?</p> <p>We suggest removing R2 to avoid double jeopardy because methods of protection (R1) should include destruction – making R1 sufficient. Plus, R2 is asset based while BCSI is information. This Standard and R1 are focused on information protection</p>	
Likes	0
Dislikes	0
Response	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller	
Answer	No
Document Name	
Comment	
<p>RE: CIP-003</p> <p>o The addition of controls for low impact in Attachment 1 Section 5 are the same/similar to the addition of controls for high/medium impact in CIP-010 Attachment 1, Section 1. This addition for low impact is overly burdensome and would stretch the resources of companies that have a significant number of low impact assets, with a minimal increase in the security/protection of the BES. While low impact should be protected, the protection should be appropriate for the impact rating to the BES and not on the same level as high/medium impact.</p>	
Likes	0
Dislikes	0
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC Entity Monitoring	

Answer	Yes
Document Name	
Comment	
<p>WECC supports the revisions but has one question for consideration.</p> <p>Considering SCI is included in the applicability table of CIP-009-7 R1 Part 1.5. Was it the intent of the SDT to exclude SCI from other requirements? Specifically, this exclusion appears to not require a PSP or ESP for SCI.</p>	
Likes	0
Dislikes	0
Response	
Joni Jones - Wabash Valley Power Association - 1	
Answer	Yes
Document Name	
Comment	
no further comments	
Likes	0
Dislikes	0
Response	
George Brown - Acciona Energy North America - 5	
Answer	Yes
Document Name	
Comment	
<p>Acciona Energy supports Midwest Reliability Organization's (MRO) NERC Standards Review Forum's (NSRF) comments on this question.</p>	
Likes	0
Dislikes	0
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	

Answer	Yes
Document Name	
Comment	
MPC supports comments submitted by the MRO NERC Standards Review Forum (NSRF).	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Texas RE suggests the language “except during CIP Exceptional Circumstances” in CIP-006 Part 2.2 can be removed as it is part of the parent Requirement R2 and thus applies to all parts.	
Likes 0	
Dislikes 0	
Response	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
AZPS agrees with the proposed changes to the additional CIP standards contained within Project 2016-02.	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - SERC,RF	
Answer	Yes
Document Name	

Comment

We agree with the proposed changes.

Likes 0

Dislikes 0

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

Yes

Document Name**Comment**

CEHE agrees with the conforming changes to the remaining requirements.

Likes 0

Dislikes 0

Response**JT Kuehne - AEP - 6****Answer**

Yes

Document Name**Comment**

AEP supports the proposed changes in CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013. AEP also suggests minor edit by adding the word "are" in Attachment 2 to CIP-003-Y, Section 3, item 1, "... that the Responsible Entity deems necessary, except where an entity provides rationale that communications **are** between Protection Systems."

Likes 0

Dislikes 0

Response**Bridget Silvia - Sempra - San Diego Gas and Electric - 3****Answer**

Yes

Document Name**Comment**

SDG&E supports EEI's comments:

CIP-003 – EEI supports the proposed changes made to CIP-003. (Note the proposed change to Attachment 1 was incorporated into the standard.)

CIP-004 – EEI supports the proposed changes made to CIP-004.

CIP-006 – EEI supports the proposed changes made to CIP-006

CIP-008 – EEI supports the proposed changes made to CIP-008, however, the phrase “SCI supporting an Applicable System in this Part” is missing from Requirement R2, subpart 2.3.

CIP-009 – EEI supports the proposed changes made to CIP-009.

CIP-011 – EEI supports the proposed changes made in CIP-011.

CIP-013 – EEI supports the proposed changes made in CIP-013.

Likes 0

Dislikes 0

Response

patricia ireland - DTE Energy - 4

Answer

Yes

Document Name

Comment

Patty Ireland on behalf of DTE Energy, Segments 3 and 4

Likes 0

Dislikes 0

Response

Jennifer Malon - Jennifer Malon On Behalf of: Brooke Voorhees, Black Hills Corporation, 3, 5, 1, 6; Derek Silbaugh, Black Hills Corporation, 3, 5, 1, 6; Don Stahl, Black Hills Corporation, 3, 5, 1, 6; Seth Nelson, Black Hills Corporation, 3, 5, 1, 6; - Jennifer Malon

Answer

Yes

Document Name

Comment

It would be helpful with large scale changes such as this to be able to see an example/draft of the new ERT that could be released to track the new information required.

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Comments: We agree with limiting the changes in CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013 to only what is needed to conform with the changes in CIP-005, CIP-007, and CIP-010. We believe this is a far more efficient and implementable approach.

Likes 0

Dislikes 0

Response

Maggy Powell - Amazon Web Services - 7

Answer Yes

Document Name

Comment

N/A

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Southern supports the changes made to CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013.

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

CIP-003 – EEI supports the proposed changes made to CIP-003. (Note the proposed change to Attachment 1 was incorporated into the standard.)

CIP-004 – EEI supports the proposed changes made to CIP-004.

CIP-006 – EEI supports the proposed changes made to CIP-006

CIP-008 – EEI supports the proposed changes made to CIP-008, however, the phrase “SCI supporting an Applicable System in this Part” is missing from Requirement R2, subpart 2.3.

CIP-009 – EEI supports the proposed changes made to CIP-009.

CIP-011 – EEI supports the proposed changes made in CIP-011.

CIP-013 – EEI supports the proposed changes made in CIP-013.

Likes 0

Dislikes 0

Response

John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1

Answer Yes

Document Name

Comment

Tacoma Power suggests reinstating a modified version of CIP-006 R1 Part 1.10 to exclude the Super ESP concepts, referring to one geographical location work with the Exemption 4.2.3.3 language.

Suggested CIP-006 R1.10 modification:

“Restrict physical access to cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same geographic location and Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter.”

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

The current draft is significantly more digestable than previous drafts by limiting changes to the other less technical standards and fits today's current configurations while allowing flexibility for new and future technologies.

Likes 0

Dislikes 0

Response

Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC) 2016-02 Virtualization (Draft 3)

Answer Yes

Document Name

Comment

The SRC does not have concern with these proposed conforming changes and agrees with them.

SPP did not participate in this response.

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 comments submitted by EEI

Likes 0

Dislikes 0

Response

Kimberly Turco - Constellation - 6

Answer Yes

Document Name

Comment

Constellation has elected to align with Exelon in response to this question.

Kim Turco, on behalf of Constellation Segments 5 and 6

Likes 0

Dislikes 0

Response

Alison Mackellar - Constellation - 5

Answer Yes

Document Name

Comment

Constellation has elected to align with Exelon in response to this question.

Kim Turco, on behalf of Constellation Segments 5 and 6

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 Hirschak, 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

See EEI comment.

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

AEPCO is signing on to ACES comments below.

ACES Comments: The current draft is significantly more digestable than previous drafts by limiting changes to the other less technical standards and fits today's current configurations while allowing flexibility for new and future technologies.

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

Alliant Energy supports the comments submitted by the MRO NSRF.

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

We agree with limiting the changes in CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013 to only what is needed to conform with the changes in CIP-005, CIP-007, and CIP-010. We believe this is a far more efficient and implementable approach.

Likes 0

Dislikes 0

Response

Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,5 - RF

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

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

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

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

Ryan Strom - Buckeye Power, Inc. - 5

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Joseph Amato - Joseph Amato On Behalf of: Darnez Gresham, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Joseph Amato

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	
Justin Welty - NextEra Energy - Florida Power and Light Co. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bryan Koyle - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Dwanique Spiller - Dwanique Spiller On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Berkshire Hathaway - NV Energy - 5 - WECC

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Donald Lock - Talen Generation, LLC - 5

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Hien Ho - Tacoma Public Utilities (Tacoma, WA) - 4

Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Amy Wesselkamper - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes	0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Glen Farmer - Avista - Avista Corporation - 5

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Jesus Sammy Alcaraz - Imperial Irrigation District - 1

Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Likes	0

Dislikes 0

Response

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

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

Justin MacDonald - Midwest Energy, Inc. - 1

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

Scott Kinney - Avista - Avista Corporation - 3

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Daniel Gacek - Exelon - 1

Answer

Document Name

Comment

Exelon will align with EEI in response to this question.

Likes 0

Dislikes 0

Response

Kinte Whitehead - Exelon - 3

Answer

Document Name

Comment

Exelon will align with EEI in response to this question.

Likes 0

Dislikes 0

Response

12. The SDT has revised numerous VSL's for simplification. Do you agree with the proposed changes? If not, please provide the basis for your disagreement.

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6

Answer No

Document Name

Comment

We agree with the approach to simplify the VSLs. However, some updates are needed.

CIP-003: lower VSL, R2 – delete “but” (The Responsible Entity but failed to manage its Transient Cyber Asset(s)...)”

CIP-004: For CIP-004, the SDT is proposing adding new VSLs for R4.1. The suggested additions read, “The Responsible Entity did not authorize electronic access or unescorted physical access based on need for” one, two, etc. individuals. We think the intent here is that Responsible Entities are out of compliance if they provide electronic or unescorted physical access without properly processing the individual(s) through the established CIP-004 access management program. The added VSLs as written, however, imply the opposite, that a Responsible Entity is out of compliance if they ever refuse access. We urge the SDT to clarify the wording of these VSLs.

Further on CIP-004 VSLs for R4.1, the VSLs should begin under the Lower category (not Moderate), and the SDT should consider revising how many individuals are in each category (ex. one to two for Lower, three to five for Moderate, six to nine for High, anything over that for Severe). Alternatively, rather than classify the VSL by number of individuals, perhaps it should instead be based on length of time that the violation occurred. If 10 individuals are accidentally granted unescorted physical access but only for an hour or less, that may not be a severe risk. If a single individual has erroneously had electronic access for over a year, that's a different matter entirely.

For CIP-004 R6, the last item in moderate VSL is missing “not.”

CIP-005: R1.3 severe VSL needs “per cyber asset capability” added. The reference to “method to protect data traversing” item should be Part 1.4, not Part 1.3.

CIP-007 R4.3 high VSL needs to have “per cyber asset capability” added.

Likes 0

Dislikes 0

Response

Thomas Breene - WEC Energy Group, Inc. - 3

Answer No

Document Name

Comment

We are in agreement with NSRFs comments regarding VSLs.

Likes 0

Dislikes 0

Response

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

Answer No

Document Name

Comment

CIP-010-5 R1 VSL, the first violation under Moderate VSL and High VSL are worded exactly the same. In CIP-010-4 the difference is leaving out 3/5 baseline elements vs 2/5 baseline elements. Without this quantitative distinction, it is difficult to determine VLS for potential non-compliance.

Likes 0

Dislikes 0

Response

Dwanique Spiller - Dwanique Spiller On Behalf of: Kevin Salisbury, Berkshire Hathaway - NV Energy, 5; - Berkshire Hathaway - NV Energy - 5 - WECC

Answer No

Document Name

Comment

We agree with the approach to simplify the VSLs. However, some updates are needed.

- CIP-003: lower VSL, R2 – delete “but” (The Responsible Entity but failed to manage its Transient Cyber Asset(s)...)”
- CIP-004: For CIP-004, the SDT is proposing adding new VSLs for R4.1. The suggested additions read, “The Responsible Entity did not authorize electronic access or unescorted physical access based on need for” one, two, etc. individuals. We think the intent here is that Responsible Entities are out of compliance if they provide electronic or unescorted physical access without properly processing the individual(s) through the established CIP-004 access management program. The added VSLs as written, however, imply the opposite, that a Responsible Entity is out of compliance if they ever refuse access. We urge the SDT to clarify the wording of these VSLs.
- Further on CIP-004 VSLs for R4.1, the VSLs should begin under the Lower category (not Moderate), and the SDT should consider revising how many individuals are in each category (ex. one to two for Lower, three to five for Moderate, six to nine for High, anything over that for Severe). Alternatively, rather than classify the VSL by number of individuals, perhaps it should instead be based on length of time that the violation occurred. If 10 individuals are accidentally granted unescorted physical access but only for an hour or less, that may not be a severe risk. If a single individual has erroneously had electronic access for over a year, that’s a different matter entirely.
- For CIP-004 R6, the last item in moderate VSL is missing “not.”
- CIP-005: R1.3 severe VSL needs “per cyber asset capability” added. The reference to “method to protect data traversing” item should be Part 1.4, not Part 1.3.
- CIP-007 R4.3 high VSL needs to have “per cyber asset capability” added.

Likes 0

Dislikes 0

Response

Joseph Amato - Joseph Amato On Behalf of: Darnez Gresham, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Joseph Amato

Answer No

Document Name

Comment

We agree with the approach to simplify the VSLs. However, some updates are needed.

CIP-003: lower VSL, R2 – delete “but” (The Responsible Entity but failed to manage its Transient Cyber Asset(s)…”

CIP-004: For CIP-004, the SDT is proposing adding new VSLs for R4.1. The suggested additions read, “The Responsible Entity did not authorize electronic access or unescorted physical access based on need for” one, two, etc. individuals. We think the intent here is that Responsible Entities are out of compliance if they provide electronic or unescorted physical access without properly processing the individual(s) through the established CIP-004 access management program. The added VSLs as written, however, imply the opposite, that a Responsible Entity is out of compliance if they ever refuse access. We urge the SDT to clarify the wording of these VSLs.

Further on CIP-004 VSLs for R4.1, the VSLs should begin under the Lower category (not Moderate), and the SDT should consider revising how many individuals are in each category (ex. one to two for Lower, three to five for Moderate, six to nine for High, anything over that for Severe). Alternatively, rather than classify the VSL by number of individuals, perhaps it should instead be based on length of time that the violation occurred. If 10 individuals are accidentally granted unescorted physical access but only for an hour or less, that may not be a severe risk. If a single individual has erroneously had electronic access for over a year, that’s a different matter entirely.

For CIP-004 R6, the last item in moderate VSL is missing “not.”

CIP-005: R1.3 severe VSL needs “per cyber asset capability” added. The reference to “method to protect data traversing” item should be Part 1.4, not Part 1.3.

CIP-007 R4.3 high VSL needs to have “per cyber asset capability” added.

Likes 0

Dislikes 0

Response

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

Answer No

Document Name

Comment

We agree with the approach to simplify the VSLs. However, some updates are needed.

CIP-003: lower VSL, R2 – delete “but” (The Responsible Entity but failed to manage its Transient Cyber Asset(s)…”

CIP-004: For CIP-004, the SDT is proposing adding new VSLs for R4.1. The suggested additions read, “The Responsible Entity did not authorize electronic access or unescorted physical access based on need for” one, two, etc. individuals. We think the intent here is that Responsible Entities are out of compliance if they provide electronic or unescorted physical access without properly processing the individual(s) through the established CIP-004

access management program. The added VSLs as written, however, imply the opposite, that a Responsible Entity is out of compliance if they ever refuse access. We urge the SDT to clarify the wording of these VSLs.

Further on CIP-004 VSLs for R4.1, the VSLs should begin under the Lower category (not Moderate), and the SDT should consider revising how many individuals are in each category (ex. one to two for Lower, three to five for Moderate, six to nine for High, anything over that for Severe). Alternatively, rather than classify the VSL by number of individuals, perhaps it should instead be based on length of time that the violation occurred. If 10 individuals are accidentally granted unescorted physical access but only for an hour or less, that may not be a severe risk. If a single individual has erroneously had electronic access for over a year, that's a different matter entirely.

For CIP-004 R6, the last item in moderate VSL is missing “not.”

CIP-005: R1.3 severe VSL needs “per cyber asset capability” added. The reference to “method to protect data traversing” item should be Part 1.4, not Part 1.3.

CIP-007 R4.3 high VSL needs to have “per cyber asset capability” added.

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

We largely agree with the proposed changes but also urge the following changes.

For CIP-003: lower VSL, R2 – delete the word “but” (The Responsible Entity but failed to manage its Transient Cyber Asset(s)...)”

For CIP-004, the SDT is proposing adding new VSLs for R4.1. The suggested additions read, “The Responsible Entity did not authorize electronic access or unescorted physical access based on need for” one, two, etc. individuals. We think the intent here is that Responsible Entities are out of compliance if they provide electronic or unescorted physical access without properly processing the individual(s) through the established CIP-004 access management program. The added VSLs as written, however, imply the opposite, that a Responsible Entity is out of compliance if they ever refuse access. We urge the SDT to clarify the wording of these VSLs.

Further on CIP-004 VSLs for R4.1, the VSLs should begin under the Lower category (not Moderate), and the SDT should consider revising how many individuals are in each category (ex. one to two for Lower, three to five for Moderate, six to nine for High, anything over that for Severe). Alternatively, rather than classify the VSL by number of individuals, perhaps it should instead be based on length of time that the violation occurred. If 10 individuals are accidentally granted unescorted physical access but only for an hour or less, that may not be a severe risk. If a single individual has erroneously had electronic access for over a year, that's a different matter entirely.

For CIP-005, the R1.3 severe VSL should have “per system capability” added. The reference to “method to protect data traversing” item should be Part 1.4, not Part 1.3.

For CIP-007, the R4.3 high VSL should have “per system capability” added.

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

Alliant Energy supports the comments submitted by the MRO NSRF.

Likes 0

Dislikes 0

Response

Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirschak, 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

See EEI comment.

Likes 0

Dislikes 0

Response

Alison Mackellar - Constellation - 5

Answer

Yes

Document Name

Comment

Constellation has elected to align with Exelon in response to this question.

Kim Turco, on behalf of Constellation Segments 5 and 6

Likes 0

Dislikes 0

Response

Kimberly Turco - Constellation - 6

Answer

Yes

Document Name

Comment

Constellation has elected to align with Exelon in response to this question.

Kim Turco, on behalf of Constellation Segments 5 and 6

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 comments submitted by EEI

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

We agree with the new language. It is easier to read when VSLs explain what should have been done (per Requirements) but was not done.

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

EEl agrees with the proposed revisions to the VSLs.

Likes 0

Dislikes 0

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1

Answer

Yes

Document Name

Comment

We support NPCC TFIST comments..

We agree with the new language. It is easier to read when VSLs explain what should have been done (per Requirements) but was not done.

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

We agree with the new language. It is easier to read when VSLs explain what should have been done (per Requirements) but was not done.

Likes 0

Dislikes 0

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer

Yes

Document Name

Comment

IESO supports the comments provided by NPCC and IRC

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 changes to the VSLs.

Likes 0

Dislikes 0

Response

Maggy Powell - Amazon Web Services - 7

Answer

Yes

Document Name

Comment

N/A

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Comments: We largely agree with the proposed changes but also urge the following changes.

For CIP-003: lower VSL, R2 – delete the word “but” (The Responsible Entity but failed to manage its Transient Cyber Asset(s)…”

For CIP-004, the SDT is proposing adding new VSLs for R4.1. The suggested additions read, “The Responsible Entity did not authorize electronic access or unescorted physical access based on need for” one, two, etc. individuals. We think the intent here is that Responsible Entities are out of compliance if they provide electronic or unescorted physical access without properly processing the individual(s) through the established CIP-004 access management program. The added VSLs as written, however, imply the opposite, that a Responsible Entity is out of compliance if they ever refuse access. We urge the SDT to clarify the wording of these VSLs.

Further on CIP-004 VSLs for R4.1, the VSLs should begin under the Lower category (not Moderate), and the SDT should consider revising how many individuals are in each category (ex. one to two for Lower, three to five for Moderate, six to nine for High, anything over that for Severe). Alternatively, rather than classify the VSL by number of individuals, perhaps it should instead be based on length of time that the violation occurred. If 10 individuals are accidentally granted unescorted physical access but only for an hour or less, that may not be a severe risk. If a single individual has erroneously had electronic access for over a year, that’s a different matter entirely.

For CIP-005, the R1.3 severe VSL should have “per system capability” added. The reference to “method to protect data traversing” item should be Part 1.4, not Part 1.3.

For CIP-007, the R4.3 high VSL should have “per system capability” added.

Likes 0

Dislikes 0

Response

Carl Pineault - Hydro-Quebec Production - 5

Answer Yes

Document Name

Comment

We agree with the new language. It is easier to read when VSLs explain what should have been done (per Requirements) but was not done.

Likes 0

Dislikes 0

Response

patricia ireland - DTE Energy - 4

Answer Yes

Document Name

Comment

Patty Ireland on behalf of DTE Energy, Segments 3 and 4

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

We agree with the new language. It is easier to read when VSLs explain what should have been done (per Requirements) but was not done.

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

CEHE agrees with the approach to simplify the VSL's.

Likes 0

Dislikes 0

Response

Ellese Murphy - Duke Energy - 1,3,5,6 - SERC,RF

Answer Yes

Document Name	
Comment	
We agree with the proposed changes.	
Likes 0	
Dislikes 0	
Response	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
AZPS agrees with the proposed changes to the VSLs.	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
MPC supports comments submitted by the MRO NERC Standards Review Forum (NSRF).	
Likes 0	
Dislikes 0	
Response	
George Brown - Acciona Energy North America - 5	
Answer	Yes
Document Name	
Comment	

Acciona Energy supports Midwest Reliability Organization's (MRO) NERC Standards Review Forum's (NSRF) comments on this question.

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Scott Kinney - Avista - Avista Corporation - 3

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

Justin MacDonald - Midwest Energy, Inc. - 1

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Mike Magruder - Avista - Avista Corporation - 1

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 3

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Jesus Sammy Alcaraz - Imperial Irrigation District - 1

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Glen Farmer - Avista - Avista Corporation - 5

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name SPP RTO

Answer Yes

Document Name

Comment	
Likes 0	
Dislikes 0	
Response	
Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
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	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
William Steiner - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Jennifer Malon - Jennifer Malon On Behalf of: Brooke Voorhees, Black Hills Corporation, 3, 5, 1, 6; Derek Silbaugh, Black Hills Corporation, 3, 5, 1, 6; Don Stahl, Black Hills Corporation, 3, 5, 1, 6; Seth Nelson, Black Hills Corporation, 3, 5, 1, 6; - Jennifer Malon	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Hien Ho - Tacoma Public Utilities (Tacoma, WA) - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donald Lock - Talen Generation, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bridget Silvia - Sempra - San Diego Gas and Electric - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response

JT Kuehne - AEP - 6

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Bryan Koyle - Southern Indiana Gas and Electric Co. - 3,5,6 - RF

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response**Josh Johnson - Lincoln Electric System - 1****Answer**

Yes

Document Name**Comment**

Likes 0

Dislikes 0

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

Yes

Document Name**Comment**

Likes 0

Dislikes 0

Response**Richard Jackson - U.S. Bureau of Reclamation - 1****Answer**

Yes

Document Name**Comment**

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Ryan Strom - Buckeye Power, Inc. - 5

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Mike Marshall - IDACORP - Idaho Power Company - 1

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Patricia Lynch - NRG - NRG Energy, 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

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,5 - RF

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Kinte Whitehead - Exelon - 3

Answer	
Document Name	
Comment	
Exelon will align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	
Exelon will align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	
Document Name	
Comment	
NST has no comment.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	

Comment

Texas RE noticed CIP-005 is missing VSLs for CIP-005 R1.4.

Likes 0

Dislikes 0

Response

13. The SDT has revised the Implementation Plan to include the Planned and Unplanned Changes provisions and to allow for early adoption. Do you agree with the proposed Implementation Plan? If not, please provide the basis for your disagreement and an alternate proposal.

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

Answer No

Document Name

Comment

Time frames to implement seem to be rather constrained. Propose 36 months.

Likes 0

Dislikes 0

Response

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

Answer No

Document Name

Comment

- NEE is requesting the implementation period be extended to 36-months. Supply chain risks including parts and staffing availability impact the implementation especially for large entities required to support multiple locations, divergent technologies and large geographical areas spanning multiple NERC regions. Managing the tiered implementation creates risk for enterprise based procedures and training spanning multiple NERC registrations supporting all the impact ratings applicable to the updated NERC CIP standards.
- Currently implemented technology limitations prevent compliance in some instances requiring complex projects coordinated with multiple vendors and suppliers which are estimated to take at minimum 24-months, for example to address the SCI shared memory and CPU requirements. Replacement of capital hardware and depreciation can have adverse economic costs for Cyber Assets approved in rate cases and on existing financial depreciation schedules.
- Another recommendation worthy of consideration would allow for grandfathering of some equipment out to 36 or 46 months for replacement of equipment to apply the new definitions and requirements.

Likes 0

Dislikes 0

Response

JT Kuehne - AEP - 6

Answer No

Document Name

Comment

AEP recommends adding a time frame for the planned changes to account for planned changes that may not have enough lead time because of last minute changes. Therefore, AEP recommends modifying the first sentence as follows, "Planned changes, **further out than 12-month**, refer to any changes of the electric system or BES Cyber System which were planned and implemented by the Responsible Entity and subsequently identified through the annual assessment under CIP-002-7, Requirement R2." And for the unplanned changes, AEP recommends adding transfer of ownership as an unplanned change and add it to the "Scenario of Unplanned Changes After the Effective Date" table of the implementation plan with a 24-month compliance implementation.

Likes 0

Dislikes 0

Response

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

Answer

No

Document Name

Comment

Although we agree with the option of early adoption, PNMR recommends extending the implementation. Highly complex and wholesale changes across all standards creates significant burden to utilities. Just the learning curve to fully understand the standards may be excessive. Expertise and resource availability adds additional risk to compliance. This requires a paradigm shift in security and compliance management. We would expect significant and ongoing outreach and training. Due to the complexity, PNMR would recommend 36 month implementation timeline.

Likes 0

Dislikes 0

Response

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

Answer

No

Document Name

Comment

Given the number and extend of the changes to the Reliability Standards to support virtualization, the time and cost to budget for and purchase additional equipment, and because there could be significant architectural changes to an entity's network infrastructure, SMUD would propose a longer implementation plan of 36-months. This would ensure that entities have proper time to design, fund, implement, document, and adjust training associated with the proposed changes. A 24-month implementation might work for entities that need to make only minor adjustments, but 24 months could be difficult to meet for entities that are currently co-mingling SCI resources on a much larger scale.

Likes 0

Dislikes 0

Response

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

Answer No

Document Name

Comment

We question if 12 months is sufficient when the entity has a significant increase in High or Medium Impact.

Likes 0

Dislikes 0

Response

Kimberly Turco - Constellation - 6

Answer No

Document Name

Comment

Constellation has elected to align with Exelon in response to this question.

Kim Turco, on behalf of Constellation Segments 5 and 6

Likes 0

Dislikes 0

Response

Alison Mackellar - Constellation - 5

Answer No

Document Name

Comment

Constellation has elected to align with Exelon in response to this question.

Kim Turco, on behalf of Constellation Segments 5 and 6

Likes 0

Dislikes 0

Response

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

Answer

No

Document Name

Comment

Likes 0

Dislikes 0

Response

Joni Jones - Wabash Valley Power Association - 1

Answer

Yes

Document Name

Comment

no further comments

Likes 0

Dislikes 0

Response

George Brown - Acciona Energy North America - 5

Answer

Yes

Document Name

Comment

Acciona Energy supports Midwest Reliability Organization's (MRO) NERC Standards Review Forum's (NSRF) comments on this question.

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

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

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

AZPS agrees with he proposed Implementation Plan.

Likes 0

Dislikes 0

Response

Ellese Murphy - Duke Energy - 1,3,5,6 - SERC,RF

Answer

Yes

Document Name

Comment

We agree with the proposed changes.

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

CEHE agrees with the revised implementation plan.

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

Generally, we agree with the revised Implementation Plan but request the SDT consider if 12 months is sufficient when the entity has a significant increase (change) in High or Medium Impact Level.

Likes 0

Dislikes 0

Response

patricia ireland - DTE Energy - 4

Answer Yes

Document Name

Comment

Patty Ireland on behalf of DTE Energy, Segments 3 and 4

Likes 0

Dislikes 0

Response

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

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	Yes
Document Name	
Comment	
Generally, we agree with the revised Implementation Plan but request the SDT consider if 12 months is sufficient when the entity has a significant increase (change) in High or Medium Impact Level.	
Likes 0	
Dislikes 0	
Response	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	
This is related to unplanned changes to asset classifications, not unplanned (Emergency) changes, thus no issues for IT Change Management (PEB)	
Likes 0	
Dislikes 0	
Response	
Maggy Powell - Amazon Web Services - 7	
Answer	Yes

Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern supports the revised Implementation Plan.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
IESO supports the comments provided by NPCC and IRC	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	Yes
Document Name	
Comment	

Generally, we agree with the revised Implementation Plan but request the SDT consider if 12 months is sufficient when the entity has a significant increase (change) in High or Medium Impact Level.

Likes 0

Dislikes 0

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1

Answer

Yes

Document Name

Comment

We support NPCC TFIST comments.

Generally, we agree with the revised Implementation Plan but request the SDT consider if 12 months is sufficient when the entity has a significant increase (change) in High or Medium Impact Level.

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

EI supports the proposed Implementation Plan.

Likes 0

Dislikes 0

Response

Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC) 2016-02 Virtualization (Draft 3)

Answer

Yes

Document Name

Comment

The SRC does not have concern with the revised Implementation Plan and agrees with the proposed change.

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

ITC supports the comments submitted by EEI

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 Hirschak, 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

See EEI comment.

Likes 0

Dislikes 0

Response

Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,5 - RF

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Wagner - Santee Cooper - 1,3,5,6, Group Name Santee Cooper	
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	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Mike Marshall - IDACORP - Idaho Power Company - 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	
Ryan Strom - Buckeye Power, Inc. - 5	
Answer	Yes
Document Name	

Comment

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Joseph Amato - Joseph Amato On Behalf of: Darnez Gresham, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Joseph Amato

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

Josh Johnson - Lincoln Electric System - 1

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Bryan Koyle - Southern Indiana Gas and Electric Co. - 3,5,6 - RF

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Dwanique Spiller - Dwanique Spiller On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Berkshire Hathaway - NV Energy - 5 - WECC

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Donald Lock - Talen Generation, LLC - 5

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Hien Ho - Tacoma Public Utilities (Tacoma, WA) - 4

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Jennifer Malon - Jennifer Malon On Behalf of: Brooke Voorhees, Black Hills Corporation, 3, 5, 1, 6; Derek Silbaugh, Black Hills Corporation, 3, 5, 1, 6; Don Stahl, Black Hills Corporation, 3, 5, 1, 6; Seth Nelson, Black Hills Corporation, 3, 5, 1, 6; - Jennifer Malon

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

William Steiner - Midwest Reliability Organization - 10

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

Likes 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

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name SPP RTO

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Thomas Breene - WEC Energy Group, Inc. - 3

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response**Glen Farmer - Avista - Avista Corporation - 5****Answer**

Yes

Document Name**Comment**

Likes 0

Dislikes 0

Response**Jesus Sammy Alcaraz - Imperial Irrigation District - 1****Answer**

Yes

Document Name**Comment**

Likes 0

Dislikes 0

Response**David Jendras - Ameren - Ameren Services - 3****Answer**

Yes

Document Name**Comment**

Likes 0

Dislikes 0

Response

James Baldwin - Lower Colorado River Authority - 1

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

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

Justin MacDonald - Midwest Energy, Inc. - 1

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

Scott Kinney - Avista - Avista Corporation - 3

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

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

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

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer

Document Name

Comment

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

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

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

However, the first and third paragraphs in the proposed implementation plan appears to conflict with this reading. Specifically, the first paragraph states: "Planned changes refer to any changes of the electric system or BES Cyber System which were planned and implemented by the Responsible Entity and subsequently identified through the annual assessment under CIP-002-7, Requirement R2." Furthermore, the proposed implementation plan's third paragraph states: "For planned changes resulting in a higher categorization, the Responsible Entity shall comply with all applicable requirements in the CIP Cyber Security Standards on the update of the identification and categorization of the affected BES Cyber System and any applicable and associated Physical Access Control Systems, Electronic Access Control and Monitoring Systems and Protected Cyber Assets, with

additional time to comply for requirements in the same manner as those timelines specified in the section Initial Performance of Certain Periodic Requirements of the CIP-002-7 Implementation Plan.”

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

Regarding the proposed implementation plan’s concerning unplanned changes, Texas RE is concerned the language could be read to result in a reliability gap. Specifically, the first paragraph of the implementation plan states “Unplanned changes refer to any changes of the electric system or BES Cyber System which were not planned by the Responsible Entity and subsequently identified through the annual assessment under CIP-002-7, Requirement R2.”

Texas RE notes that while it is true that during a CIP-002 R2 review an entity may discover that a BCS now meets a higher BCS threshold than it previously held, this is not the only situation in which an entity may become aware of the need for a higher categorization. For example, if an entity is informed by their RC, PC, or TP that an asset is critical to the derivation of an IROL then the knowledge that the systems must meet the medium impact criteria is immediate and as such the 12-month timer to implement medium impact controls should begin immediately. As written, the language in the implementation plan could result in a situation where a Registered Entity could delay the implementation of medium impact controls at such a substation or power plant for up to 27 calendar months, if the IROL notification arrived immediately after a CIP-002 R2 evaluation. Texas RE recommends the SDT revise the proposed implementation plan language around “unplanned changes” to preclude this result.

Likes 0

Dislikes 0

Response

Daniel Gacek - Exelon - 1

Answer

Document Name

Comment

Exelon would like the Standard Drafting Team to consider a 36-month implementation plan prior to enforcement.

Likes 0

Dislikes 0

Response

Kinte Whitehead - Exelon - 3

Answer	
Document Name	
Comment	
	Exelon would like the Standard Drafting Team to consider a 36-month implementation plan prior to enforcement.
Likes 0	
Dislikes 0	
Response	

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

David Rudolph - Basin Electric Power Cooperative - 1

Answer

Document Name

Comment

By eliminating the language for BCSI repositories, complying with the new CIP-004_R6 will be nearly impossible.

Likes 0

Dislikes 0

Response

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

Answer

Document Name

Comment

Alliant Energy supports the comments submitted by the MRO NSRF.

Likes 0

Dislikes 0

Response

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

Answer

Document Name

Comment

Thank you for the opportunity to provide feedback.

Likes 0

Dislikes 0

Response

Selene Willis - Edison International - Southern California Edison Company - 5

Answer

Document Name

Comment

“See comments submitted by the Edison Electric Institute”

Likes 0

Dislikes 0

Response

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

Alison Mackellar - Constellation - 5

Answer

Document Name

Comment

Constellation has elected to align with Exelon in response to this question.

Kim Turco, on behalf of Constellation Segments 5 and 6

Likes 0

Dislikes 0

Response

Kimberly Turco - Constellation - 6**Answer****Document Name****Comment**

Constellation has elected to align with Exelon in response to this question.

Kim Turco, on behalf of Constellation Segments 5 and 6

Likes 0

Dislikes 0

Response**Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott****Answer****Document Name****Comment**

ITC has received this comment from one of our departments:

As far as the implantation plan.. I'd like some more clarity that the 'upon commission' language has been removed from planned changes and the CIP standards only apply to impacted planned changes upon completion of the next annual assessment.

Likes 0

Dislikes 0

Response**Brian Evans-Mongeon - Utility Services, Inc. - 4****Answer****Document Name****Comment**

There is inconsistent capatilization of Applicable Systems (CIP-005 R3.2, CIP-013 VSL)

Likes 0

Dislikes 0

Response

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

Answer

Document Name

Comment

We would like to thank the Project 2016-02 SDT on their hard work, dedication, and continuing to listen to industry feedback to meet the FERC order and not create significantly more compliance burden.

Likes 0

Dislikes 0

Response

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

Answer

Document Name

Comment

- In some Reliability Standards, acronyms are used prior to expanding them at first use (e.g. VCA, SCI, etc.).
- In some cases acronyms are expanded (e.g. EACMS and PACS) and other times the acronyms are used (e.g. BCS, TCA).
- Sometime the term BCS is used and other times the term BCA is used (especially around device capability)
- Moving some of the requirement language in the existing Reliability Standards to the “measures” section of the proposed new Standards is confusing (e.g. specifically CIP-010 R1.1). It’s unclear what security controls from CIP-005 and CIP-007 are supposed to be tracked in the new requirement. Only in the measures section does it mention anything about elements to monitor, however, none of those items exist in CIP-005 or CIP-007. This makes the controls vague because the details are no longer in CIP-005 and CIP-007.
- The current wording in CIP-010 is preferred over the proposed language.
- There are changes to requirements that do not seem to directly support virtualization technologies. The focus should be putting SCI and Management Interfaces in the applicability sections and only changing the requirements where necessary to support virtualization (e.g. CIP-005).

Likes 0

Dislikes 0

Response

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6

Answer

Document Name

Comment

We compliment the standard drafting team on great progress at addressing industry comments submitted during the last posting. While we are providing few comments on the standards themselves, we believe some changes are needed to several definitions. Since there is no ballot for the definitions alone, we will be voting negative on CIP-005, the standard that we think is most affected by issues with the definitions.

We request that NERC propose consolidation of the effective dates for CIP-004-7 and CIP-011-3 with the effective dates of this project. This would reduce the administrative burden of having to implement multiple versions for these two standards within a short time period.

Likes 0

Dislikes 0

Response

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

Answer

Document Name

Comment

EEl would like to convey our sincere appreciation to the Project 2016-02 Standards Drafting Team for their diligent efforts and dedication to excellence throughout this long and difficult project. We would also like to assure all of you that your efforts and hard work have not gone unnoticed by EEI and the industry broadly. Many thanks to all of you!

Likes 0

Dislikes 0

Response

Kinte Whitehead - Exelon - 3

Answer

Document Name

Comment

Exelon will align with EEI in response to this question.

Likes 0

Dislikes 0

Response

Daniel Gacek - Exelon - 1

Answer

Document Name

Comment

Exelon will align with EEI in response to this question.

Likes 0

Dislikes 0

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer

Document Name

Comment

No additional comment

Likes 0

Dislikes 0

Response

Maggy Powell - Amazon Web Services - 7

Answer

Document Name

Comment

The SDT is clear that this project SAR focuses on on-premise virtualization, however, many virtualization concepts convey use of cloud. AWS suggests explicitly stating whether these new terms/requirements, specifically SCI, will apply to cloud or not. If these terms/requirements do not apply to cloud, it should be obvious to the reader.

Likes 0

Dislikes 0

Response

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

Answer

Document Name

Comment

Tri-State appreciates the hard work the drafting team did to incorporate industry feedback into this project.

Likes 0

Dislikes 0

Response

Lindsey Mannion - ReliabilityFirst - 10

Answer

Document Name

Comment

Conflating support for both High-, Medium-, and Low-Impact Cyber Assets within a single Virtualization Cluster could create confusion. Clusters by their very nature include pools of shared SCI to include CPU, Memory, Disk, and network resources that are shared between all Cluster members to allow for balancing resources, recovery from failed hardware, and maintaining high availability. The complexity required to balance these pooled resources and disallow different impact levels of VM guests from running on the same physical resources could be high. Moving VM guests can take place without the need for clustering and would allow for segregated siloing of different impact Cyber Assets without the requirement of determining high-water marking every time a VM guest is moved. Communications play a key role in determining the current health and configuration of clusters – especially with heartbeats and SCSI data requests. Responsible Entities have a high bar to assure that these communications are not to the point that they create common networking connections that would start to include additional VM Guests as PCA.

Likes 0

Dislikes 0

Response

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

Answer

Document Name

Comment

We compliment the Project 2016-02 Standard Drafting Team on being receptive to industry feedback, to rethinking past proposed revisions, and to proposing a path forward that we believe is as efficient and implementable as possible for allowing for technologies to be utilized for critical infrastructure protection.

Regarding the lack of a separate ballot for the definitions, we believe this is an oversight that needs to be corrected. The definitions are crucially important, particularly in this project. If not corrected, we request action by NERC to ensure that in future this circumstance does not recur.

Likes 0

Dislikes 0

Response

Carl Pineault - Hydro-Qu?bec Production - 5

Answer

Document Name

Comment

No additional comment

Likes 0

Dislikes 0

Response

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

Answer

Document Name

Comment

NST has no further comments.

Likes 0

Dislikes 0

Response

Jennifer Malon - Jennifer Malon On Behalf of: Brooke Voorhees, Black Hills Corporation, 3, 5, 1, 6; Derek Silbaugh, Black Hills Corporation, 3, 5, 1, 6; Don Stahl, Black Hills Corporation, 3, 5, 1, 6; Seth Nelson, Black Hills Corporation, 3, 5, 1, 6; - Jennifer Malon

Answer

Document Name

Comment

When large changes that add and remove requirements are performed on a standard we feel it would be very helpful to not re-use existing requirement numbers for very different requirements. For example CIP-005 has a large number of requirement numbers that drastically change the intent and requirement between the new and old versions. We fear that this could lead to confusion and potential for errors as both human memory and systems built to monitor specific requirements struggle to adapt to the drastic change in intent.

Likes 0

Dislikes 0

Response

Donald Lock - Talen Generation, LLC - 5

Answer

Document Name

Comment

The sea change being attempted in NERC's CIP definitions makes the success of the virtualization initiative highly dependent on clear communications, making significantly expanded explanations (with examples) appropriate, including clarifying that the new term, "Shared Cyber Infrastructure," applies to hypervisors and not GO-TO communications systems

Likes 0

Dislikes 0

Response

Dwanique Spiller - Dwanique Spiller On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Berkshire Hathaway - NV Energy - 5 - WECC

Answer

Document Name

Comment

We compliment the standard drafting team on great progress at addressing industry comments submitted during the last posting. While we are providing few comments on the standards themselves, we believe some changes are needed to several definitions. Since there is no ballot for the definitions alone, we will be voting negative on CIP-005, the standard that we think is most affected by issues with the definitions.

We request that NERC propose consolidation of the effective dates for CIP-004-7 and CIP-011-3 with the effective dates of this project. This would reduce the administrative burden of having to implement multiple versions for these two standards within a short time period.

Likes 0

Dislikes 0

Response

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

Answer

Document Name

Comment

N/A

Likes 0

Dislikes 0

Response

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

Answer

Document Name

Comment

CEHE believes requirements CIP-008 R3 and CIP-009 R3 are administrative in nature and do not add to reliability or security. Sub-requirements in R3 around 90-day and 60-day notifications have been more of an administrative burden than a reliability benefit. The parent requirement of having a plan and executing the plan every 15 calendar months should suffice. CEHE recommends the SDT re-evaluate these requirements for potential revision or retirement.

Likes 0

Dislikes 0

Response

Bryan Koyle - Southern Indiana Gas and Electric Co. - 3,5,6 - RF

Answer

Document Name

Comment

SIGE believes requirements CIP-008 R3 and CIP-009 R3 are administrative in nature and do not add to reliability or security. Sub-requirements in R3 around 90-day and 60-day notifications have been more of an administrative burden than a reliability benefit. The parent requirement of having a plan and executing the plan every 15 calendar months should suffice. CenterPoint Energy recommends the SDT re-evaluate these requirements for potential revision or retirement.

Likes 0

Dislikes 0

Response

Ellese Murphy - Duke Energy - 1,3,5,6 - SERC,RF

Answer

Document Name

Comment

We would like to thank the SDT for their hard work producing this draft. Duke Energy has no additional comments.

Likes 0

Dislikes 0

Response

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

Answer

Document Name

Comment

- CIP-002-7 Please update Technical Rationale and Justification for Reliability Standard replacing CIP-002-5.1 with CIP-002-7 in the Table of Contents and other references such as Appendix 1
- Please add references and application to Technical Rationale and Justification for Reliability Standard for the new SCI, VCA, CS, MI.

Likes 0

Dislikes 0

Response

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

Answer

Document Name

Comment

Reclamation recommends that improved resilience or reliability of the BES should be the primary consideration before an entity adopts any new or emerging technologies for BES reliability operating services.

Reclamation identifies that in the drafts for CIP-005 and CIP-010, the drafting team has inserted new requirements in the existing numbering structure (shifting subsequent numbers by +1). So, if the requirement was R3, and a new requirement was inserted before, R3 would now become R4 and so on. Or if a requirement was removed, the subsequent numbers are decreased accordingly. O&P standard drafting teams have deployed a method to mark deleted requirement numbers as "Reserved" to maintain the consistency of the number sequence. Reclamation recommends this practice be adopted for CIP standards and also recommends that if new requirements are added, they should be added at the end of the existing requirements to preserve

the existing v5 number sequence. If new requirements are added after a space in the sequence has opened, they can be inserted without changing the rest of the numbering.

Reclamation also recommends utilizing existing FedRAMP criteria and air gapping Industrial Control Systems from external communications where possible.

Reclamation appreciates the SDT's efforts to incorporate the NIST Framework into the NERC standards. Reclamation encourages the SDT to continue this practice moving forward to ensure that NERC standards and requirements do not duplicate the NIST Framework.

Likes 0

Dislikes 0

Response

Joseph Amato - Joseph Amato On Behalf of: Darnez Gresham, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Joseph Amato

Answer

Document Name

Comment

We compliment the standard drafting team on great progress at addressing industry comments submitted during the last posting. While we are providing few comments on the standards themselves, we believe some changes are needed to several definitions. Since there is no ballot for the definitions alone, we will be voting negative on CIP-005, the standard that we think is most affected by issues with the definitions.

We request that NERC propose consolidation of the effective dates for CIP-004-7 and CIP-011-3 with the effective dates of this project. This would reduce the administrative burden of having to implement multiple versions for these two standards within a short time period.

Likes 0

Dislikes 0

Response

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

Answer

Document Name

Comment

CHPD found in its review of Draft 3 drafting errors such as comma splices and other errors which lead to significant changes to the intended meaning. CHPD respectfully encourages the SDT to take the amount of time needed to ensure Standards read as intended.

With regards to the definition of PCA and CIP-007 R1.3, CHPD firmly believes there still has been no demonstrated risk of hardware-based virtualization attacks that warrant this requirement. CISA's [Known Exploited Vulnerabilities Catalog | CISA](#) only lists a single VM escape vulnerability, which was patched before it was disclosed, and is disputed by the vendor as being in the wild. While a number of VM escape techniques have been disclosed, all have been patched and saw no confirmed exploitation in the wild.

Even speculative execution vulnerabilities like Spectre and Meltdown have not seen any confirmed exploitation in the wild and are effectively patched. Future vulnerabilities can be effectively managed by a Responsible Entity's CIP-007 R2 patching program (or mitigated by a mitigation plan if patching is not possible) and CIP-010 R3 Vulnerability Assessment program. This requirement only serves to restrict entities on architectures and to increase the cost of virtualization making it untenable.

We can also look to NIST 800-125A, Security Recommendations for Server-based Hypervisor Platforms. While VM Process Isolation is considered the first and possibly most important of the baseline functions, preventing VMs from sharing CPU or memory is not listed as any of the security recommendations to secure hypervisor baseline functions.

Looking to the technical aspects, it is CHPD's opinion that this requirement misuses the functionality of DRS (or similar for non-VMware vendors) in ways that were not intended. DRS affinity rules were not intended as a cyber security tool to prevent side channel attacks, but are intended to ensure availability and performance of VMs, as DRS is fundamentally a tool to allocate distributed resources. There are typically three types of rules; VM-to-VM affinity rules which ensure VM stay together for performance reasons, VM-to-VM anti-affinity rules which ensure that VMs stay apart for redundancy reasons incase a host fails, and VM-to-host rules, which ensure that VMs either stay connected to a specific physical resource. Because DRS rulesets were not intended for security, affinity rules do not generally allow you to specify groups of VMs and cannot share CPU with another group of VMs. That means, for example, an EACMS VM would need to have a rule for every VM that it cannot share CPU and memory with to comply with this requirement. Even if a Responsible Entity were to do this, this would create a massive web of affinity rules that would be unmanageable and potentially create a reliability issue in the event of a hardware failure, where critical VMs might not be able to find a suitable host to run on given affinity restrictions.

Setting aside the security and technical problems, the requirement itself is not clear in what it allows. It is very easy to interpret the requirement as contradicting the definition of SCI. There is a very fine line drawn with the terminology in the definition of SCI ("cluster") and the wording of CIP-007 R1.3 (sharing of CPU and memory). Some might interpret the specific hosts allowed to host CIP devices (according to the affinity ruleset) as the "cluster", meaning that R1.3 essentially contradicts the definition of SCI. There is also the question of if a high watermarked BCA still counts as its Medium Impact self. Even though you must treat it as a high impact PCA, it is still fundamentally a medium impact BCA and according to the requirement, it cannot coexist on the same CPU and memory as it is of a different impact classification. The language of R1.3 combined with the definition of SCI creates too vague of a security control to implement without significant compliance risk.

Likes 0

Dislikes 0

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer

Document Name

Comment

Texas RE recommends including an acronyms section at the beginning of each standard so the terms are clear and consistent.

Likes 0

Dislikes 0

Response

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

Answer

Document Name

Comment

We compliment the standard drafting team on great progress at addressing industry comments submitted during the last posting. While we are providing few comments on the standards themselves, we believe some changes are needed to several definitions. Since there is no ballot for the definitions alone, we will be voting negative on CIP-005, the standard that we think is most affected by issues with the definitions.

We request that NERC propose consolidation of the effective dates for CIP-004-7 and CIP-011-3 with the effective dates of this project. This would reduce the administrative burden of having to implement multiple versions for these two standards within a short time period.

Likes 0

Dislikes 0

Response

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

Answer

Document Name

Comment

The SCI acronym has not been defined as "Shared Cyber Infrastructure" in the proposed CIP-002, CIP-005, CIP-007, CIP-009, or CIP-010 Standard revision. The drafting team may consider defining all acronyms or not defining any acronyms as conforming changes to promote consistency within the CIP Standards.

Likes 0

Dislikes 0

Response

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

Answer

Document Name

Comment

When will the Guidelines and Technical Basis that was removed from the Standards be available in the Technical Rationale or Implementation Guidance?

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

George Brown - Acciona Energy North America - 5

Answer

Document Name

Comment

Acciona Energy supports Midwest Reliability Organization's (MRO) NERC Standards Review Forum's (NSRF) comments on this question.

Likes 0

Dislikes 0

Response

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

Answer

Document Name

Comment

TFE

SRP has recognized that for the standards and requirements where technical feasibility exemptions currently exist, the language has been removed and now uses the verbiage "per system capability", this leads us to believe that requirements where TFE's were available will no longer have the ability to file a TFE. SRP recommends a definition be created explaining what "per system capability" is for BES cyber systems and associated cyber assets.

CIP-002-7

Would like confirmation how or if the Guidelines and Technical Basis for CIP-002 which includes the BROS will be changed. The section now states "This section contains a "cut and paste" of the former Guidelines and Technical Basis (GTB) as-is of from the CIP-002- 5.1a standard to preserve any historical references. No modifications have been made."

CIP-007-7

Need some clarification on CIP-007-7 R1.1. The previous rationale states that ports and services should be managed on the cyber asset level and not just on the firewall. The new rationale and wording seems a bit vague and can easily be interpreted that blocking ports and services can be done on a system level (i.e. the firewall of an ESP)

CIP-010-5

R1.1 – Would like a little more clarity on the requirements for this. The new language seems a bit vague. An example scenario:

We add a new asset which previously would have required it's own baseline configuration but does not change any of the existing controls for CIP-005 and CIP-007. Do we not need to document the change? How would we know existing states of our assets to know what we are doing constitutes a change? Would impacted security controls be on particular systems or for all of our assets? An example of this would be changing a port that is used in a particular ESP. Would future additions of devices using this same port on different ESP's constitute a change?

Would we be required to document changes within a timeline (30 days) like in the current R1.3?

Likes 0

Dislikes 0

Response

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

Answer

Document Name

Comment

The proposed revision improves and makes much clearer the obligations on entities when using virtualization technologies.

Suggest modify SCI infrastructure model such that compute SCI may host mixed trust VCAs consistent with the model applied for shared storage and networking resources, similar to NIST guidance. This change would support innovation and support adoption of emerging technologies.

Likes 0

Dislikes 0

Response

Joni Jones - Wabash Valley Power Association - 1

Answer

Document Name

Comment

no further team comments. Thank you

Likes 0

Dislikes 0

Response

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

Answer

Document Name

Comment

None.

Likes 0

Dislikes 0

Response