Comment Report

Project Name: 2016-02 Modifications to CIP Standards | Virtualization Updates for CIP-005 and Associated Definitions

Comment Period Start Date: 8/9/2019

Comment Period End Date: 9/26/2019

Associated Ballots:

There were 54 sets of responses, including comments from approximately 135 different people from approximately 108 companies representing 10 of the Industry Segments as shown in the table on the following pages.

Questions

1. The SDT is proposing the new Virtual Cyber Asset (VCA) and Shared Cyber Infrastructure (SCI) definitions to allow requirements to be specifically targeted at virtualized environments. The SDT is also proposing conforming changes in several other definitions to allow VCA's as an option. Do you agree with the development of new terms and the proposed definition of those terms? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification. (NOTE: Future CIP-011 requirements to be developed to address logical isolation within storage systems and will be coordinated with Project 2019-02 (BCSI)). (CIP-005 Technical Rationale pages 11-12).

2. The CIP SDT tried to maintain backwards compatibility throughout CIP-005. However, in order to take advantage of emergent technologies the existing firewall that were associated with an EAP will now fall into the SCI definition and be subject to CIP-005 Requirement R1 Part 1.6, which requires management plane separation. What level of effort would be required to accommodate these changes? Do you agree? If not, please provide comments to support your response. (CIP-005 Technical Rationale pages 11, 13, and 29-32).

3. The SDT is proposing the new term Electronic Security Zone (ESZ) to enable future technologies such as policy based environments. Do you agree with the proposed definition? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification. Note: ESP will be retained for backwards compatibility. (CIP-005 Technical Rationale pages 10, 14-18, 22-26, and 38-40).

- **Electronic Security Zone (ESZ): A segmented section of a network that contains systems and components to create logical isolation.**

4. The SDT is addressing the risk of systems of different impact, trust, or security levels ("mixed trust") environments that are possible on Shared Cyber Infrastructure by modifying the definition of Protected Cyber Asset (PCA) so that it includes those VCA's that can share a hypervisor's CPU or memory. Do you agree with the proposed modifications? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification. (CIP-005 Technical Rationale pages 8, and 14-15).

5. The SDT proposes to address infrastructure that is shared between differing BCS impact ratings that share CPU and memory resources by aligning the CIP Requirements for all systems within an ESZ or ESP and affinity to prevent sharing of CPU and memory between Virtual Cyber Assets of differing impact ratings. Do you agree with these changes? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification. (CIP-005 Technical Rationale pages 11, 12, and 14).

6. The SDT is proposing the addition of exemption 4.2.3.3 and CIP-005 requirement R1 part 1.3 for "Super-ESP" scenarios where single ESP's or ESZ's span multiple geographic locations. Do you agree with the proposed modifications? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification. (CIP-005 Technical Rationale pages 18, and 25-26).

7. The SDT is proposing to retire EACMS and develop two new terms: EACS and EAMS. These terms will allow changes within the applicable systems column of the relevant requirements to allow third party monitoring. Monitoring and logging data will be handled within CIP-011 in a future posting. Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification. NOTE: Project 2016-02 will coordinate with Project 2019-02 (BCSI) and Project 2019-03 (Supply Chain) on this topic. (CIP-005 Technical Rationale pages 9, 10, 13, and 19).

8. The V5TAG document request the SDT to "Clarify the IRA definition to address the placement of the phrase "using a routable protocol" in the definition and clarity with respect to Dial-up Connectivity." Therefore, the SDT proposes modifications to the IRA definition and CIP-005 Requirement R2. These modifications will clarify scenarios where Interactive Remote Access applies to serial only devices. Do you agree? If

you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification. (CIP-005 Technical Rationale pages 7, 19-21, 27, and 33-37).

9. The SDT is proposing modifications to CIP-005 Requirement R1. Do you agree with these changes? Please provide comments to support your response. (CIP-005 Technical Rational pages 22-32).

10. The SDT is proposing modifications to CIP-005 Requirement R2. Do you agree with these changes? Please provide comments to support your response. (CIP-005 Technical Rationale pages 33-37).

11. Backwards Compatibility: What level of effort is required to migrate from existing definitions to new definitions on existing virtualized architecture?

12. The SDT posted a draft CIP-005-7 Technical Rationale document to explain the basis behind these proposed changes. Please provide any additional comments on this document

13. Provide any additional comments for the SDT to consider, if desired

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
FirstEnergy - FirstEnergy Corporation	Aubrey Short	1,3,4		Aubrey Short, On Behalf of:	aubrey short	FirstEnergy	4	RF
					Julie Severino	FirstEnergy - FirstEnergy Corporation	1	RF
					Aaron Ghodooshim	FirstEnergy - FirstEnergy Corporation	3	RF
					Robert Loy	FirstEnergy - FirstEnergy Solutions	5	RF
					Ann Carey	FirstEnergy - FirstEnergy Solutions	6	RF
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
MRO	Dana Klem	1,2,3,4,5,6	MRO	MRO NSRF	Joseph DePoorter	Madison Gas & Electric	3,4,5,6	MRO
					Larry Heckert	Alliant Energy	4	MRO
					Michael Brytowski	Great River Energy	1,3,5,6	MRO
					Jodi Jensen	Western Area Power Administration	1,6	MRO
					Andy Crooks	SaskPower Corporation	1	MRO
					Bryan Sherrow	Kansas City Board of Public Utilities	1	MRO
					David Heins	Omaha Public Power District	1,3,5,6	MRO

					Jeremy Voll	Basin Electric Power Cooperative	1	MRO
					David Zwergel	Midcontinent ISO	2	MRO
					Douglas Webb	Kansas City Power & Light	1,3,5,6	MRO
					Fred Meyer	Algonquin Power Co.	1	MRO
					James Nail	Independence Power & Light (Indepdence Missouri)	1,3,5	MRO
					James Williams	Southwest Power Pool, Inc.	2	MRO
					Jamie Monette	Minnesota Power / ALLETE	1	MRO
					Jamison Cawley	Nebraska Public Power	1,3,5	MRO
					Sing Tay	Oklahoma Gas & Electric	1,3,5,6	MRO
					Terry Harbour	MidAmerican Energy	1,3	MRO
					Troy Brumfield	American Transmission Company	1	MRO
Public Utility District No. 1 of Chelan County	Davis Jelusich	1,3,5,6		Public Utility District No. 1 of Chelan County	Joyce Gundry	Public Utility District No. 1 of Chelan County	3	WECC
					Jeff Kimbell	Public Utility District No. 1 of Chelan County	1	WECC
					Meaghan Connell	Public Utility District No. 1 of Chelan County	5	WECC
					Davis Jelusich	Public Utility District No. 1 of Chelan County	6	WECC

PPL - Louisville Gas and Electric Co.	Devin Shines	1,3,5,6	RF,SERC	PPL NERC Registered Affiliates	Brenda Truhe	PPL Electric Utilities Corporation	1	RF
					Charles Freibert	PPL - Louisville Gas and Electric Co.	3	SERC
					JULIE HOSTRANDER	PPL - Louisville Gas and Electric Co.	5	SERC
					Linn Oelker	PPL - Louisville Gas and Electric Co.	6	SERC
Great Plains Energy - Kansas City Power and Light Co.	Douglas Webb	1,3,5,6	MRO,SPP RE	Westar-KCPL	Doug Webb	Westar	1,3,5,6	MRO
					Doug Webb	KCP&L	1,3,5,6	MRO
ACES Power Marketing	Jodirah Green	1,3,4,5,6	MRO,NA - Not Applicable,RF,SERC,Texas RE,WECC	ACES Standard Collaborations	Bob Solomon	Hoosier Energy Rural Electric Cooperative, Inc.	1	SERC
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					John Shaver	Arizona Electric Power Cooperative	1	WECC
					Bill Hutchison	Southern Illinois Power Cooperative	1	SERC
					Tara Lightner	Sunflower Electric Power Corporation	1	MRO
					Colette Caudill	East Kentucky Power Cooperative	1,3	SERC
Duke Energy	Masuncha Bussey	1,5,6	FRCC,RF,SERC	Duke Energy	Laura Lee	Duke Energy	1	SERC
					Dale Goodwine	Duke Energy	5	SERC
					Greg Cecil	Duke Energy	6	RF
Southern Company - Southern	Pamela Hunter	1,3,5,6	SERC	Southern Company	Adrianne Collins	Southern Company - Southern	1	SERC

Company Services, Inc.						Company Services, Inc.		
					Joel Dembowski	Southern Company - Alabama Power Company	3	SERC
					William D. Shultz	Southern Company Generation	5	SERC
					Ron Carlsen	Southern Company - Southern Company Generation	6	SERC
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	RSC no NGrid and Eversource	Guy V. Zito	Northeast Power Coordinating Council	10	NPCC
					Randy MacDonald	New Brunswick Power	2	NPCC
					Glen Smith	Entergy Services	4	NPCC
					Brian Robinson	Utility Services	5	NPCC
					Alan Adamson	New York State Reliability Council	7	NPCC
					David Burke	Orange & Rockland Utilities	3	NPCC
					Michele Tondalo	UI	1	NPCC
					Helen Lainis	IESO	2	NPCC
					Sean Cavote	PSEG	4	NPCC
					Kathleen Goodman	ISO-NE	2	NPCC
					David Kiguel	Independent	NA - Not Applicable	NPCC
					Silvia Mitchell	NextEra Energy - Florida Power and Light Co.	6	NPCC

Paul Malozewski	Hydro One Networks, Inc.	3	NPCC
Nick Kowalczyk	Orange and Rockland	1	NPCC
Joel Charlebois	AESI - Acumen Engineered Solutions International Inc.	5	NPCC
Mike Cooke	Ontario Power Generation, Inc.	4	NPCC
Salvatore Spagnolo	New York Power Authority	1	NPCC
Shivaz Chopra	New York Power Authority	5	NPCC
Mike Forte	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
Ashmeet Kaur	Con Ed - Consolidated Edison	5	NPCC
Caroline Dupuis	Hydro Quebec	1	NPCC
Chantal Mazza	Hydro Quebec	2	NPCC
Sean Bodkin	Dominion - Dominion Resources, Inc.	6	NPCC
Laura McLeod	NB Power Corporation	5	NPCC
Randy MacDonald	NB Power Corporation	2	NPCC

					Gregory Campoli	New York Independent System Operator	2	NPCC
Dominion - Dominion Resources, Inc.	Sean Bodkin	3,5,6		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

1. The SDT is proposing the new Virtual Cyber Asset (VCA) and Shared Cyber Infrastructure (SCI) definitions to allow requirements to be specifically targeted at virtualized environments. The SDT is also proposing conforming changes in several other definitions to allow VCA's as an option. Do you agree with the development of new terms and the proposed definition of those terms? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification. (NOTE: Future CIP-011 requirements to be developed to address logical isolation within storage systems and will be coordinated with Project 2019-02 (BCSI)). (CIP-005 Technical Rationale pages 11-12).

Teresa Cantwell - Lower Colorado River Authority - 1,5

Answer	No
Document Name	

Comment

Unsure if SCI is including the hypervisor as there is an inclusion for "management systems". PSP: Definition needs to provide a scope of what is being protected. Current definition has BCA, BCSs…IS should have clearer distinction from an EACS. An IS should be a Cyber Asset that does not provide the electronic access control of an EACS, but a Cyber Asset that is a jumpbox into an ESP/ESZ.

Likes 0	
Dislikes 0	

Response

Bruce Reimer - Manitoba Hydro - 1,3,5,6

Answer	No
Document Name	

Comment

1). We disagree with a separate VCA definition. Any requirement should be allowable to apply to virtual and physical CIP Cyber Assets for the consistency as long as it is applicable. If the Cyber Asset definitions is split into two separate ones, you may have to specify which requirements apply to virtual CIP Cyber Assets and which requirements apply to physical CIP Cyber Assets and then the applicable system will become more complicated such as Virtual BCA, Physical BCA , Virtual EACMS and Physical EACMS, etc. We suggest modifying Cyber Asset definition to include the virtual cyber asset as follows:

"A programmable electronic or virtual devices, including the hardware or virtual hardware, software, and data in those devices, where a virtual device is a logical instance of an operating system, firmware, or self-contained application hosted on a physical device. Each virtual machine and host is a distinct device."

2). We disagree with SCI definition. The following are the rational for not defining the SCI:

a) Hypervisor Host and Management Plane Device

· If the VM is a BCA, its hypervisor host and management plane (e.g., vCener) should be identified as BCA devices since they can delete and modify the VM within 15 minutes and meet the BCA definition.

· If the VM is an EACMS or PACS, its hypervisor host and management plane should be identified as EACMS or PACS devices since they can delete and modify the virtual EACMS or PACS resulting in removing or changing the electronic/physical access control functions and meet the EACMS or PACS definition. For ensuring that the hypervisor host and management plane devices are identified correctly, we suggest modifying the definition of EACMS and PACS as follows:

EACMS: “Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes the Cyber Assets that can create, modify or delete the said Cyber Assets and Intermediate Systems”

PACS: “Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers. This includes the Cyber Assets that can create, modify or delete the said Cyber Assets.”

b) Storage Device and SAN

If the storage device or SAN is used for VM running rather than backing up information, the storage device should be considered a part of the VM since the VM cannot run without it. Any requirements that apply to the VM should also apply to the storage device and SAN network.

Based on the above rationale, given that the SCI falls within the existing definition of BCA, EACMS or PACS, the SCI definition is not needed.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

ERCOT agrees with the concepts of the new definitions. However, it raises the following issues with the definitions:

SCI: Consider rewording as “storage and its associated network transport” and providing clarification on how a switch within an ESP should be classified under this new construct.

VCA: The definition does not address “data” consistent with the Cyber Asset definition.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Southern Company appreciates the opportunity to provide feedback on the SDTs current proposals. We support the SDT efforts to enable registered entities to utilize virtualization within their NERC CIP Cyber Security Programs. While we recognize that current auditing and enforcement of such practices is inconsistent across the regions, this latest approach is another positive step forward to finding secure solutions for the use of virtualization technologies that provide ultimate benefit to Entities and reliability. In support of these positive steps forward, Southern provides the following comments and suggestions in seeking additional clarity on new defined terms and applicability of new requirements.

Southern asks the SDT to consider the following changes to the Shared Cyber Infrastructure definition:

Shared Cyber Infrastructure (SCI): Programmable electronic devices, and their management systems, hosting a Virtual Cyber Asset whose compute, storage (including network transport), or network resources are shared with one or more other Virtual Cyber Assets.

Virtual Cyber Assets (VCA): A logical instance of an operating system, firmware, or self-contained application hosted on Shared Cyber Infrastructure.

This proposed definition change removes the statement “or that perform logical isolation for an ESZ or ESP” in order to delineate between the ability to maintain physical devices to perform logical isolation or alternatively, to use virtual devices to perform logical isolation. For those that choose to utilize physical devices (EACS) and their management systems (EACS) to perform logical isolation, the proposed definition changes may help keep them clearly scoped differently from virtual assets used for the same purpose. Additionally, it should be considered that any Cyber Asset or Virtual Cyber Asset that performs logical isolation for an ESZ or ESP meets the definition of being an EACS, and therefore does not have to also be included in the definition of Shared Cyber Infrastructure – the EACS itself will either be physical or virtual.

Southern asks the SDT to consider a potential conflict between the proposed R1.1 requirement where “All applicable systems shall reside within one or more defined ESPs or ESZs”, and includes EACS hosted on SCI as an applicable system; yet, the proposed R2.1 requirement states “Ensure that all Interactive Remote Access is through an Intermediate System that is not inside an applicable ESP or ESZ.” Given that Intermediate Systems (IS) are also classified as EACS, it would be impossible to require all IS-EACS to be in an ESZ (R1.1) and not (R2.1) at the same time.

Southern also seeks additional clarity on the use of the Applicable System “High Impact BES Cyber Systems and their associated: EACS hosted on SCI”. Is it the intent of the SDT that EACS (or PACS) hosted on SCI and associated with a h/m impact BCS be subject to the requirement even if there are no BCS hosted on the same SCI? Or is the intent for the requirement to only apply to EACS (or PACS) hosted on SCI and associated with a h/m impact BCS when that h/m BCS is hosted, but logically isolated, on the same SCI? As currently written, the latter does not appear to be the case, and the SDTs intention here should be made clearer through modification of the applicability of SCI, and EACS and PACS – whether hosted on SCI with a h/m BCS or not.

Likes 0	
Dislikes 0	

Response

Trevor Tidwell - PNM Resources - Public Service Company of New Mexico - 1,3

Answer	No
Document Name	

Comment

PNM Resources appreciates the effort of the SDT and getting this product out for informal comment. We support the direction the SDT would like to go. Thus our comments are intended to help give feedback to the SDT so a better product can be produced.

We agree with the VCA term and the conforming changes to other definitions to support the term.

We disagree with the definition for Shared Cyber Infrastructure (SCI). The first two of three parts are acceptable, “Programmable electronic devices whose compute, storage (including network transport), or network resources are shared with one or more Virtual Cyber Assets….”   It is the third part that is a problem, “or that perform logical isolation for an ESZ or ESP.” A device performing logical isolation is by definition an EACS, “Cyber Assets or Virtual Cyber Assets that provide electronic access control to an ESP, ESZ or BES Cyber System.” It seems redundant to redefine it here. Also, the third bullet results in infinite recursion of CIP-005 R1.1 where SCI as an applicable system shall reside within one or more defined ESPs or ESZ. If the device is providing isolation, then by definition it cannot reside fully within the boundary. You can simply remove the third part and include EACS where ever SCI is also an applicable system and the requirement is addressing a risk to the EACS. It is unclear what risk are attempted to be mitigated for an EACS that perform logical isolation for an ESZ or ESP.

With regard to SCI definition including “management systems” it is unclear what management systems are. The standards and rationale refer to the management plane. So for clarity the SDT should define what it believes management systems are with an official definition.

We agree with PACS, PAMS, EACS, and EAMS along with the retirement of EAP and EACMS.

We believe PCA may need to be revised in the third bullet regarding the sharing of compute resources. The third bullet would be better phrased as "Share computing resources (CPU or memory) with Shared Cyber Infrastructure hosting a BES Cyber Asset." Currently by proposed definition a BCA excludes SCI and a BES Cyber System is a grouping of BES Cyber Assets. Thus you would never have a PCA on BES Cyber System by definition.	
Likes 0	
Dislikes 0	
Response	
Jenifer Holmes - Alliant Energy Corporation Services, Inc. - 4 - MRO,RF	
Answer	No
Document Name	
Comment	
Alliant supports MRO NSRF's comments.	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF	
Answer	No
Document Name	
Comment	
These new terms and definitions should not only address CIP-005-7, but all CIP standards that would be impacted by virtualization. All standard updates should occur concurrently. The efforts for the entities to adopt these changes would be significant. Also, the proposed definition for PCA is too broad that could potentially bring many more assets into CIP scope.	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion	
Answer	No
Document Name	
Comment	

Dominion Energy supports EEI comments and shares the concerns regarding the ESZ definition.	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Cleco Corporation - 1,3,5,6 - SERC	
Answer	No
Document Name	
Comment	
See EEI Comments.	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	No
Document Name	
Comment	
Oncor supports EEI's comment.	
Likes 0	
Dislikes 0	
Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	
VCA – agree with proposed definition.	

SCI – request clarification on what is meant by “its management systems.”

In the SCI definition - Recommend deleting “or ESP” to confine SCI to virtualized firewalls for ESZs, allowing non-virtualized firewall hardware to be solely classified as EACS and not require dual categorization as both EACS and SCI.

Also recommend retaining the EAP definition (at least within the Glossary of Terms) as a useful and necessary term for management of ESPs, but have no objection to the removal of EAP from R1.2 to accommodate virtualization. Note: If EAP is to be removed, also need to remove the reference in VSL Table under R1 on p. 17.

IRA definition change – this revision to the definition goes beyond what is necessary for a conforming change and what was requested and authorized by the SAR (see Question 8).

The SAR recommends improving clarity within the IRA definition of the phrase “using a routable protocol” with respect to Dial-up Connectivity. This could most easily be addressed by simply changing the phrase to “using a routable or dial-up protocol.”

We agree with EEI comments that changes to the IRA definition should be limited to modifying the phrase to “using a routable or dial-up protocol.”

Likes 0	
Dislikes 0	

Response

Andy Crooks - SaskPower - 1,3,5,6,9 - MRO

Answer	No
Document Name	

Comment

VCA – agree with proposed definition.

SCI – request clarification on what is meant by “its management systems.”

In the SCI definition - Recommend deleting “or ESP” to confine SCI to virtualized firewalls for ESZs, allowing non-virtualized firewall hardware to be solely classified as EACS and not require dual categorization as both EACS and SCI.

Also recommend retaining the EAP definition (at least within the Glossary of Terms) as a useful and necessary term for management of ESPs, but have no objection to the removal of EAP from R1.2 to accommodate virtualization. Note: If EAP is to be removed, also need to remove the reference in VSL Table under R1 on p. 17.

IRA definition change – this revision to the definition goes beyond what is necessary for a conforming change and what was requested and authorized by the SAR (see Question 8).

The SAR recommends improving clarity within the IRA definition of the phrase “using a routable protocol” with respect to Dial-up Connectivity. This could most easily be addressed by simply changing the phrase to “using a routable or dial-up protocol.”

We agree with EEI comments that changes to the IRA definition should be limited to modifying the phrase to “using a routable or dial-up protocol.”

Likes 0	
Dislikes 0	

Response

Kent Feliks - AEP - 3,5

Answer	No
Document Name	

Comment

AEP is appreciative of the Standards Drafting Team's efforts to consider concerns within the industry during this informal comment period. We are thankful for the opportunity to provide feedback on the modifications currently being proposed.

While AEP holds the opinion that these proposed changes are a step in the right direction in finding beneficial solutions for the industry as a whole, we believe that some definitions and changes to the standard would benefit from some clarification. Therefore, we suggest the following for the SDT to consider:

AEP had difficulties agreeing with the Virtual Cyber Asset (VCA) and Shared Cyber Infrastructure (SCI) definitions proposed because they both rely on the proposed Electronic Security Zone (ESZ) definition. AEP found the ESZ definition to be unclear and would benefit from clarification regarding what "systems" and "components" are included in this definition.

Recommendation: AEP recommends that the SDT clarify the new proposed NERC Glossary Terms. AEP also asks SDT to ensure that those who do not plan on implementing virtualization are not affected by these proposed modifications.

Likes 0	
Dislikes 0	

Response

Davis Jelusich - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Public Utility District No. 1 of Chelan County

Answer	No
Document Name	

Comment

CHPD conditionally agrees with the VCA definition, although not in combination with the proposed SCI definition. The SCI definition currently appears to apply to any virtual system even if that system hosts no CIP-classified systems due to the use of the language "Virtual Cyber Assets **or** that perform logical isolation for an ESZ or ESP". This appears to create "chicken or egg" scenario when Cyber Assets against the SCI and VCA definitions. CHPD recommends that either the VCA definition be adjusted to scope this classification to more closely resemble the PCA definition or revise the SCI definition to only be applicable when a virtual system is hosting a classified BES Cyber Asset.

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment

VCA – agree with proposed definition.

SCI – request clarification on what is meant by “its management systems.”

In the SCI definition - Recommend deleting “or ESP” to confine SCI to virtualized firewalls for ESZs, allowing non-virtualized firewall hardware to be solely classified as EACS and not require dual categorization as both EACS and SCI.

Also recommend retaining the EAP definition (at least within the Glossary of Terms) as a useful and necessary term for management of ESPs, but have no objection to the removal of EAP from R1.2 to accommodate virtualization. Note: If EAP is to be removed, also need to remove the reference in VSL Table under R1 on p. 17.

IRA definition change – this revision to the definition goes beyond what is necessary for a conforming change and what was requested and authorized by the SAR (see Question 8).

The SAR recommends improving clarity within the IRA definition of the phrase “using a routable protocol” with respect to Dial-up Connectivity. This could be addressed by changing the phrase to “using a routable or dial-up protocol.”

We agree with EEI comments that changes to the IRA definition should be limited to modifying the phrase to “using a routable or dial-up protocol.”

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1,3,5,6

Answer	No
Document Name	

Comment

The Exelon companies agree with the comments submitted by EEI.

Likes 0	
Dislikes 0	

Response

Quintin Lee - Eversource Energy - 1,3

Answer	No

Document Name	

Comment

Eversource believes that virtualization is permitted under the current versions of the CIP standards and modification to the existing CIP standards to accommodate the concept of virtualization is not necessary.

Based on the proposed language, Eversource does not support the current definition of the Electronic Security Zone (ESZ) and, therefore, cannot not support the Virtual Cyber Asset (VCA) and Shared Cyber Infrastructure (SCI) definitions that rely on the ESZ definition. The ESZ definition provided does not clearly identify what an ESZ is or what the terms “systems” or “components” actually mean or would include. We recommend that ESZ definition be revised to clearly identify what those items are and what they would include.

Also, for entities who do not have ESZ in their environment, the current proposal has the potential to create a substantial compliance burden by requiring integration of this concept into their current processes and require these entities to demonstrate they are not utilizing a virtual environment within their networks.

For this reason, Eversource members are concerned that the proposed changes to the base construct of the CIP Standards will prove to be expensive to administer while providing little or no associated reliability and security benefit over the existing CIP language.

Recommendation: Eversource asks the SDT to consider revisiting the current approach that includes new NERC Glossary Terms along with revisions to existing terms and Requirements. We believe virtualization is already permissible within the current language in the existing CIP Standards.

Eversource recommends segregating the proposed changes to the CIP standards into smaller activities, or a more measured incremental approach, to address virtualization. The proposed modifications to CIP-007 R2 and CIP-010 R1 are places where incremental changes could be made without incorporating the ESZ and related virtualization concepts.

Likes 0	
Dislikes 0	

Response

Michael Puscas - ISO New England, Inc. - 2

Answer	No
Document Name	

Comment

While ISO-NE agrees that the current definitions associated with BES Cyber Systems do not adequately account for virtualization, ISO-NE cautions that adding new terms and definitions continues to foster an object of requirement approach instead of moving towards an information security objective based approach.

It is difficult to ascertain whether the definitions of Virtual Cyber Asset (VCA) and Shared Cyber Information (SCI) are adequate and determine the impact of the new definitions without seeing the revisions in the other standards/requirements, specifically CIP-007 and CIP-010.

To achieve the backwards compatibility, all existing terms must remain in place. In addition, introducing the concept that assets can be have multiple classifications can have profound influence on processes and tools already implemented.

The definition of SCI includes shared storage as one of the functions involved with such systems that requires appropriate protections be considered as part of developing systems and services leveraging virtualized resources. However, the requirements including SCI among Applicable Systems do not then refer to sharing of storage when sharing of CPU or memory is mentioned (CIP-005-7 R1.6, R2.6).	
Likes 0	
Dislikes 0	
Response	
Jennifer Wright - Sempra - San Diego Gas and Electric - 1,3,5	
Answer	No
Document Name	
Comment	
SDG&E supports EEI’s comments submitted on our behalf.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - MRO, Group Name Westar-KCPL	
Answer	No
Document Name	
Comment	
Westar / Kansas City Power & Light support Edison Electric Institute’s (EEI) response to Question 1.	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	

EEI supports SDT efforts that enable registered entities to utilize virtualization within their NERC CIP Cyber Security Networks. While we recognize that a limited number of registered entities have already deployed some form of virtualization within their networks in ways that have been deemed acceptable by their Regional Entities, current auditing and enforcement of such practices is inconsistent across the regions. For this reason, EEI appreciates SDT efforts to listen and respond to industry concerns shared during the previous informal commenting opportunity. EEI's members understand the complex issues the SDT is seeking to address and we appreciate the opportunity to provide feedback on its current proposals.

EEI is of the opinion that the changes provided in this latest proposed approach to virtualization is another good step forward in finding solutions that benefit the Industry broadly. However, additional clarity is still needed. Within this context we offer the following suggestions for SDT consideration:

The currently proposed definition for Electronic Security Zone (ESZ) is not clear. The ESZ definition should address what the terms "systems" or "components" mean or would include. It is difficult to support the Virtual Cyber Asset (VCA) and Shared Cyber Infrastructure (SCI) definitions currently since they rely on the ESZ definition. In contrast, the non-virtualized and currently approved term Electronic Security Perimeter (ESP) provides clear language that limits an ESP to "networks to which BES Cyber Systems are connected" providing well-defined direction to entities. For this reason, we ask the SDT to revise the proposed definition of ESZ consistent with the approved definition of ESP.

In addition to the concerns identified above, we would like to offer some additional suggestions for SDT consideration:

1. Electronic Access Point (EAP) – EEI recommends that the SDT not propose the retirement of EAP given "ESP's and EAPs remain a valid option and are one method of implementing logical isolation." (see Technical Rationale, Section: Logical Isolation; page 14)

2. Interactive Remote Access (IRA) – EEI recommends that the SDT retain much of the existing text contained within the approved definition for IRA. While we recognize that the SAR directs the SDT to improve the clarity of ESPs, ERCs and IRAs, we are of the opinion that the proposed IRA language may create even more ambiguity. For this reason, we suggest limiting future revisions to the definition of IRA to the following:

User-initiated access by a person employing a remote access client or other remote access technology using a routable **or dial-up** protocol. Remote access originates from a Cyber Asset that is not an Intermediate System and ……

Whether the SDT modifies the existing definition of IRA or develops a revised version of what is currently proposed, efforts should be made by the SDT to ensure that the scope of IRA is clear and doesn't bring in cyber assets not currently covered under this definition.

Recommendation: EEI asks the SDT to clarify the new NERC Glossary Terms along with revisions to existing terms and Requirements and ensure that entities not currently planning to implement virtualization are not impacted by the proposed changes. While virtualization has been permitted within the current language of the CIP Reliability Standards, EEI understands that such practices are not consistently applied by all regions at this time. For this reason, we support the SDT's efforts to develop solutions that make it easier for entities to more fully deploy virtualization as they deem appropriate to achieve internal efficiencies. Additionally, we appreciate efforts by the SDT to ensure that those not seeking to deploy virtualization will not have their existing policies, processes, and procedures upended as a result.

Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 1,3,6	
Answer	No
Document Name	
Comment	

The term VCA by the definition provided includes current EACM (EAC and EAM) and PACS (PAC and PAM) devices without making a differentiation between them and BCAs and PCAs that are also Virtual. In our opinion, this lack of differentiation of the terms will create ambiguity in the drafting of CIP standards. The currently proposed change to CIP-005 R1.1 would require any virtual PAC or EAC to be included in an ESP or ESZ while Physical PACs and EACs could be located outside that ESP or ESZ.

Additionally the proposed term SCI includes both virtual hypervisor systems as well as traditional firewalls and systems. Technologically speaking those systems are vastly different and will apply to standards in different ways. For example, the proposed change to CIP-005 R2.1 requires that Interactive remote access be limited to an intermediary system for SCI which would be possible for a Hypervisor inside of an ESP but a firewall that creates the boundary of the ESP can't easily have its external interfaces limited down to just the Intermediate system due to its placement in the network.

We propose that SDT modify the definition of "Cyber Asset" to include "Virtual Cyber Assets" instead of establishing another term with essentially no difference of criticality, protection, or evidence within the standard.

Likes 0	
Dislikes 0	

Response

Greg Davis - Georgia Transmission Corporation - 1

Answer	No
Document Name	

Comment

Can the drafting team explain if the intent or expectation of the proposed BES CA definition relative to CIP-002 categorization? Does the team expect 1.) No change? 2.) Decrease in scope by removal of existing BESCA hardware hosting in-scope VCA? Or 3.) Increase in scope by the addition of excluded Cyber Assets that contain “in-scope VCAs”?

The inclusion of both Cyber Asset and Virtual Cyber Asset in the revised definition of BES Cyber Asset could lead to an expansion of Cyber Assets and BES Cyber Assets that are in scope. This could have unintended consequences to the fleet of CIP Standards and could unintentionally cause ambiguity and complexity in tracking procurements of BES Cyber Assets applicable to CIP-013-1 by including “excluded programmable devices” containing “in scope Virtual Cyber Assets”.

Additionally, due to the ambiguity described above, GTC encourages the team to develop a reference document modeled after NERC’s “Bulk Electric System Definition Reference Document” to include various examples containing diagrams of Virtual Cyber Assets and Shared Cyber Infrastructure at each CIP-002 asset location (control center, transmission station and substation, generation resources, etc.) to assist the industry with the application and to provide clarification of the new and revised definition(s) in a consistent, continent-wide basis for the majority of BES Cyber Assets under the proposed definition.

Likes 0	
Dislikes 0	

Response

Roger Fradenburgh - Network and Security Technologies - 1 - NA - Not Applicable

Answer	No

Document Name	

Comment

N&ST disagrees with the proposal to break out monitoring functions from the existing EACMS and PACS definitions in order to serve the goal of easily accommodating third-party, possibly cloud-based, electronic and/or physical access monitoring. We strongly disagree with the rationale that “access monitoring” is somehow less critical, and poses less inherent risk, than “access control,” particularly in light of the fact the 2016 SANS / E-ISAC analysis of the attack on Ukrainian power grid cited a lack of monitoring as a key factor in the attack’s success.

N&ST believes the proposed definition of “ESZ” is inadequate and lacks any intrinsic meaning. We suggest that it be modified by adding words that convey it is a logical boundary, established in a virtual environment, that contains one or more virtual cyber assets and provides logical isolation.

N&ST believes the proposed definition of “SCI” should be modified to reflect the fact that it includes hardware, as per the Technical Rationale document.

N&ST believes the proposed modification of “IRA” has been watered down to the point where it basically defines “Interactive Remote Access” as remote access that’s interactive. While we concur with removing as much “requirements-like” language from Glossary definitions, we believe the revised definition should retain the information that “IRA” is access to a BES Cyber System or associated applicable system and that it is initiated from outside the ESP or ESZ where the system being accessed is located.

Likes 0	
Dislikes 0	

Response

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5

Answer	No
Document Name	

Comment

VCA – agree with proposed definition.

SCI – request clarification on what is meant by “its management systems.”

In the SCI definition - Recommend deleting “or ESP” to confine SCI to virtualized firewalls for ESZs, allowing non-virtualized firewall hardware to be solely classified as EACS and not require dual categorization as both EACS and SCI.

Also recommend retaining the EAP definition (at least within the Glossary of Terms) as a useful and necessary term for management of ESPs, but have no objection to the removal of EAP from R1.2 to accommodate virtualization. Note: If EAP is to be removed, also need to remove the reference in VSL Table under R1 on p. 17.

IRA definition change – this revision to the definition goes beyond what is necessary for a conforming change and what was requested and authorized by the SAR (see Question 8).

The SAR recommends improving clarity within the IRA definition of the phrase “using a routable protocol” with respect to Dial-up Connectivity. This could be addressed by changing the phrase to “using a routable or dial-up protocol.”

We agree with EEI comments that changes to the IRA definition should be limited to modifying the phrase to “using a routable or dial-up protocol.”

Likes 0	

Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Andrea Barclay - Georgia System Operations Corporation - 3,4

Answer	Yes
Document Name	

Comment

In general, GSOC/OPC supports the development of new terms and definitions to ensure appropriate clarity regarding the use of virtualization within environments to which CIP is applicable. GSOC/OPC does, however, have concerns regarding clarity around the potential for non-CIP virtual instances being pulled into "scope" by virtue of the expansive nature of the definition of Cyber Asset. In particular, GSOC/OPC is concerned that the inclusion of both Cyber Asset and Virtual Cyber Asset (VCA) in the revised definition of BES Cyber Asset (BCA) could create redundancy and lead to an expansion of the Cyber Assets and BCAs that are in scope. Specifically, the term Cyber Asset has traditionally encompassed hardware and all instances of software thereon. While VCA is applicable only to the logical instances of a Cyber Asset on Shared Cyber Infrastructure (SCI), the inclusion of the term Cyber Asset without additional clarification could be interpreted to pull in the physical infrastructure associated with a VCA and, as a result, all other logical instances running within the virtualized environment. For this reason, GSOC/OPC recommends that the SDT consider adding clarification to the definition of a BCA to ensure that instances of non-CIP virtualized cyber assets that are logically isolated from BCAs or any other applicable system and being maintained on the same hardware as a VCA (without any other interaction) are not pulled into scope of the CIP Reliability Standards.

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

Note: Virtual Cyber Assets that are logically isolated from and not classified as a BES Cyber Asset are excluded.

Alternatively, if the recommendation for clarification to the definition is not accepted, GSOC/OPC would recommend that the SDT develop compliance and/or implementation guidance concurrently with its standards drafting activities that addresses the need for this clarification. Such effort to develop concurrent compliance and/or implementation guidance was conducted by the SDT to ensure clarity during the development of the BES Definition and was enormously well received by and helpful to the industry during compliance implementation. GSOC/OPC would suggest that any compliance and/or implementation guidance provide diagrams similar to those provided on pages 39 - 40 (Pinecone Energy).

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	
Please add language to help describe tools such as AV, etc.	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	Yes
Document Name	
Comment	
Reclamation agrees with the rationale behind adding Virtual Cyber Asset (VCA) and Shared Cyber Infrastructure (SCI) to allow requirements to be specifically targeted at virtualized environments. Reclamation recommends the SDT create a new term for Physical Cyber Assets, and have Cyber Assets be the generic term for both physical and virtual.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
SWG agrees with the concepts of the new definitions. However, there are issues with the definitions.	

SCI: Consider rewording as “storage and its associated network transport.” Provide clarification on how a switch within an ESP or should be classified under this new construct. VCA: The definition does not address “data” consistent with the Cyber Asset definition.	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1,3,5	
Answer	Yes
Document Name	
Comment	
Can the SCI section in the Technical Rationale document have a graphic and description added to address Logical Unit Number (LUN) isolation with respect to Logical Isolation Zones? The document is currently silent on LUN Isolation with respect to satisfying requirements. Additionally, there should be consideration for creating a new term Physical Cyber Assets to support the use of the term or Cyber Assets should be modified to Physical Cyber Assets. Recommend the SDT make considerations for all CIP standards impacted by virtualization be updated concurrently to ensure efforts to make the necessary modifications to existing architecture by the entity.	
Likes 0	
Dislikes 0	
Response	
Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC	

Answer	Yes
Document Name	

Comment

Seattle City Light appreciates the long and hard efforts of the Standards Drafting Team (SDT) in conceiving a way forward for virtualization within the context of the CIP Standards, and for creating extensive supporting materials to explain the proposed concepts and changes. City Light agrees that CIP Standard changes are necessary to support virtualization, and that some new definitions will be required.

However, City Light is concerned about both the expanding number of new definitions and their unique NERC-only nature. Specifically, is the operational function or risk presented by PAMS and EAMS sufficient that they require unique definitions and requirements, or would it reduce risk enough if the data/information contained within them be protected as BCSI (and the terms PAMS and EAMS be dropped entirely)? Could they be considered as another kind of PCA or VCA?

Regarding the proposed change to the PSP definition—"the physical border at which access is controlled"—City Light requests that the SDT clarify what it is the border ***of****. Presumably of something around subject BCS, BCA, VCA hosts, SCI hosts, EACS hosts, etc., but the definition as proposed is in no way clear and promises all kinds of possible audit shenanigans.*

Likes 0	
Dislikes 0	

Response

James Brown - California ISO - 2 - WECC

Answer	Yes
Document Name	

Comment

CAISO agrees with the concepts of the new definitions. However, there are issues with the definitions.

SCI: Consider rewording as "storage and its associated network transport." Provide clarification on how a switch within an ESP should be classified under this new construct.

VCA: The definition does not address "data" consistent with the Cyber Asset definition.

Likes 0	
Dislikes 0	

Response

Masuncha Bussey - Duke Energy - 1,5,6 - SERC, Group Name Duke Energy

Answer	Yes
Document Name	

Comment

Duke Energy generally supports the need for the definition of Virtual Cyber Assets and Shared Cyber Infrastructure in the CIP environments.This definition doesn't address the issue of mixed trust environment. It doesn't allow for the existence of non-BES and BES cyber assets (or Virtual Cyber Assets) to exit within the same SCI. SCI is subject to same level of requirement as BCA, and doesn't help entities employing mixed trust environment.	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2 - MRO,SERC,RF	
Answer	Yes
Document Name	
Comment	
MISO agrees with the concepts of the new definitions; however, recommends the following issues be addressed. SCI: Consider rewording as “storage and its associated network transport.” Provide clarification on how a switch within an ESP should be classified under this new construct. VCA: The definition does not address “data” consistent with the Cyber Asset definition.	
Likes 0	
Dislikes 0	
Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5	
Answer	Yes
Document Name	
Comment	
Tri-State recommends the term SCI be changed to “Virtual Infrastructure” and then within the definition add a clarifying statement regarding cloud. Something like: “This infrastructure resides on the Responsible Entity’s premises; not in a 3rd party’s infrastructure.” Additionally, we think the use of “shared” within the definition is problematic, as it carries different meanings and could be interpreted in multiple ways. So, we recommend the team modify this to reflect what we think was intended, which is a mixed or hybrid infrastructure that includes both virtual and physical assets. Everything else about the definition we think is ok, as it relates to the proposed CIP-005. We will need to see how it is applied in the other CIP standards, especially CIP-007 and CIP-010, before we are completely comfortable with the new definition. Tri-State does not agree with the new IRA definitions; see question 8 for additional comments.	
Likes 0	
Dislikes 0	

Response	
Michael Johnson - Pacific Gas and Electric Company - 1,3,5 - WECC	
Answer	Yes
Document Name	
Comment	
PG&E indicates the following: 1 - Agrees with the proposed new definitions. 2 – Understands the addition of these definitions will allow Entities to use the more advanced features of the technology, while at the same time establishing the conditions within the Requirements to protect the virtualized environments from some their unique vulnerabilities due to the elimination of mixed-trust environments. 3 – Understands the use of these definitions will require modifications to the internal CIP-002 process to document that a BES Cyber System (BCS) can be comprised of more than the current BES Cyber Asset (BCA).	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Langston - Tallahassee Electric (City of Tallahassee, FL) - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
faranak sarbaz - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no NGrid and Eversource	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Chinedu Ochonogor - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Neil Swearingen - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Boody - Lakeland Electric - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aubrey Short - FirstEnergy - FirstEnergy Corporation - 1,3,4, Group Name Aubrey Short, On Behalf of:	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE disagrees with the explicit exclusion of Shared Cyber Infrastructure (SCI) from the proposed definition of BES Cyber Asset. In the provided rationale document the SDT states that it recognizes that SCI has the same impact as a virtual BCA, or more so if the SCI is hosting multiple virtual BCAs. It appears the SDT acknowledged this by expressing its intention to include SCI in all requirements that currently affect BCA and to include SCI in additional requirements. It also seems it is not consistent with how other categorizations are being applied. The SDT did not include exclusions for	

SCI in the definitions of EACS, EAMS, PACS, or PAMS. Additionally, the solution outlined by the SDT requires that all future drafting teams include SCI in the applicable system column for, at a minimum, those requirements applicable to BES Cyber Systems.

Other situations also arise. Will SCI that hosts EACS that are associated with Medium/High Impact BES Cyber Systems be included in Applicable Systems? Will Applicable Systems in include SCI hosting PACS that are associated with Medium/High Impact BES Cyber Systems? For example, CIP-007-6 R2 requires that registered entities maintain a security patch management process for applicable systems. Will this requirement be re-scoped to apply to SCI hosting EACS, SCI hosting PACS, etc.? If yes, then this has the potential to make the applicable systems column of certain requirements unnecessarily verbose when including all combinations of BCS, EACS, EAMS, PACS, PCAs, and the SCI hosting all of these. If no, then this has the potential for a compliance gap for SCI that are not hosting BCS but are hosting EACS or PACS. For example, if CIP-007-6 R2 is not written to apply to “SCI hosting EACS associated with High or Medium Impact BES Cyber Systems” then the SCI may receive less protection then the VCAs it hosts.

Alternatively, if the expectation is that SCI hosting PACS are categorized as PACS and SCI hosting EACS are categorized as EACS then the categorization of SCI hosting BCS will not follow the same logic.

Instead, Texas RE recommends that applying multiple categorizations to Cyber Assets that perform multiple functions is the easiest solution to this issue. Currently if an entity has an EACMS and places it inside an ESP, it is expected to comply with EACMS and PCA requirements. SCI should be treated in the same manner. If a Cyber Asset is performing the function of an SCI then it should be categorized as an SCI and inherit all of the categorizations of the VCAs it hosts.

Likes 0	
Dislikes 0	
Response	

2. The CIP SDT tried to maintain backwards compatibility throughout CIP-005. However, in order to take advantage of emergent technologies the existing firewall that were associated with an EAP will now fall into the SCI definition and be subject to CIP-005 Requirement R1 Part 1.6, which requires management plane separation. What level of effort would be required to accommodate these changes? Do you agree? If not, please provide comments to support your response. (CIP-005 Technical Rationale pages 11, 13, and 29-32).

Jenifer Holmes - Alliant Energy Corporation Services, Inc. - 4 - MRO,RF

Answer	No
Document Name	

Comment

Alliant supports MRO NSRF's comments.

Likes 0	
Dislikes 0	

Response

Trevor Tidwell - PNM Resources - Public Service Company of New Mexico - 1,3

Answer	No
Document Name	

Comment

We disagree with the premise of the question. Per CIP-005 R1.6 it applies to only SCI hosting HIBCS and MIBCS. If the EAP is on SCI that does not host HIBCS or MIBCS then management plane separation is not required. If that we the intent, then the proposed requirement failed to achieve the objective. Also, per our response in comment #3 the SCI definition needs to have the third bullet struck due to the infinite recursion of CIP-005 R1.1.

The purpose of the proposed CIP-005 is “To protect BES Cyber Systems against compromise by allowing only known and controlled communication to and from the system and logically isolating all other communication.” Controlling access to the management plane of a device that isn’t a BES Cyber System appears to be outside the purpose of the standard, thus EACS performing logical isolation should not have their management plane in scope.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Please see the comments to Question 1. Southern does not agree that all EACS should be dual classified as SCI as well; some should, some should not. The level of effort required to accommodate these changes could be significant, but could be lessened by consideration of proposed changes provided in our responses to previous questions.	
Likes 0	
Dislikes 0	
Response	
Bruce Reimer - Manitoba Hydro - 1,3,5,6	
Answer	No
Document Name	
Comment	
Based on our comments in the question 1, SCI is not needed since it would fall within the definition of BCS, EACMS or PACS. Therefore CIP-005 R1 Part 1.6 applicable system should be changed to high and medium BCS and associated EACMS and PACS.	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5	
Answer	No
Document Name	
Comment	
This is not only an addition to CIP-005, but also CIP-007 and CIP-010.	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	

There is no need to sacrifice backwards compatibility by incorporating the existing firewalls (EAPs) associated with ESPs into the SCI definition.

A “next gen” firewall with virtualized firewalls can be designated SCI per the definition (although the device could also meet the definition of EACS, complicating categorization and compliance tracking). If “or ESP” is deleted from the SCI definition, then hardware firewalls associated with ESPs can be EACS and not be subject to SCI applicability, maintaining backwards compatibility.

If a firewall is not virtualized, there is nothing to do per R1.6; it doesn’t apply, so also delete “or ESP” from the Requirements of R1.6.

Likes 0

Dislikes 0

Response

David Jendras - Ameren - Ameren Services - 1,3,6

Answer	No
Document Name	

Comment

We believe the combination of Virtual infrastructure and traditional firewalls and switches into a single definition will be confusing in the drafting of CIP standards. Both systems provide drastically different functions and will be located in two distinct parts of the network. Due to the placement of a firewall system at the edge of an ESP/ESZ a great deal of extra effort would need to happen to create a new interface and ESP for a new management plane.

Likes 0

Dislikes 0

Response

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

Answer	No
Document Name	

Comment

See EEI's response to Question 1

Likes 0

Dislikes 0

Response

Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - MRO, Group Name Westar-KCPL

Answer	No
Document Name	
Comment	
Westar / Kansas City Power & Light support Edison Electric Institute’s (EEI) response to Question 2.	
Likes 0	
Dislikes 0	
Response	
Jennifer Wright - Sempra - San Diego Gas and Electric - 1,3,5	
Answer	No
Document Name	
Comment	
SDG&E supports EEI’s comments submitted on our behalf.	
Likes 0	
Dislikes 0	
Response	
Michael Puscas - ISO New England, Inc. - 2	
Answer	No
Document Name	
Comment	
As already mentioned above, to achieve the backwards compatibility, all existing terms must remain in place. In addition, introducing the concept that assets can be have multiple classifications can have profound influence on processes and tools already implemented.	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1,3	
Answer	No
Document Name	

Comment	
See Eversource response to Question 1	
Likes 0	
Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	No
Document Name	
Comment	
PPL NERC Registered Affiliates appreciate the SDT's effort to make the updated requirements backwards compatible. We agree that in a mixed-mode virtual environment, isolation between the management plane and data plane is imperative (with mixed-mode meaning, for example, high/medium BES Cyber Systems, BES Cyber Systems/EACS, or CIP/non-CIP). However, if an entity sets up separate virtual environments (i.e. a high impact BES Cyber System virtual environment and a separate associated High Impact EACS environment), we believe that isolation between the management plane and the data plane will require a significant amount of additional work (i.e. design changes on every existing firewall) resulting in elevated compliance risk and zero benefit. The SDT should continue to consider that not all virtual environments that involve CIP will be mixed-mode.	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1,3,5,6	
Answer	No
Document Name	
Comment	
The Exelon companies agree with the comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Chinedu Ochonogor - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	No

Document Name	
Comment	
AZPS warns against retiring the EAP definition. If the ESP definition will be maintained the EAP definition should follow. This modification would force changes throughout the categorization process AZPS has in place and does not allow for the specific requirements to be applied to a virtual vs. physical firewall. Further, requirement part 1.6 does not include instruction on how to address a physical EAP with a nonexistent separate management plane.	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
There is no need to sacrifice backwards compatibility by incorporating the existing firewalls (EAPs) associated with ESPs into the SCI definition. A “next gen” firewall with virtualized firewalls can be designated SCI per the definition (although the device could also meet the definition of EACS, complicating categorization and compliance tracking). If “or ESP” is deleted from the SCI definition, then hardware firewalls associated with ESPs can be EACS and not be subject to SCI applicability, maintaining backwards compatibility. If a firewall is not virtualized, there is nothing to do per R1.6; it doesn’t apply, so also delete “or ESP” from the Requirements of R1.6.	
Likes 0	
Dislikes 0	
Response	
Davis Jelusich - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Public Utility District No. 1 of Chelan County	
Answer	No
Document Name	
Comment	
CHPD cannot ascertain how to achieve compliance with the proposed language. CHPD requests a definition for “Management System” and “Management Plane”. CHPD also requests clarification on the inclusion of CPU and memory and how those terms are applied to this requirement. Please include a real-world example of successful compliance with this language.	
Likes 0	
Dislikes 0	
Response	

Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	No
Document Name	
Comment	
The Technical Rationale explains that the purpose of this requirement is to require isolation between the data and management planes, therefore the requirement should directly state that to be clear on its intent. Also, the word “may” should be replaced with “can” to be more definite and provide better clarity. CenterPoint Energy Houston Electric, LLC (CenterPoint Energy) recommends the following language: “Management systems must be logically isolated from the data plane and can only share CPU, memory or ESZ or ESP with other management systems and the management plane.”	
Likes 0	
Dislikes 0	
Response	
Kent Feliks - AEP - 3,5	
Answer	No
Document Name	
Comment	
Please see AEP’s response to Question #1	
Likes 0	
Dislikes 0	
Response	
Andy Crooks - SaskPower - 1,3,5,6,9 - MRO	
Answer	No
Document Name	
Comment	
There is no need to sacrifice backwards compatibility by incorporating firewalls associated with ESPs into the SCI definition. A “next gen” firewall with virtualized firewalls can be designated SCI per the definition (although the device could also meet the definition of EACS, complicating categorization and compliance tracking). If “or ESP” is deleted from the SCI definition, then hardware firewalls associated with ESPs can be EACS and not be subject to SCI applicability, maintaining backwards compatibility. If a firewall is not virtualized, there is nothing to do per R1.6; it doesn’t apply, so also delete “or ESP” from the Requirements of R1.6.	

Likes 0	
Dislikes 0	
Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	
There is no need to sacrifice backwards compatibility by incorporating firewalls associated with ESPs into the SCI definition. A “next gen” firewall with virtualized firewalls can be designated SCI per the definition (although the device could also meet the definition of EACS, complicating categorization and compliance tracking). If “or ESP” is deleted from the SCI definition, then hardware firewalls associated with ESPs can be EACS and not be subject to SCI applicability, maintaining backwards compatibility. If a firewall is not virtualized, there is nothing to do per R1.6; it doesn’t apply, so also delete “or ESP” from the Requirements of R1.6.	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	No
Document Name	
Comment	
Oncor supports EEI's comment.	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Cleco Corporation - 1,3,5,6 - SERC	
Answer	No
Document Name	
Comment	

See EEI Comments.	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion	
Answer	No
Document Name	
Comment	
Dominion Energy supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
ERCOT agrees with the concept. The level of effort for implementation will be dependent on how entities have already architected systems.	
Likes 0	

Dislikes 0	

Response

Michael Johnson - Pacific Gas and Electric Company - 1,3,5 - WECC

Answer	Yes
Document Name	

Comment

For the two (2) part question, PG&E indicates:

1 – The effort to accommodate the indicated changes will be minimal. PG&E currently approaches the separation of the management plane in a manner that is similar to what is shown in the proposed Requirement part 1.6.

2 – PG&E agrees with the proposed modification on the separation of the management plane from other Cyber Asset types (i.e. BCS), but has a concern that the phrase “may only share CPU, memory, or ESZ or ESP with other management systems and the management plane” indicates the same condition being presented in Questions 4 and 5, which may not be clear to many.   Questions 4 and 5 indicate PCA (virtual type) or BCS of different impact ratings must take on the impact rating of the highest impact-rated Cyber Asset in the same ESZ, ESP, or sharing the same CPU and memory (i.e. no mixed-trust). PG&E believes this condition extends to SCI, but that is not made clear by the mixed-trust section of the currently-drafted Technical Rationale document.

Recommendation - If PG&E’s understanding is correct and SCI of different impact ratings cannot share the same CPU and memory (i.e. no mixed-trust), PG&E recommends the Technical Rationale section on mixed-trust be modified to clearly indicate SCI of different impact ratings cannot share the same CPU and memory.

Likes 0	
Dislikes 0	

Response

Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5

Answer	Yes
Document Name	CIP 005_Q2 Diagram.pdf

Comment

Based on the current draft, it appears we would have to purchase multiple pieces of physical hardware to create a management plane separate from the SCI. The level of effort depends on how the auditors approach/define management systems, management plane and data plane. We feel the SDT should define management systems, management plane, data plane, and give examples for all three terms. Here are some suggested definitions for each:

In this scenario the Hypervisor is classified as a BCA based on the high water mark. Let’s assume to access the hypervisor an administrator authenticates to the hypervisor through a web interface hosted on the hypervisor. The web connection is initiated from a workstation (BCA) from inside the ESP. All traffic between VLANs run through a switch to the firewall, for logical isolation. In this example, the hypervisor will share the same CPU and memory as the data plane, therefore would not be compliant with CIP-005 R1.6. So would the hypervisor or workstation be considered a management system in this situation? The standards should allow for this type of configuration when there is no typical “management system” used to administer multiple VM infrastructures.

- Management system – a device used to remotely manage a VM infrastructure. This is a separate device that does not share CPU or memory with the VM infrastructure. This does not include the local hypervisor embedded management interface.
- Management plane – a collection of management systems used to remotely manage VM infrastructures. This is a separate collection of devices that do not share CPU or memory with the VM infrastructure. This does not include the local hypervisor embedded management interface.
- Data plane – shared storage system used by more than one SCI (does not include the hypervisor local storage)

We agree with this approach if the entity is using a separate, central “management system” to administer multiple virtual infrastructures (virtual farm). However, based on the wording of CIP-005 R1.6, it does not allow for a single virtual infrastructure inside the ESP to be managed locally by directly logging into the hypervisor. An entity would need additional physical equipment in order to manage the hypervisor and be compliant with CIP-005 R1.6. Any hypervisor would essentially share resources such as CPU, Memory and Disk with its locally managed VMs.

We have a scenario we would like to see addressed in the standard changes; see uploaded diagram in addition to the following comments:

In this scenario the Hypervisor is classified as a BCA based on the high water mark. Let’s assume to access the hypervisor an administrator authenticates to the hypervisor through a web interface hosted on the hypervisor. The web connection is initiated from a workstation (BCA) from inside the ESP. All traffic between VLANs run through a switch to the firewall, for logical isolation. In this example, the hypervisor will share the same CPU and memory as the data plane, therefore would not be compliant with CIP-005 R1.6. So would the hypervisor or workstation be considered a management system in this situation? The standards should allow for this type of configuration when there is no typical “management system” used to administer multiple VM infrastructures.

Likes 0	
Dislikes 0	

Response

Bobbi Welch - Midcontinent ISO, Inc. - 2 - MRO,SERC,RF

Answer	Yes
Document Name	

Comment

MISO agrees with the concept. The level of effort for implementation will be dependent on how entities have already architected systems. Worth noting, this particular subpart is somewhat prescriptive and will be wholly new. Many entities may have difficulty complying if the timeline for compliance is short; i.e. less than 3 years. MISO is recommending a 3-year timeline for implementation as, depending upon when the standard is approved, an entity will need to identify the additional equipment needed, plan for the anticipated expense duing its next budget cycle, order the equipment once the budget is approved and test and install the equipment upon delivery.

Likes 0	
Dislikes 0	

Response

Patricia Boody - Lakeland Electric - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Changes to eliminate to defined term EAP will require a moderate level of effort for a small entity with limited number of EAP devices. For a larger entity, the level of effort could be significant. It will require changes to policies, procedures, network diagrams, and possibly other evidence artifacts to incorporate the new defined terms and remove the old ones.	
Likes 0	
Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,5,6 - SERC, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy supports the direction of backwards compatibility and is currently assessing the impact of the SCI definition requiring management plane separation	
Likes 0	
Dislikes 0	
Response	
James Brown - California ISO - 2 - WECC	
Answer	Yes
Document Name	
Comment	
CAISO agrees with the concept. The level of effort for implementation will be dependent on how entities have already architected systems. Worth noting, this particular subpart is somewhat prescriptive and will be wholly new. Many entities may have difficulty complying if the timeline for compliance is short.	
Likes 0	
Dislikes 0	
Response	

Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC

Answer	Yes
Document Name	

Comment

City Light judges that the level of effort required to configure and maintain the required Shared Cyber Infrastructure (SCI) management plane separation is not burdensome given the operational benefits provided by the SCI concept.

City Light also asks that the SDT clarify if an accessing device for a Management Plane (out of band network) can be virtual, or must it be completely separate from the VCA or SCI?

Likes 0	
Dislikes 0	

Response

Gladys DeLaO - CPS Energy - 1,3,5

Answer	Yes
Document Name	

Comment

Answer assumes that software defined firewalls are in scope of the question. The level of effort is considered low for new implementation. For existing implementations, the level effort can be high depending on the existing architecture. Will Entities be provided a phased in consideration for existing architecture and the implantation guidelines be reflective of the phased in approach?

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

While not a significant level of effort will be required to technically accommodate R1 Part 1.6, this will require a change in culture which introduces compliance risk. This will require Entities to train EAP administrators on the new requirement and modify CIP-010 Change Management process(es) for EAP/LIZ/ESZ. For Entities not moving forward with emergent technologies, this will force programmatic changes to maintain backwards compatibility.

Further, we have spoken with various major Distributed Control System, SCADA, and Industrial Control System vendors and none of them have customers asking for policy based controls and thus do not have plans in the next 24 months to develop and or integrate them into their products.	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
For BPA, the effort will consist of drawing and documentation updates.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
SWG agrees with the concept. The level of effort for implementation will be dependent on how entities have already architected systems. Worth noting, this particular subpart is somewhat prescriptive and will be wholly new. Many entities may have difficulty complying if the timeline for compliance is short.	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	Yes
Document Name	
Comment	

Reclamation sees minimal impact to current and future operations. Reclamation follows FISMA and NIST guidelines in addition to NERC Standards.	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 3,4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Network and Security Technologies - 1 - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Aubrey Short - FirstEnergy - FirstEnergy Corporation - 1,3,4, Group Name Aubrey Short, On Behalf of:	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Neil Swearingen - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
faranak sarbaz - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Langston - Tallahassee Electric (City of Tallahassee, FL) - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE agrees that management plane separation should be required. However, Texas RE seeks clarification in Part 1.6 which states, “Management systems may only share CPU, memory, or ESZ or ESP with other management systems and the management plane.” Does this mean an entity can have SCI that contains corporate **and** CIP management systems/plane, which can share CPU, memory, or ESZ or ESP; thus creating a potential mixed trust virtual environment? This appears to be supported by the CIP-005 Technical Rationale on pages 14-15. Although, mixed trust risks are identified and two option examples are given mixed trust is allowed which is concerning when one could have SCI that includes BCAs: EMS, SCADA, etc. Additionally, based on the proposed BCA definition; SCI is excluded from the BCA definition.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no NGrid and Eversource	

Answer	
Document Name	
Comment	
Recommend changing the proprietary term “hypervisor” with a generic term like “VM host” Request clarification of the diagrams on pages 30-32. Legends explaining the color coding and dotted lines will help. We are not sure about the unmarked boundaries. At least one diagram includes a physical box yet this topic is virtualization . . . thereby confusing what is physical vs what is virtualization Some of us have Part 1.7 on page 32 while others have Part 1.6. Yet both versions are August 2019. Suggest posting once or if updating please broadcast an announcement of new versions. GENERAL COMMENT - this technology is complex which will require a lot of training beyond today’s training. Expecting to re-write documentation too.	
Likes 0	
Dislikes 0	
Response	

3. The SDT is proposing the new term Electronic Security Zone (ESZ) to enable future technologies such as policy based environments. Do you agree with the proposed definition? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification. Note: ESP will be retained for backwards compatibility. (CIP-005 Technical Rationale pages 10, 14-18, 22-26, and 38-40).

- **Electronic Security Zone (ESZ): A segmented section of a network that contains systems and components to create logical isolation.**

Andrea Barclay - Georgia System Operations Corporation - 3,4

Answer	No
Document Name	

Comment

GSOC/OPC respectfully suggests that the definition be revised for greater consistency with the definition of an Electronic Security Perimeter (ESP) as follows:

ESZ: A logically isolated section of a network that contains BES Cyber Asset(s), Electronic Access Control System(s), Electronic Access Monitoring System(s), Physical Access Control System(s), Physical Access Monitoring System(s), Protected Cyber Asset(s) or their management components.

Further, even in this revised definition, it is unclear how this definition would apply for policy based environments when the policy is applied to workloads and not network segments. It appears that while the issue of whether the policy has to apply at layer 3 in the OSI model is addressed, the effect is that it is still only permissible for the policy to apply to the network - instead of other elements of the system that may effectively control access.

Likes 0	
Dislikes 0	

Response

Teresa Cantwell - Lower Colorado River Authority - 1,5

Answer	No
Document Name	

Comment

Current definition could lead to the inclusion on VLANs that are used for performance and not necessarily security.

Likes 0	
Dislikes 0	

Response

Bruce Reimer - Manitoba Hydro - 1,3,5,6

Answer	No
Document Name	

Comment	
We disagree with ESZ definition. Given that SCI is not needed for addressing the virtualization (See our rationale in question 1), the ESZ is not needed either. The following are the rational for not defining the ESZ: · If the ESZ is for the defense in depth and adds network layer access control for further protecting EACMS and PACS (the current requirements don't require zone protection for EACMS and PACS), we suggest modifying the existing ESP to address this as follows: "The logical bonder surrounding a network to which BES Cyber Systems, EACMS and PACS are connected through using routable protocol."	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
ERCOT agrees with the concept and offers the following modification for your consideration: "One or more segmented sections of a network used to create logical isolation."	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	
Southern asks the SDT to consider the following changes to the Electronic Security Zone definition: **Electronic Security Zone (ESZ):** A segmented logical boundary used to protect Virtual Cyber Asset applicable systems using logical isolation.	

This proposed change attempts to clarify the use of ESZs as being in virtual space, allowing for backward compatibility and continued use of traditional ESP/EAP configurations for those choosing not to apply virtualized concepts. Additionally, we recommend removing the words “of a network” as this is in conflict with the overall virtualization concepts.	
Likes 0	
Dislikes 0	
Response	
Trevor Tidwell - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	No
Document Name	
Comment	
We agree with the definition of ESZ, but ESP needs to be revised or retired. The definition of Electronic Security Zone does not have a qualifier to restrict scope to BES Cyber Systems like its sister term, ESP. Furthermore CIP-005 R1.1 has been expanded to include PACS and EACS hosted on SCI. If those PACS and EACS are not on the same network as a BCS then by definition they are not within an ESP and an entity must place them in the ESZ since no such qualifier currently exists. There are other issues, but they relate to the requirement and are addressed in comment #9. It would seem that ESP could be retired and replaced with just the ESZ term as written. We have not thought of a case where the term ESZ term could not be used in place of ESP. This would still keep backwards compatibility as older ESPs just now be an ESZ. In addition, PSP was revised with its qualifying language removed indicating it will be moved to CIP-006 requirement. This is another reason to provide conformity and replace ESP with ESZ.	
Likes 0	
Dislikes 0	
Response	
Jenifer Holmes - Alliant Energy Corporation Services, Inc. - 4 - MRO,RF	
Answer	No
Document Name	
Comment	
Alliant supports MRO NSRF's comments.	
Likes 0	
Dislikes 0	
Response	

Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	No
Document Name	
Comment	
Consider using ESZ or ESP and elaborating on the definition of the one used.	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion	
Answer	No
Document Name	
Comment	
Dominion Energy supports EEI comments	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Cleco Corporation - 1,3,5,6 - SERC	
Answer	No
Document Name	
Comment	
See EEI Comments.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No

Document Name	
Comment	
SWG agrees with the concept. We offer a modification for your consideration, “One or more segmented sections of a network used to create logical isolation.”	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	No
Document Name	
Comment	
Oncor supports EEI's comment.	
Likes 0	
Dislikes 0	
Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	
We agree with EEI comments that undefined “systems and components” is unclear. If the objective is to create a parallel term to mirror the concept of an ESP to define a virtualized environment, the definition can be simplified to “A logically isolated section of a network containing one or more VCAs.” From a security perspective we do not believe it is wise to allow mixed trust ESZs to be hosted on common hardware. We believe all ESZs on a given SCI should share the same impact, trust, or security levels. See Question 5	
Likes 0	
Dislikes 0	
Response	
Andy Crooks - SaskPower - 1,3,5,6,9 - MRO	
Answer	No

Document Name	
Comment	
We agree with EEI comments that undefined “systems and components” is unclear. If the objective is to create a parallel term to mirror the concept of an ESP to define a virtualized environment, the definition can be simplified to “A logically isolated section of a network containing one or more VCAs.” From a security perspective we do not believe it is wise to allow mixed trust ESZs to be hosted on common hardware. We believe all ESZs on a given SCI should share the same impact, trust, or security levels. See Question 5.	
Likes 0	
Dislikes 0	
Response	
Kent Feliks - AEP - 3,5	
Answer	No
Document Name	
Comment	
Please see AEP’s response to Question #1	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	No
Document Name	
Comment	
The definition is unclear, technically and in its literal meaning. A zone is not a network or a segmented section of a network. A zone does not contain only the systems or components that create logical isolation, but also includes the systems or components being isolated. CenterPoint Energy recommends the following definition for the term Electronic Security Zone: “Systems or components that create policy-based logical isolation to control access to and/or from applicable Cyber Systems, applications, or data whether singly or by group.”	
Likes 0	
Dislikes 0	
Response	

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no NGrid and Eversource	
Answer	No
Document Name	
Comment	
Comments on the Definition We recommend changing from “A segmented section of a network that contains systems and components to create a logical isolation” to “is a network that is logically isolated” because the network is logically isolated, a segment is not. The network does not “contain systems and components to create a logical isolation.”	
Likes 0	
Dislikes 0	
Response	

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
We agree with EEI comments that undefined “systems and components” is unclear. If the objective is to create a parallel term to mirror the concept of an ESP to define a virtualized environment, the definition can be simplified to “A logically isolated section of a network containing one or more VCAs.” From a security perspective we do not believe it is wise to allow mixed trust ESZs to be hosted on common hardware. We believe all ESZs on a given SCI should share the same impact, trust, or security levels. See Question 5.	
Likes 0	
Dislikes 0	
Response	

Chris Scanlon - Exelon - 1,3,5,6	
Answer	No
Document Name	
Comment	
The Exelon companies agree with the comments submitted by EEI.	
Likes 0	
Dislikes 0	

Response	
Quintin Lee - Eversource Energy - 1,3	
Answer	No
Document Name	
Comment	
See Eversource response to Question 1	
Likes 0	
Dislikes 0	
Response	
James Brown - California ISO - 2 - WECC	
Answer	No
Document Name	
Comment	
CAISO agrees with the concept. We offer a modification for your consideration, “One or more segmented sections of a network used to create logical isolation.”	
Likes 0	
Dislikes 0	
Response	
Michael Puscas - ISO New England, Inc. - 2	
Answer	No
Document Name	
Comment	
Comments: The term “segmented” should be clarified regarding the properties of a given network that would be used to identify systems in or out of a given “segment” (generally, layer 1, layer 2, and/or layer 3 would make sense). This could mean IP Address-based segmentation (i.e. layer 3), or MAC address based list of specific network interfaces (or vlans) (i.e. layer 2), or use of specific sets of cables (i.e. layer 1). It would also help to better define the concept of “isolation” with respect to member systems in a “segment.” Does “isolation” in this case specify limiting network traffic altogether between member systems or only between member systems and non-member systems or something else entirely? Or can isolation involve only partial restriction of network traffic (i.e. white/black lists of ports or protocols or even particular attributes of application use of a protocol)? It would be much more clear to identify what characteristics of communication are expected to be addressed with “isolation.” If the intended	

effect is to cut off all network communication between isolated and non-isolated systems, this might be better described as network isolation or communication isolation.

Another approach to addressing the term “logical isolation” might be to clearly call out the parameters associated with “logical” (e.g. addresses, cyber asset make, cyber asset model, connected vlan, http post request headers, etc.).   Since particular parameter choices might be considered prescriptive in terms of technology, it may be better to address the goals involved with “logical isolation.” There should be a statement that explains the goal of the “logical isolation” (i.e. whether it is supposed assist with audit, security, or service definition goals related to identifying sets of systems included in “isolation” groups.

Likes 0	
Dislikes 0	

Response

Jennifer Wright - Sempra - San Diego Gas and Electric - 1,3,5

Answer	No
Document Name	

Comment

SDG&E supports EEI’s comments submitted on our behalf.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - MRO, Group Name Westar-KCPL

Answer	No
Document Name	

Comment

Westar / Kansas City Power & Light support Edison Electric Institute’s (EEI) response to Question 3.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment	
See EEI's response to Question 1	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2 - MRO,SERC,RF	
Answer	No
Document Name	
Comment	
MISO agrees with the concept. We offer a modification for your consideration, “One or more segmented sections of a network used to create logical isolation.”	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 1,3,6	
Answer	No
Document Name	
Comment	
We believe the term Logical Isolation is unclear and open to misinterpretation by auditors. We request the SDT to include a definition of Logical Isolation or the information in the Technical Rationale in a guidance document to remove any confusion. Without it, some serial devices may be inadvertently pulled into scope for requirements that they do not pertain to.	
Likes 0	
Dislikes 0	
Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5	
Answer	No
Document Name	

Comment	
Tri-State agrees with the proposed definition.	
Likes 0	
Dislikes 0	
Response	
Greg Davis - Georgia Transmission Corporation - 1	
Answer	No
Document Name	
Comment	
GTC respectfully suggests that the definition be revised for greater consistency with the definition of an ESP as follows: ESZ: A logically isolated section of a network that contains BES Cyber Asset(s), Electronic Access Control System(s), Electronic Access Monitoring System(s), Physical Access Control System(s), Physical Access Monitoring System(s), Protected Cyber Asset(s) or their management components. Further, even in this revised definition, it is unclear how this definition would apply for policy based environments when the policy is applied to workloads and not network segments. It appears that while the issue of whether the policy has to apply at layer 3 in the OSI model is addressed, the effect is that it is still only permissible for the policy to apply to the network - instead of other elements of the system that may effectively control access.	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Network and Security Technologies - 1 - NA - Not Applicable	
Answer	No
Document Name	
Comment	
N&ST believes the proposed definition of “ESZ” is inadequate and lacks any intrinsic meaning. We suggest that it be modified by adding words that convey it is a logical boundary, established in a virtual environment, that contains one or more virtual cyber assets and provides logical isolation.	
Likes 0	
Dislikes 0	
Response	

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	
We agree with EEI's comments that undefined “systems and components” is unclear. If the objective is to create a parallel term to mirror the concept of an ESP to define a virtualized environment, the definition can be simplified to “A logically isolated section of a network containing one or more VCAs.” From a security perspective we do not believe it is wise to allow mixed trust ESZs to be hosted on common hardware. We believe all ESZs on a given SCI should share the same impact, trust, or security levels. See Question 5.	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	Yes
Document Name	
Comment	
Reclamation recommends replacing “zone” with “enclave”. Electronic Security Enclave (ESE) – A segmented section of a network that contains systems and components to create logical isolation.	
Likes 0	
Dislikes 0	
Response	

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
While this opens the standards to future technologies, each vendor's approach to policy based environments will be different and will change with technology advances. This will bring auditing challenges for auditors as each vendor will have differing approaches to policy based environments, policy outputs, and ways to present policy versus existing environments with firewalls which can be presented uniformly. We feel prior to approval(s) a standardized approved audit approach should be published for auditing policy based environments.	
Likes 0	
Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1,3,5	
Answer	Yes
Document Name	
Comment	
The ESZ provides additional flexibility.	
Likes 0	
Dislikes 0	
Response	

Chinedu Ochonogor - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
AZPS agrees with the added request of including the term VLAN to reduce misinterpretation.	
Likes 0	
Dislikes 0	
Response	
Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
City Light suggests that the measures for CIP-005-7 R1.2 (and perhaps others) include examples of how the new requirement is met by ESP/EAP concepts, in addition to how the new concepts are applied. To ensure backwards compatibility, it should be clear in the measure provided for these requirements how the SDT envisions that both the old and new approaches can be applied to demonstrate compliance.	
Likes 0	
Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,5,6 - SERC, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy supports the direction of backwards compatibility and the definition of ESZ.	
Likes 0	
Dislikes 0	
Response	
Patricia Boody - Lakeland Electric - 1,3,5,6	

Answer	Yes
Document Name	
Comment	
Changes to incorporate the defined term ESZ will require a moderate level of effort for a small entity with limited number of SCI devices. For a larger entity, the level of effort could be significant. It will require changes to policies, procedures, network diagrams, and possibly other evidence artifacts to incorporate the new defined terms and distinguish where the old terms are still being used.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Pacific Gas and Electric Company - 1,3,5 - WECC	
Answer	Yes
Document Name	
Comment	
PG&E agrees with the proposed definition of ESZ since it is the virtual equivalent of ESP. PG&E does have the concern that the addition of this definition will result in additional administrative effort related to documentation of the ESZ since it is possible an ESZ can be created for each virtual Cyber Asset (i.e. micro-segmentation). **Recommendation** - PG&E recommends the SDT get input from the industry on the potential burden and administrative impact, in order to fully understand future documentation effort.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
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	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Langston - Tallahassee Electric (City of Tallahassee, FL) - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
faranak sarbaz - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Davis Jelusich - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Public Utility District No. 1 of Chelan County	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Neil Swearingen - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Aubrey Short - FirstEnergy - FirstEnergy Corporation - 1,3,4, Group Name Aubrey Short, On Behalf of:	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

4. The SDT is addressing the risk of systems of different impact, trust, or security levels (“mixed trust”) environments that are possible on Shared Cyber Infrastructure by modifying the definition of Protected Cyber Asset (PCA) so that it includes those VCA’s that can share a hypervisor’s CPU or memory. Do you agree with the proposed modifications? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification. (CIP-005 Technical Rationale pages 8, and 14-15).

Trevor Tidwell - PNM Resources - Public Service Company of New Mexico - 1,3

Answer	No
Document Name	

Comment

It is unclear what risks the SDT is trying to address. The rationale mentions the risk of side channel attacks in pages 14-15. However it isn’t clear in the standard that is the risk being addressed. The purpose of the proposed CIP-005 is “To protect BES Cyber Systems against compromise by allowing only known and controlled communication to and from the system and logically isolating all other communication.” Per the purpose we should protect BES Cyber Systems communications and side channel could be considered a form of communication. However it isn’t clear why PACS and EACS hosted on SCI are included throughout the standard since protecting their communication is not the purpose of the standard. The page 36 of rationale indicates it is because of the mixed trust issues when they utilize the same SCI. A PACS or EACS utilizing the same SCI as a BES Cyber Asset is by proposed definition a PCA. If the PACS or EACS is virtualized and on the same SCI then bullet #3 of PCA applies. If the PACS or EACS are physical yet are within the same ESZ as the BES Cyber Asset then it could be argued per current proposed definition they are sharing SCI that performs logical isolation of an ESZ or ESP. It is a fallacy of industry that an EACS and PACS cannot be a PCA. By proposed definition if they reside within the same ESP, same ESZ, or share computing resources then they are also a PCA. If the intent is to prevent side channel attacks from EACS or PACS sharing SCI with BCAs then strike PACS hosted on SCI and EACS hosted on SCI from the Applicable Systems as they are already covered by the term PCA. If the intent is to prevent side channel attacks on EACS and PACS then the purpose of the standard needs to be revised and consider controlling communication to all EACS and PACS both physical and virtual. As it stands right now the requirements rope in any EACS or PACS that is virtualized and not just the ones that are on the same SCI as BCAs. The definition of SCI does not restrict to only those devices shared with BCAs. When one looks at the CIP-005 purpose and the rationale it appears expansion of scope to virtualized EACS and PACS is beyond what was intended.

Also, the risk of shared storage is not addressed, but it isn't a communication issue so this could be a CIP-007 item. A VCA could theoretically use up all the remaining storage on the storage array if it was allowed to grow as needed. This could result in a DoS of additional storage needed by a BCA on the same SCI. The problem is not sharing of CPU, memory, or storage. The problem is if there are no policies policing the use of CPU, memory, or storage. Proper policies would mitigate the risk just as well as physically separate hardware.

Likes 0	
Dislikes 0	

Response

Bruce Reimer - Manitoba Hydro - 1,3,5,6

Answer	No
Document Name	

Comment

Based on our comments in the question 1, given that SCI would fall within the definition of BCS, EACMS or PACS, the mixed trust environment cannot be used, where the hypervisor or management plane for hosting or managing the CIP Cyber Assets has to be separated from those that are not used for hosting or managing non-CIP cyber assets.

Likes 0	
Dislikes 0	

Response

Teresa Cantwell - Lower Colorado River Authority - 1,5

Answer	No
Document Name	

Comment

The definition groups too many categories together. For example, there may be specific software for the hypervisor. That is not the same as an out of scope VM.

Likes 0	
Dislikes 0	

Response

Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5

Answer	No
Document Name	

Comment

We think more work is needed to future-proof the definition. Would like the definition to be less prescriptive and more qualitative. Would like modifications at a higher level, so we are not limited to today’s environment and explanations. For example, imagine a scenario where multiple VMs with different CIP classifications are hosted on a single hypervisor. Each VM is connected on a separate VLAN to a single virtual managed switch. The virtual switch is connected to a physical switch through a trunked port that carries all the VLANs. The physical switch is physically connected to a firewall, which provides routing and logical separation with ACL.

In this scenario, is there sufficient logical segregation so that we could have an EACMS VM, Out of Scope VM on the same SCI with the hypervisor declared as an EACMS?

Likes 0	
Dislikes 0	

Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
EEI does not support the SDT’s current approach to mixed trust environments. Our primary concern centers on the hypervisor, which is known to have vulnerabilities to cyber-attack through any of the Virtual Cyber Assets (VCA) on the hypervisor. It is our view that securing the VCAs in a lower risk environment at a lower cyber security posture versus the VCAs in the higher risk environment increases the hypervisor’s vulnerability to attack diminishing the protections already established under the CIP Standards. We are also concerned that the proposed definition of PCAs may introduce similar risks, given the linkage between the two terms (i.e., VCAs and PCAs). It is our recommendation that the hypervisor and the control(s) it enables, logical separation of VCAs, need to be considered just as vulnerable as any computer system, whether connected to BES Cyber Systems or not.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - MRO, Group Name Westar-KCPL	
Answer	No
Document Name	
Comment	
Westar / Kansas City Power & Light support Edison Electric Institute’s (EEI) response to Question 4.	
Likes 0	
Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,5,6 - SERC, Group Name Duke Energy	
Answer	No
Document Name	
Comment	

Duke Energy does not support the modified definition of PCA as currently proposed.This definition does not adequately address the issue of mixed trust environment nor does it allow for the existence of non-BES and BES cyber assets (or Virtual Cyber Assets) to exit within the same SCI. SCI is subject to same level of requirement as BCA, and doesn't help entities employing mixed trust environment.	
Likes 0	
Dislikes 0	
Response	
Jennifer Wright - Sempra - San Diego Gas and Electric - 1,3,5	
Answer	No
Document Name	
Comment	
SDG&E supports EEI’s comments submitted on our behalf.	
Likes 0	
Dislikes 0	
Response	
Michael Puscas - ISO New England, Inc. - 2	
Answer	No
Document Name	
Comment	
Comments: If the definition of shared attributes (CPU, memory) is to be consistent with the SCI definition, please include in the PCA definition VCAs that share storage with a hypervisor as well.	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1,3	
Answer	No
Document Name	
Comment	

Eversource does not support the SDT’s current approach to mixed trust environments. Our primary concern centers on the hypervisor, which is known to have vulnerabilities to cyber-attack through any of the Virtual Cyber Assets (VCA) on the hypervisor. It is our view that securing the VCAs in a lower risk environment at a lower cyber security posture versus the VCAs in the higher risk environment increases the hypervisor’s vulnerability to attack diminishing the protections already established under the CIP Standards. It is our recommendation that the hypervisor and the control(s) it enables, logical separation of VCAs, need to be considered just as vulnerable as any computer system, whether connected to BES Cyber Systems or not.	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1,3,5,6	
Answer	No
Document Name	
Comment	
The Exelon companies agree with the comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no NGrid and Eversource	
Answer	No
Document Name	
Comment	
Request confirmation that the intent of new, third bullet in the PCA definition is “Other tenants that share the same host VM as a BES Cyber System become an associated PCA” Request clarification on this “mixed trust.” Does high watermarking apply in a mixed trust situation?	
Likes 0	
Dislikes 0	
Response	
Davis Jelusich - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Public Utility District No. 1 of Chelan County	

Answer	No
Document Name	

Comment

CHPD believes that this is an improvement from the prior definition; however, the inclusion of the third bullet “Share compute resources (CPU or memory) with a BES Cyber System” eliminates the benefits of sharing virtual infrastructure between CIP and non-CIP devices (all non-CIP virtual systems hosted on the same SCI will become PCAs under this language). CHPD proposes that the third bullet be removed.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

The proposed requirement prevents or severely limits use of cloud-based systems. While the risk of virtual machine escape is not zero, it is very small and mitigation through hypervisor patching, integrity checking, or other means is more appropriate than bringing all other hosted tenants into scope. Isolation from other tenants may be impossible on cloud-based systems today, and future industry hosted systems as virtualized environments become the normal way or even required or the only option. The SDT must consider an acceptable way to mitigate virtual machine escape risk that is independent of other tenants.

Likes 0	
Dislikes 0	

Response

Kent Feliks - AEP - 3,5

Answer	No
Document Name	

Comment

AEP does not currently support mixed trust environments, as we believe that hypervisor needs to be considered equally vulnerable as any system regardless of its connectivity to BES Cyber Systems. AEP is of the opinion that the SDT’s current approach makes the hypervisor more vulnerable to attack, negatively affecting the protections already in place as a result of the CIP standards.

Likes 0	
Dislikes 0	

Response	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	No
Document Name	
Comment	
Oncor supports EEI's comment.	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Cleco Corporation - 1,3,5,6 - SERC	
Answer	No
Document Name	
Comment	
See EEI Comments.	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion	
Answer	No
Document Name	
Comment	
Dominion Energy supports EEI comments	
Likes 0	
Dislikes 0	
Response	

Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF	
Answer	No
Document Name	
Comment	
Items separated in the different ESZs should not be categorized as PCAs in order to make the new requirements feasible for implementation. Implementation of Virtual Environments requires the replacement of a certain number of cyber assets to be economically viable. Entities whose physical ESP devices do not themselves reach this threshold will have additional compliance burden and cost from changes to this standard since they will not choose the greater cost to use CIP Virtual Environments due to separate ESZ devices now coming into PCA scope.	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jenifer Holmes - Alliant Energy Corporation Services, Inc. - 4 - MRO,RF	
Answer	Yes
Document Name	
Comment	
Alliant supports MRO NSRF's comments.	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	

Answer	Yes
Document Name	
Comment	
Regarding the definition of PCA, please provide an example of a PCA that would be on an ESP. On bullet 2, ERCOT suggests replacing “that” with “and.”	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 3,4	
Answer	Yes
Document Name	
Comment	
GSOC/OPC agrees with the intent. However, as discussed above, the inclusion of both Cyber Asset and VCA in the revised definitions of BCA and Protected Cyber Asset (PCA) could create redundancy, lead to an expansion of the Cyber Assets and BCAs that are in scope, and could unintentionally cause ambiguity. For example, the inclusion of a provision around “shared compute resources” seems at odds with the concept of logical isolation proposed and appears to result in a clear expansion of “in scope” cyber assets. For this reason, the proposed definitions could have unintended consequences to the fleet of CIP Standards including CIP-013-1, e.g., the structure of the definitions could result in the inclusion of “excluded programmable devices.” As discussed above, revisions and/or clarification to the structure of the definitions is requested to ensure that those VCAs intended to be excluded by virtue of logical isolation are, in fact, excluded and are not inadvertently brought into scope. Alternatively, clarification and guidance could be provided through the development of compliance and/or implementation guidance, similar to the effort that the SDT team undertook when drafting the BES Definition. Such guidance issued should include appropriate diagrams such as those provided on pages 39 – 40 of the Technical Rationale document.	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
We agree with the modifications to the PCA definition to incorporate VCAs and shared resources, but do not believe this is sufficient to permit mixed trust, as addressed in Question 5.	

Likes 0	
Dislikes 0	
Response	
Greg Davis - Georgia Transmission Corporation - 1	
Answer	Yes
Document Name	
Comment	
We agree with the intent. However, as discussed above, the inclusion of both Cyber Asset and Virtual Cyber Asset in the revised definitions of BES Cyber Asset and Protected Cyber Asset could create redundancy, lead to an expansion of the Cyber Assets and BES Cyber Assets that are in scope, and could unintentionally cause ambiguity. For example, the inclusion of a provision around “shared compute resources” seems at odds with the concept of logical isolation proposed and appears to result in a clear expansion of “in scope” cyber assets. For this reason, the proposed definitions could have unintended consequences to the fleet of CIP Standards including CIP-013-1, e.g., the structure of the definitions could result in the inclusion of “excluded programmable devices.” As discussed above, revisions and/or clarification to the structure of the definitions is requested to ensure that those Virtual Cyber Assets intended to be excluded by virtue of logical isolation are, in fact, excluded and are not inadvertently brought into scope. Alternatively, clarification and guidance could be provided through the development of compliance and/or implementation guidance, similar to the effort that the SDT team undertook when drafting the BES Definition. Such guidance issued should include appropriate diagrams such as those provided on pages 39 – 40 of the Technical Rationale document.	
Likes 0	
Dislikes 0	
Response	
Aubrey Short - FirstEnergy - FirstEnergy Corporation - 1,3,4, Group Name Aubrey Short, On Behalf of:	
Answer	Yes
Document Name	
Comment	
This will require discrete zones/networks (CIP management ESZs or ESPs) for ERC to hypervisors as the hypervisor will be considered an associated PCA of the highest impact rating of a guest OS that the hypervisor maintains.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Pacific Gas and Electric Company - 1,3,5 - WECC	
Answer	Yes

Document Name	
Comment	
PG&E agrees with the modification of PCA to include VCA’s. This clearly indicates that a PCA can be the current “physical” type of device or the newer “virtual” type of device.	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2 - MRO,SERC,RF	
Answer	Yes
Document Name	
Comment	
Regarding the definition of PCA, please provide an example of a PCA that would be "on an ESP." On bullet 2, replace “that” with “and."	
Likes 0	
Dislikes 0	
Response	
James Brown - California ISO - 2 - WECC	
Answer	Yes
Document Name	
Comment	
Regarding the definition of PCA, please provide an example of a PCA that would be on an ESP. On bullet 2, replace “that” with “and”.	
Likes 0	
Dislikes 0	
Response	
Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	

City Light agrees with the concept to high watermark a mixed trust environment, but we find the proposed modifications to the PCA definition can be confusing. Please provide additional clarification.	
Likes 0	
Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1,3,5	
Answer	Yes
Document Name	
Comment	
Is it technology capable to prioritize one VM/VCA over another from a reservation perspective? Not sure how this functionality is involved with respect to ensuring that a ‘mixed trust’ event will not occur. If it is involved, can additional information in the Guidance document be provided?	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
We agree with the modifications to the PCA definition to incorporate VCAs and shared resources, but do not believe this is sufficient to permit mixed trust, as addressed in Question 5.	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	

BPA believes that mixed trust is not the correct term for shared infrastructure that implements security controls between the differing security zones. Modern technology starts with a zero trust model and then adds necessary, controlled levels of trust through a whitelisting or additive model and therefore controls the risk. The benefit of shared infrastructure includes lower cost of ownership, but also focuses cyber security efforts on what is important rather than spreading scarce personnel or fiscal resources thin for minimal return on effort.

"Mixed trust" as used in other industry and best practices guidance typically means that assets subject to different levels of security control have no security mechanism between them. This is not the case in a properly configured virtual environment.

BPA also believes that there needs to be clear understanding around the difference between “impact level” and “Risk level” as impact is simply one aspect of overall risk, which includes probability, threat actors, vulnerabilities, etc.

Likes 0	
Dislikes 0	

Response

Andy Crooks - SaskPower - 1,3,5,6,9 - MRO

Answer	Yes
Document Name	

Comment

Agree with the modifications to the PCA definition to incorporate VCAs and shared resources, but do not believe this is sufficient to permit mixed trust, as addressed in Question 5.

Likes 0	
Dislikes 0	

Response

Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	Yes
Document Name	

Comment

Agree with the modifications to the PCA definition to incorporate VCAs and shared resources, but do not believe this is sufficient to permit mixed trust, as addressed in Question 5.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
Regarding the definition of PCA, please provide an example of a PCA that would be on an ESP. On bullet 2, replace “that” with “and”.	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Consider that quality of service configuration can be applied to overcome mixed trust issues. You can have virtualization workloads with PCA and non PCA environments while guaranteeing compute resources to PCA environments.	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Network and Security Technologies - 1 - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 1,3,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Patricia Boody - Lakeland Electric - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Neil Swearingen - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Chinedu Ochonogor - APS - Arizona Public Service Co. - 1,3,5,6	
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, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

faranak sarbaz - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Langston - Tallahassee Electric (City of Tallahassee, FL) - 1,3,5	
Answer	Yes
Document Name	
Comment	

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

Texas RE seeks the following clarification on the Protected Cyber Asset (PCA) definition:

- Regarding the statement “*or on an Electronic Security Perimeter*”, what does this mean logically from a networking perspective when A PCA IP address is within an ESP? ESPs are usually IP addresses (ranges, subnets, vlans, etc.).

Likes 0	
Dislikes 0	
Response	

5. The SDT proposes to address infrastructure that is shared between differing BCS impact ratings that share CPU and memory resources by aligning the CIP Requirements for all systems within an ESZ or ESP and affinity to prevent sharing of CPU and memory between Virtual Cyber Assets of differing impact ratings. Do you agree with these changes? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification. (CIP-005 Technical Rationale pages 11, 12, and 14).	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	
We agree with EEI's comments. We do not believe that cyber infrastructure can be shared among VCAs of differing impact, trust, or security levels without rendering all VCAs on SCI susceptible to disruption by a successful attack on the VCA with the lowest level of impact, trust, or security. Although this proposal protects the CPU and memory, it still leaves the Hypervisor vulnerable. SCI needs to be limited to a single impact, trust, or security level; each level needs its own SCI. If virtualization and all its benefits are to be pursued, it cannot be at the expense of compromised security in pursuit of reducing the monetary expense of SCI by hosting mixed trust zones on a single common infrastructure.	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5	
Answer	No
Document Name	
Comment	
This equates to not being able to use a shared virtual environment for even EACS, there would need to be dedicated environments.	
Likes 0	
Dislikes 0	
Response	
Bruce Reimer - Manitoba Hydro - 1,3,5,6	
Answer	No
Document Name	
Comment	

We agree with the principle and disagree with the changes. Based on our comments in the question 1, given that SCI would fall within the definition of BCS, EACMS or PACS, the hypervisor or management plane would be protected at the same level as one of the BCA, EACMS or PACS it hosts or manages. We suggest change R1 Part 1.6 to the following:

“All applicable systems shall not share CPU and memory with non-applicable systems.”

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

See Southern’s comments to previous questions.

Likes 0	
Dislikes 0	

Response

Trevor Tidwell - PNM Resources - Public Service Company of New Mexico - 1,3

Answer	No
Document Name	

Comment

Where did the SDT prevent the sharing of CPU and memory between VCAs of differing impact ratings? The CPU and memory sharing come up in R1.6 and R2.6. R1.6 is only for management systems and not the actual VCAs. There is no language that the sharing cannot be across impact ratings. Also if VCAs are of differing impact ratings then the lower impact rating VCA is by proposed definition a PCA. Is the SDT proposing to not allow BCAs and PCAs to share CPU and memory on SCI?

Both R1.6 and R2.6 are not what was promised by objective and not prescriptive. As discussed at the end of response to comment #4, good policies on CPU, memory, and storage usage could address the risk associated with sharing those resources. However the SDT has prescribed that the “Thou shall not share CPU or memory” as the only means to address the risk. Both R1.6 and R2.6 have other problems which are addressed in other comments, but they are clearly prescriptive and not objective. Consider language of “Have a means to reduce risk of a VCA utilizing CPU, memory, or storage in a way that prevents other VCAs from having access to those resources.” An entity can either physically separate the systems or use policies to achieve the objective.

Likes 0	
Dislikes 0	
Response	
Jenifer Holmes - Alliant Energy Corporation Services, Inc. - 4 - MRO,RF	
Answer	No
Document Name	
Comment	
Alliant supports MRO NSRF's comments.	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF	
Answer	No
Document Name	
Comment	
Items separated in the different ESZs should not be categorized as PCAs in order to make the new requirements feasible for implementation. Implementation of Virtual Environments requires the replacement of a certain number of cyber assets to be economically viable. Entities whose physical ESP devices do not themselves reach this threshold will have additional compliance burden and cost from changes to this standard since they will not choose the greater cost to use CIP Virtual Environments due to separate ESZ devices now coming into PCA scope.	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion	
Answer	No
Document Name	
Comment	
Dominion Energy supports EEI comments	

Likes 0	
Dislikes 0	
Response	
Clay Walker - Cleco Corporation - 1,3,5,6 - SERC	
Answer	No
Document Name	
Comment	
See EEI Comments.	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	No
Document Name	
Comment	
Oncor supports EEI's comment.	
Likes 0	
Dislikes 0	
Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	
We agree with EEI comments. We do not believe that cyber infrastructure can be shared among VCAs of differing impact, trust, or security levels without rendering all VCAs on SCI susceptible to disruption by a successful attack on the VCA with the lowest level of impact, trust, or security. Although this proposal protects the CPU and memory, it still leaves the Hypervisor vulnerable. SCI needs to be limited to a single impact, trust, or security level; each level needs its own SCI. If	

virtualization and all its benefits are to be pursued, it cannot be at the expense of compromised security in pursuit of reducing the monetary expense of SCI by hosting mixed trust zones on a single common infrastructure	
Likes 0	
Dislikes 0	
Response	
Andy Crooks - SaskPower - 1,3,5,6,9 - MRO	
Answer	No
Document Name	
Comment	
We agree with EEI comments. We do not believe that cyber infrastructure can be shared among VCAs of differing impact, trust, or security levels without rendering all VCAs on SCI susceptible to disruption by a successful attack on the VCA with the lowest level of impact, trust, or security. Although this proposal protects the CPU and memory, it still leaves the Hypervisor vulnerable. SCI needs to be limited to a single impact, trust, or security level; each level needs its own SCI. If virtualization and all its benefits are to be pursued, it cannot be at the expense of compromised security in pursuit of reducing the monetary expense of SCI by hosting mixed trust zones on a single common infrastructure.	
Likes 0	
Dislikes 0	
Response	
Kent Feliks - AEP - 3,5	
Answer	No
Document Name	
Comment	
Please see AEP's response to Questions #1 and #4	
Likes 0	
Dislikes 0	
Response	
Davis Jelusich - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Public Utility District No. 1 of Chelan County	
Answer	No
Document Name	

Comment

CHPD disagrees with the proposed changes. The proposed changes would require implementation of additional infrastructure in order to keep non-BES Cyber Systems out of scope. See the comments in questions #1, #2, and #4, above, for recommendations. Correction to these other areas are first needed before CHPD can evaluate the effects of the language on differing impact ratings.

Likes 0

Dislikes 0

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no NGrid and Eversource

Answer No

Document Name

Comment

Since “affinity” is not a defined term, and not used in the Requirement, it is difficult to respond positively to this question. We suggest that the Technical Rationale is expanding and guiding not justifying the Requirement. We request clarification.

GENERAL COMMENT – we recommend that these questions (1 – 8) should focus on what the auditor will use (Definitions and Standards), and less so on the Technical Rationale.

We agree with the concept that all tenants on the same VM host should be high watermarked against BES Cyber System impact rating.

Likes 0

Dislikes 0

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer No

Document Name

Comment

We agree with EEI comments.

We do not believe that cyber infrastructure can be shared among VCAs of differing impact, trust, or security levels without rendering all VCAs on SCI susceptible to disruption by a successful attack on the VCA with the lowest level of impact, trust, or security. Although this proposal protects the CPU and memory, it still leaves the Hypervisor vulnerable. SCI needs to be limited to a single impact, trust, or security level; each level needs its own SCI. If virtualization and all its benefits are to be pursued, it cannot be at the expense of compromised security in pursuit of reducing the monetary expense of SCI by hosting mixed trust zones on a single common infrastructure.

Likes 0

Dislikes 0	
Response	
Chris Scanlon - Exelon - 1,3,5,6	
Answer	No
Document Name	
Comment	
The Exelon companies agree with the comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1,3	
Answer	No
Document Name	
Comment	
See Eversource responses to Questions 1 and 4.	
Likes 0	
Dislikes 0	
Response	
Michael Puscas - ISO New England, Inc. - 2	
Answer	No
Document Name	
Comment	
ISO-NE does not agree because the concepts of shared infrastructure and affinity are not included in the requirements of the standard (e.g., “affinity” is not described or defined in the requirements). Rather, the concepts are only mentioned in the Technical Rationale. These concepts, however, should be addressed in the requirements.	
Likes 0	
Dislikes 0	

Response	
Jennifer Wright - Sempra - San Diego Gas and Electric - 1,3,5	
Answer	No
Document Name	
Comment	
SDG&E supports EEI’s comments submitted on our behalf.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - MRO, Group Name Westar-KCPL	
Answer	No
Document Name	
Comment	
Westar / Kansas City Power & Light support Edison Electric Institute’s (EEI) response to Question 5.	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
See EEI’s responses to Questions 1 and 4.	
Likes 0	
Dislikes 0	
Response	

David Jendras - Ameren - Ameren Services - 1,3,6	
Answer	No
Document Name	
Comment	
Our concern is that this prevents responsible entities from being able to efficiently leverage emerging technologies. We propose that the protections and requirements for the highest impact VCA hosted in the shared environment should be extended to all VCAs hosted, and to the SCI.	
Likes 0	
Dislikes 0	
Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5	
Answer	No
Document Name	
Comment	
No, not entirely. We agree with the scenario presented, but also think other scenarios should be permitted. See Tri-State's comments on question #2 for more information.	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes

Document Name	
Comment	
None.	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
The difference between ESP and ESZ are difficult to determine. Please provide a basis for determining the difference between the two terms.	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
The definition of Shared Cyber Infrastructure does not clearly convey mixed trust is not allowed.	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	

None	
Likes 0	
Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1,3,5	
Answer	Yes
Document Name	
Comment	
The Yes response assumes that provisions will be provided to allow existing Entity implementations within NERC environments. Will Entities be provided a phased in consideration for existing architecture and the implantation guidelines be reflective of the phased in approach? Additonally, ensure all new terms are defined.	
Likes 0	
Dislikes 0	
Response	
Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
City Light agrees with the concept to high watermark a mixed trust environment.	
Likes 0	
Dislikes 0	
Response	
James Brown - California ISO - 2 - WECC	
Answer	Yes
Document Name	
Comment	

CAISO has no additional comments regarding this question.

Likes 0	
Dislikes 0	

Response

Masuncha Bussey - Duke Energy - 1,5,6 - SERC, Group Name Duke Energy

Answer	Yes
Document Name	

Comment

Duke Energy agrees with the prevention of CPU and memory sharing between Virtual Cyber Assets of differing impact ratings.

Likes 0	
Dislikes 0	

Response

Michael Johnson - Pacific Gas and Electric Company - 1,3,5 - WECC

Answer	Yes
Document Name	

Comment

PG&E agrees with the modification and understands the reasoning for the implementation of no mixed-trust to handle the unique vulnerabilities of shared CPU and memory that continue to appear.

While the elimination of mixed-trust will reduce some of the benefits of virtualization, vulnerabilities with shared CPU and memory demonstrated over the last couple of years indicate mixed-trust could be a significant risk to the reliable operation of the Bulk Electric System (BES), necessitating the restriction.

Likes 0	
Dislikes 0	

Response

Roger Fradenburgh - Network and Security Technologies - 1 - NA - Not Applicable

Answer	Yes
Document Name	

Comment	
N&ST suggests that a contextual definition of “affinity” be included in the Technical Rational document at the very least, if not in CIP-005 itself.	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 3,4	
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	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Scott Langston - Tallahassee Electric (City of Tallahassee, FL) - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
faranak sarbaz - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Chinedu Ochonogor - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Neil Swearingen - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Patricia Boody - Lakeland Electric - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2 - MRO,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aubrey Short - FirstEnergy - FirstEnergy Corporation - 1,3,4, Group Name Aubrey Short, On Behalf of:	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Greg Davis - Georgia Transmission Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE agrees it is a best practice that VCAs of different impact ratings should not share CPU and memory.	
Likes 0	
Dislikes 0	
Response	

6. The SDT is proposing the addition of exemption 4.2.3.3 and CIP-005 requirement R1 part 1.3 for “Super-ESP” scenarios where single ESP’s or ESZ’s span multiple geographic locations. Do you agree with the proposed modifications? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification. (CIP-005 Technical Rationale pages 18, and 25-26).

Bruce Reimer - Manitoba Hydro - 1,3,5,6	
Answer	No
Document Name	
Comment	
We disagree with the “Super-ESP” scenarios. Given that protocol tunneling can explicitly bypass security restrictions and poses a serious challenge to network security, SDT shouldn’t modify the current CIP-005 requirements to allow use tunneling protocols between sites within a super ESP without protecting devices such as switches and routers within the same ESP. For the current CIP requirements, if a super ESP is designated across multiple geographic locations, all Cyber Assets within the ESP must be identified as BCAs or PCAs, which is reasonable from a sound security practice perspective. The proposed R1.3 may not be achievable since the devices could be owned by third parties.	
Likes 0	
Dislikes 0	
Response	

Roger Fradenburgh - Network and Security Technologies - 1 - NA - Not Applicable	
Answer	No
Document Name	
Comment	
While N&ST supports the concept of multi-site ESPs or ESZs (and we note that so-called “extended” ESPs exist TODAY), we are concerned about the fact the proposed new requirement includes no definition of “geographic location.” This omission will, in our view, likely lead to arguments about where and when the requirement would apply. Within a single building where applicable systems in a single ESP or ESZ are in different rooms? On different floors? In different buildings that are located at the same street address? In addition, N&ST believes the requirement to provide the type of protection sought by the proposed new requirement has already been established in CIP-006-6, specifically by R1 Part 1.10.	
Likes 0	
Dislikes 0	
Response	

David Jendras - Ameren - Ameren Services - 1,3,6	
Answer	No
Document Name	
Comment	

We believe that the wording may create some confusion for entities in implementation. Our concern is that a new term for intelligent electronic devices is used. We recommend that a proper definition with information around what it includes be provided by the SDT.	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
EEI supports the Super-ESP concept believing it has potential benefits. We also understand that some EEI members have seen their respective Regional Entities support the concept of a Super-ESP. However, the proposed ESZ definition would need to be clarified before moving forward with the proposed exemptions for Super-ESP scenarios. (See our response to Question 1)	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - MRO, Group Name Westar-KCPL	
Answer	No
Document Name	
Comment	
Westar / Kansas City Power & Light support Edison Electric Institute's (EEI) response to Question 6.	
Likes 0	
Dislikes 0	
Response	
Jennifer Wright - Sempra - San Diego Gas and Electric - 1,3,5	
Answer	No
Document Name	
Comment	

SDG&E supports EEI's comments submitted on our behalf. Additionally, SDG&E requests further clarification of the term "geographical locations."	
Likes 0	
Dislikes 0	
Response	
Michael Puscas - ISO New England, Inc. - 2	
Answer	No
Document Name	
Comment	
The requirement is potentially duplicative of CIP-006 R1.10. In addition, CIP-012 does not have a column in the requirements for Applicable Systems, but only states that Real-Time Assessment and real-time monitoring data must be protected in terms of confidentiality and integrity. CIP-005-7 is proposing to include a requirement that is applied to only Applicable Systems as listed (without clear association between systems and the data those systems manage). Because one requirement addresses concerns identified per system and the other standard addresses concerns identified per type of data, there is potential of overlapping systems / data that both standards and requirements could address. This is confusing and should be avoided where possible, particularly where both requirements identify similar security concerns, but with slightly different language.	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1,3	
Answer	No
Document Name	
Comment	
Eversource agrees the Super-ESP concept has potential benefits; however, we do not support the concept when considered within the framework of the proposed ESZ definition, as discussed in a previous response.	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1,3,5,6	
Answer	No
Document Name	

Comment	
The Exelon companies agree with the comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no NGrid and Eversource	
Answer	No
Document Name	
Comment	
We suggest reviewing the new CIP-005 Part 1.3 to determine if there is duplication or redundancy with the existing CIP-006 Part 1.10	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	No
Document Name	
Comment	
CenterPoint Energy believes that 4.2.3.3 is not needed since a simple modification to 4.2.3.2 can cover all situations. Presently the modified 4.2.3.2. is, “Cyber Assets, including third-party owned Cyber Assets, associated with communication networks and data communication links between discrete Electronic Security Perimeters or Electronic Security Zones.” CenterPoint Energy proposes that 4.2.3.2. should be modified to: “Cyber Assets, including third-party owned Cyber Assets, associated with external communication networks and external data communication links.” All Cyber Assets used for external communication networks and external data communication links should be excluded, not just those used in certain situations. With this modification, 4.2.3.3 is not needed.	
Likes 0	
Dislikes 0	
Response	
Kent Feliks - AEP - 3,5	
Answer	No

Document Name	
Comment	
AEP is of the opinion that the Super-ESP concept has potential benefits, but we feel the ESZ definition being proposed should be clarified before moving forward with the exemptions for Super-ESP situations. Please see AEP’s response to Question #1.	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	No
Document Name	
Comment	
Oncor supports EEI's comment.	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Cleco Corporation - 1,3,5,6 - SERC	
Answer	No
Document Name	
Comment	
See EEI Comments.	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion	
Answer	No
Document Name	
Comment	

Dominion Energy supports EEI comments	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	No
Document Name	
Comment	
The exemption increases vulnerability in the CIP communication architecture.	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jenifer Holmes - Alliant Energy Corporation Services, Inc. - 4 - MRO,RF	
Answer	Yes
Document Name	
Comment	
Alliant supports MRO NSRF's comments.	
Likes 0	

Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern supports the concept of Super-ESPs and the potential benefits that could be realized in implementing this concept. However, the proposed ESZ definition should be clarified or modified before moving forward with the proposed exemptions for Super-ESP scenarios.	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
None.	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 3,4	
Answer	Yes
Document Name	
Comment	
GSOC/OPC agrees with the addition of CIP-005 requirement R1 part 1.3, but has concerns that the wording of Exemption 4.2.3.3 is ambiguous and could result in confusion or misinterpretation relative to the excluded assets. For example, use of the phrase “associated with” when coupled with expansive terms such as “communication networks and data communication links” could result in differing interpretations and applications by different entities, e.g., one entity could view an asset or type of equipment as “associated with” “communication networks” and/or “data communication links” while others would not. This potential for confusion and multiple interpretations could be exacerbated where different regions and auditors manifest differences in application of the exemption during compliance monitoring activities. GSOC/OPC recommends that the SDT consider utilizing verbiage in	

the exception that hews more closely to the language utilized in the Technical Rationale document, i.e., transport networks. For example, the exemption could be revised as follows:

4.2.3.3. Cyber Assets, including third-party owned Cyber Assets, associated with transport networks and associated data communication links used to extend a discrete ESP or ESZ to one or more geographic location(s).

Likes 0	
Dislikes 0	

Response

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5

Answer	Yes
Document Name	

Comment

We agree with the specific addition of exemption 4.2.3.3 and CIP-005 requirement R1 part 1.3, provided the ESZ concerns posed in **Question 3** are addressed.

We agree with EEI's comments that undefined “systems and components” is unclear. If the objective is to create a parallel term to mirror the concept of an ESP to define a virtualized environment, the definition can be simplified to “A logically isolated section of a network containing one or more VCAs.” From a security perspective we do not believe it is wise to allow mixed trust ESZs to be hosted on common hardware. We believe all ESZs on a given SCI should share the same impact, trust, or security levels.

Likes 0	
Dislikes 0	

Response

Greg Davis - Georgia Transmission Corporation - 1

Answer	Yes
Document Name	

Comment

GTC agrees with the addition of CIP-005 requirement R1 part 1.3, but has concerns that the wording of Exemption 4.2.3.3 is ambiguous and could result in confusion or misinterpretation relative to the excluded assets. For example, use of the term “associated with” could result in differing applications by different entities, e.g., one entity could view an asset as “associated with” while others would not. This potential for confusion and multiple interpretations could be exacerbated where different regions and auditors manifest differences in application of the exemption during compliance monitoring activities. GTC recommends that the SDT consider utilizing verbiage in the exception that hews more closely to the language utilized in the Technical Rationale document, i.e., transport networks. For example, the exemption could be revised as follows:

4.2.3.3. Cyber Assets, including third-party owned Cyber Assets, associated with transport networks and associated data communication links used to extend a discrete ESP or ESZ to one or more geographic location(s).

Likes 0	
Dislikes 0	
Response	
Michael Johnson - Pacific Gas and Electric Company - 1,3,5 - WECC	
Answer	Yes
Document Name	
Comment	
PG&E agrees with the exception modification to include Electronic Security Zone (ESZ) in 4.2.3.2 and the addition of 4.2.3.3 to address the interconnection of discrete Electronic Security Perimeters (ESP) and ESZ for third-party Cyber Assets PG&E would not have direct control of. This will codify the creation of “Super-ESP/ESZ,” which many Entities are currently using and reduce potential compliance issues as a result of differences in opinion between Entities and Audit Teams on the creation of a “Super-ESP” under the current requirements. PG&E also indicates the creation of Requirement Part 1.3 clearly indicates the confidentially and integrity of communications must be maintained by the Entity, even when third-party-owned Cyber Assets are being used.	
Likes 0	
Dislikes 0	
Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5	
Answer	Yes
Document Name	
Comment	
Tri-State agrees with the proposed modifications.	
Likes 0	
Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,5,6 - SERC, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	

Duke Energy agrees with the concept of Super-ESP as long as it is optional and backward compatible to the current CIP-005 requirement.	
Likes 0	
Dislikes 0	
Response	
James Brown - California ISO - 2 - WECC	
Answer	Yes
Document Name	
Comment	
CAISO has no additional comments regarding this question.	
Likes 0	
Dislikes 0	
Response	
Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
City Light agrees that “Super-ESP” scenarios must be addressed and accepts the proposed approach as perhaps the most appropriate one possible within the CIP Standards. At the same time, City Light is concerned that about expanding the existing confusion about “communications infrastructure” into a much less well-defined space. We have spent hours at each CIP audit explaining our approach to communications infrastructure; each time it seems we need to re-educate and convince a new team of CIP auditors. We urge that extensive examples and training—for entities and auditors alike—be developed to minimize the audit risks associated with this change, before this concept takes force in a Standard. We recommend a pilot study, similar to the regional pilots of CIP v5, with lessons learned for both industry and auditors.	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	

Comment	
We agree with the specific addition of exemption 4.2.3.3 and CIP-005 requirement R1 part 1.3, provided the ESZ concerns posed in **Question 3** are addressed. We agree with EEI comments that undefined “systems and components” is unclear. If the objective is to create a parallel term to mirror the concept of an ESP to define a virtualized environment, the definition can be simplified to “A logically isolated section of a network containing one or more VCAs.” From a security perspective we do not believe it is wise to allow mixed trust ESZs to be hosted on common hardware. We believe all ESZs on a given SCI should share the same impact, trust, or security levels.	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
Andy Crooks - SaskPower - 1,3,5,6,9 - MRO	
Answer	Yes
Document Name	
Comment	
We agree with the specific addition of exemption 4.2.3.3 and CIP-005 requirement R1 part 1.3, provided the ESZ concerns posed in **Question 3** are addressed. We agree with EEI comments that undefined “systems and components” is unclear. If the objective is to create a parallel term to mirror the concept of an ESP to define a virtualized environment, the definition can be simplified to “A logically isolated section of a network containing one or more VCAs.” From a security perspective we do not believe it is wise to allow mixed trust ESZs to be hosted on common hardware. We believe all ESZs on a given SCI should share the same impact, trust, or security levels.	
Likes 0	
Dislikes 0	

Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
We agree with the specific addition of exemption 4.2.3.3 and CIP-005 requirement R1 part 1.3, provided the ESZ concerns posed in **Question 3** are addressed. We agree with EEI comments that undefined “systems and components” is unclear. If the objective is to create a parallel term to mirror the concept of an ESP to define a virtualized environment, the definition can be simplified to “A logically isolated section of a network containing one or more VCAs.” From a security perspective we do not believe it is wise to allow mixed trust ESZs to be hosted on common hardware. We believe all ESZs on a given SCI should share the same impact, trust, or security levels.	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Trevor Tidwell - PNM Resources - Public Service Company of New Mexico - 1,3	
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	
Teresa Cantwell - Lower Colorado River Authority - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aubrey Short - FirstEnergy - FirstEnergy Corporation - 1,3,4, Group Name Aubrey Short, On Behalf of:	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2 - MRO,SERC,RF	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Boody - Lakeland Electric - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Chinedu Ochonogor - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Davis Jelusich - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Public Utility District No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
faranak sarbaz - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Langston - Tallahassee Electric (City of Tallahassee, FL) - 1,3,5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE seeks clarification on why exemptions 4.2.3.2 and 4.2.3.3 exempt “third-party owned Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters or Electronic Security Zone…” • For example, if a registered entity owns a generation Facility but a third party owns Cyber Assets in that Facility and those Cyber Assets have a 15-minute impact and meet the definition of a BCA. The registered entity is responsible for those BCAs. Texas RE agrees protecting confidentiality and integrity of the data traversing communication networks and data communication links used to extend an applicable ESP or ESZ is very important and should be implemented. Logical isolation and segmenting should be implemented properly so large IP subnets are not used. Texas RE suggests the terms “Super-ESP” and “geographic location” may not be the best terms. The reasoning for CIP-005-7 includes BES Cyber System Logical Isolation. However, the SDT is allowing “Super-ESP” concepts that could include large IP ranges. Segmenting the network properly includes smaller IP ranges and logical isolation which improves access control, monitoring, performance, and containment. In addition, Texas RE recommends defining geographic location and possibly including a threshold.	
Likes 0	
Dislikes 0	
Response	
Neil Swearingen - Salt River Project - 1,3,5,6 - WECC	
Answer	
Document Name	
Comment	
Not Applicable to the High Impact Control Centers.	
Likes 0	
Dislikes 0	

Response

7. The SDT is proposing to retire EACMS and develop two new terms: EACS and EAMS. These terms will allow changes within the applicable systems column of the relevant requirements to allow third party monitoring. Monitoring and logging data will be handled within CIP-011 in a future posting. Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification. NOTE: Project 2016-02 will coordinate with Project 2019-02 (BCSI) and Project 2019-03 (Supply Chain) on this topic. (CIP-005 Technical Rationale pages 9, 10, 13, and 19).

Bruce Reimer - Manitoba Hydro - 1,3,5,6

Answer	No
Document Name	

Comment

Given that the CIP compliance program works fairly smoothly by implementing the existing requirements with all applicable system, it may not be necessary for splitting the EACMS and PACS into two separate devices from an ongoing compliance workload perspective. In addition, monitoring device cannot be treated the same level since some of them more critical than others. We suggest initiating a survey before making a decision for splitting.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no NGrid and Eversource

Answer	No
Document Name	

Comment

We recommend keeping the EACMS term while adding the new EACS and EAMS term

EACS (External Access Control System) & EAMS (External Access Monitoring System) – we request keeping the old term / definition / applicability EACMS in addition to these two new terms / definitions / applicability. We suggest that the Entity has the flexibility to use any of these three terms / definitions / applicability to avoid forcing Entities in to costly, large changes to their documentation and training, etc.

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer	No
Document Name	

Comment

While it is appreciated the cost savings that could occur as a result of third party monitoring, there is no assurance that the data or even the EAMS will be protected properly.

Likes 0	
Dislikes 0	

Response

Quintin Lee - Eversource Energy - 1,3

Answer	No
Document Name	

Comment

Eversource recommends modifying the EACMS term while adding the new EACS and EAMS terms.

We recommend modifying the existing EACMS to:

‘Cyber Assets that perform electronic access control **and** electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems.’

The Entity would be able to use these three terms as needed since some devices are used for both control and monitoring whereas some devices are only used for control or monitoring. This would avoid forcing Entities to changes to their documentation and training, etc just for a glossary term change which improves the backwards compatibility effort.

Likes 0	
Dislikes 0	

Response

Michael Puscas - ISO New England, Inc. - 2

Answer	No
Document Name	

Comment

While ISO-NE agrees that the current definitions associated with BES Cyber Systems do not adequately account for virtualization, ISO-NE cautions that adding new terms and definitions continues to foster an object of requirement approach instead of moving towards an information security objective based approach.

It is difficult to ascertain whether the definitions are adequate and determine the impact of the new definition without seeing the revisions in the other standards/requirements, specifically CIP-007 and CIP-010.

To achieve the backwards compatibility, all existing terms must remain in place. In addition, introducing the concept that assets can be have multiple classifications can have profound influence on processes and tools already implemented.

Likes 0	
Dislikes 0	
Response	
Jennifer Wright - Sempra - San Diego Gas and Electric - 1,3,5	
Answer	No
Document Name	
Comment	
SDG&E requests not retiring EACMS. There may still be instances where a single asset will be categorized as both controlling and monitoring. Keeping EACMS would allow flexibility in defining the asset as one term. Alternatively, allow for dual classification as an EACS and EAMS.	
Likes 0	
Dislikes 0	
Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5	
Answer	No
Document Name	
Comment	
Yes, we generally agree with the concept. However, we will need to see what the changes to CIP-011 look like. In particular, R2 will need to be clear on the expectations for “disposal” of a VM. Is just deleting a VM sufficient? How does an entity prove actions were taken to prevent the unauthorized retrieval of BCSI, if we’re not decommissioning the physical asset/hard disks? Will this be covered in the CIP-011 posting?	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Network and Security Technologies - 1 - NA - Not Applicable	
Answer	No
Document Name	
Comment	
N&ST disagrees with the proposal to break out monitoring functions from the existing EACMS and PACS definitions in order to serve the goal of easily accommodating third-party, possibly cloud-based, electronic and/or physical access monitoring. We strongly disagree with the rationale that “access	

monitoring" is somehow less critical, and poses less inherent risk, than "access control," particularly in light of the fact the 2016 SANS / E-ISAC analysis of the attack on Ukrainian power grid cited a lack of monitoring as a key factor in the attack's success.	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
We would like to see clarification that Cyber Assets designated as EACS are exclusively EACS and not also subject to requirements applicable to EAMS if the EACS also performs monitoring, given the understanding that EACS are more critical and will require greater security than EAMS.	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 3,4	
Answer	Yes
Document Name	
Comment	
Given the source definition, the inclusion of the term "monitor" in the Physical Access Monitoring System (PAMS) definition could be interpreted as an expansion of the scope of the existing definition and, as a result, applicable requirements. Specifically, the term "monitor" is not found/is not explicit within the current definition of Physical Access Control System (PACS). To remain consistent with the objective of merely separating the existing definition(s) without impacting scope, GSOC/OPC recommends adhering more closely to the existing verbiage when separating the current term and definition into PACS and PAMS. To achieve this, GSOC/OPC recommends referring to the language in the Technical Rationale document when finalizing this language. Additionally, GSOC/OPC would suggest greater consistency between the definitions for PAMS/PACS and Electronic Access Control System (EACS)/Electronic Access Monitoring System (EAMS). Currently, the definitions differ significantly despite the systems performing substantially the same functions/tasks. To rectify this and ensure consistency, GSOC/OPC recommends the following revisions to EACS and EAMS: **EACS: Cyber Assets or Virtual Cyber Assets that control electronic access to a BES Cyber Asset, Electronic Access Control System, Electronic Access Monitoring System, Physical Access Control System, or Physical Access Monitoring System.** **EAMS: Cyber Assets or Virtual Cyber Assets that monitor electronic access to a BES Cyber Asset, Electronic Access Control System, Electronic Access Monitoring System, Physical Access Control System, or Physical Access Monitoring System.**	
Likes 0	

Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
None.	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Please clarify with regard to the use of system tools such as AV patch management.	
Likes 0	
Dislikes 0	
Response	
Jenifer Holmes - Alliant Energy Corporation Services, Inc. - 4 - MRO,RF	
Answer	Yes
Document Name	
Comment	
Alliant supports MRO NSRF's comments.	
Likes 0	
Dislikes 0	
Response	

Clay Walker - Cleco Corporation - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
See EEI Comments.	
Likes 0	
Dislikes 0	
Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
We would like to see clarification that Cyber Assets designated as EACS are exclusively EACS and not also subject to requirements applicable to EAMS if the EACS also performs monitoring, given the understanding that EACS are more critical and will require greater security than EAMS.	
Likes 0	
Dislikes 0	
Response	
Andy Crooks - SaskPower - 1,3,5,6,9 - MRO	
Answer	Yes
Document Name	
Comment	
We would like to see clarification that Cyber Assets designated as EACS are exclusively EACS and not also subject to requirements applicable to EAMS if the EACS also performs monitoring, given the understanding that EACS are more critical and will require greater security than EAMS.	
Likes 0	
Dislikes 0	
Response	

Kent Feliks - AEP - 3,5	
Answer	Yes
Document Name	
Comment	
AEP supports the changes proposed by the SDT.	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
We would like to see clarification that Cyber Assets designated as EACS are exclusively EACS and not also subject to requirements applicable to EAMS if the EACS also performs monitoring, given the understanding that EACS are more critical and will require greater security than EAMS.	
Likes 0	
Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1,3,5	
Answer	Yes

Document Name	
Comment	
The proposed retirement and development of the two new terms provides additional capability at the Entity level. However, the remaining CIP Standards needs to be revised to reflect the new terms within the Applicable Systems. There should be considerations for all CIP standards impacted by virtualization be updated concurrently to ensure efforts to make the necessary modifications to existing architecture by the entity.	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
The Exelon companies agree with the comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
City Light understands and supports the change, in support of new monitoring technologies and services, but is not convinced that the EAMS term is necessary. Please consider if sufficient protection could be provided simply by defining the contents of proposed EAMS as BCSI and addressing risk that way, and/or if an EAMS is really just another type of PCA or VCA? See also response to Question 1, above.	
Likes 0	
Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	

Answer	Yes
Document Name	
Comment	
We agree with the retirement of the term EACMS and the creation of the two new terms, EACS and EAMS. In the interim, until all associated EACMS requirements can be updated, we believe it would be beneficial for the SDT (or another SDT) to move forward with approving the new EACS and EAMS definition but wait to retire the “EACMS” definition. We believe that all three terms could be active, and the requirements could be applied based on the applicable systems. As the requirements are updated, the SDT(s) could move away from utilizing EACMS and have EACS and/or EAMS as applicable systems instead. The ongoing delay in making the definition changes continue to have an impact on other CIP SDTs, particularly the 2018-02 CIP-008 Incident Reporting, 2019-03 CIP-013 Supply Chain, and 2019-02 BES Cyber System Information Access Management teams. Each of those teams would have benefited (or will benefit) from the updated definitions. Furthermore, the 2016-02 team would not need to continue to re-visit new or modified standards-- thus lessening the team’s burden of changes.	
Likes 0	
Dislikes 0	
Response	
James Brown - California ISO - 2 - WECC	
Answer	Yes
Document Name	
Comment	
CAISO has no additional comments regarding this question.	
Likes 0	
Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,5,6 - SERC, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy agrees with the retirement of EACMS and the development of new terms EACS and EAMS as long as it is optional and backward compatible to the current CIP-005 requirement.	
Likes 0	
Dislikes 0	

Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - MRO, Group Name Westar-KCPL	
Answer	Yes
Document Name	
Comment	
Westar / Kansas City Power & Light support Edison Electric Institute’s (EEI) response to Question 7.	
Likes 0	
Dislikes 0	
Response	
Patricia Boody - Lakeland Electric - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
While we agree with the new terminology, this will require most entities to make modifications to their entire CIP program, processes, databases, GRC tools and evidence artifacts.	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI support's the SDT's proposal.	
Likes 0	
Dislikes 0	
Response	

Michael Johnson - Pacific Gas and Electric Company - 1,3,5 - WECC

Answer	Yes
Document Name	

Comment

PG&E agrees the retirement of Electronic Access Control or Monitoring Systems (EACMS) and replacement with Electronic Access Control System (EACS) and Electronic Access Monitoring Systems (EAMS) will achieve the stated goal of applying the appropriate security controls based on risk to the Bulk Electric System (BES) and allow for the use of monitoring and alerting capabilities from third-party service providers.

Request - PG&E is requesting input from the SDT on the ability of the separated EACS and EAMS to receive updates (i.e. signatures, patterns) either from PG&E-established sources or PG&E-identified trusted supplier sources using either “push” or “pull” methods. PG&E’s current understanding is receiving EAMCS updates directly from a trusted supplier source is not allowed, and would like to know if the proposed EACS/EAMS separation will allow for this update method as other Standard modifications (i.e. CIP-007) are being considered.

Likes 0	
Dislikes 0	

Response

Greg Davis - Georgia Transmission Corporation - 1

Answer	Yes
Document Name	

Comment

The inclusion of the term “monitor” in the PAMS definition could be interpreted as an expansion of the existing definition and associated requirements as such term is not explicit within the definition for source term associated with physical access control and monitoring (PACS). GTC recommends adhering more closely to the existing verbiage when separating the current term and definition into PACS and PAMS, and in referring to the language in the Technical Rationale document when finalizing this language.

GTC would suggest greater consistency between the definitions for PAMS/PACS and EACS/EAMS. Currently, the definitions differ significantly despite the systems performing substantially the same functions/tasks. To rectify this and ensure consistency, GTC recommends the following revisions to EACS and EAMS:

EACS: Cyber Assets or Virtual Cyber Assets that control electronic access to a BES Cyber Asset, Electronic Access Control System, Electronic Access Monitoring System, Physical Access Control System, or Physical Access Monitoring System.

EAMS: Cyber Assets or Virtual Cyber Assets that monitor electronic access to a BES Cyber Asset, Electronic Access Control System, Electronic Access Monitoring System, Physical Access Control System, or Physical Access Monitoring System.

Likes 0	

Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Trevor Tidwell - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Langston - Tallahassee Electric (City of Tallahassee, FL) - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
faranak sarbaz - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Davis Jelusich - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Public Utility District No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Chinedu Ochonogor - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Neil Swearingen - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2 - MRO,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

David Jendras - Ameren - Ameren Services - 1,3,6

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Aubrey Short - FirstEnergy - FirstEnergy Corporation - 1,3,4, Group Name Aubrey Short, On Behalf of:

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	
Document Name	

Comment

Texas RE is not opposed to modifying the CIP requirements to facilitate registered entities using third party monitoring services. Texas RE recognizes that third parties may be able to provide services that some registered entities do not have the skillset or staffing to perform themselves, such as 24-hour security monitoring or alerting.

Texas RE is concerned, however, that bifurcating the current term, EACMS, into the two new terms, EACS and EAMS, will allow for carve outs of one or the other which will reduce the security obligations of monitoring systems owned, operated, and maintained by registered entities. For example, a monitoring system (proposed EAMS), such as a SIEM, typically contains a large amount of the information an attacker will need to plan their attack so it should be protected by the CIP standards. The proposed bifurcation would allow an entity to carve out SIEMs. A monitoring system, such as a SIEM, would also contain the logs a registered entity would need to perform a forensics analysis of the attack. As such, it would also be a likely target in an attack on the electric grid.

If the SDT feels that registered entities are unable to make use of third party monitoring services that would improve the security and reliability of the Bulk Electric System due to the current definition of EACMS then Texas RE recommends that the SDT consider submitting a SAR to draft a new standard that covers the acceptable use of third party services.

This new standard could be modeled after CIP-013. Whereas CIP-013's purpose is to mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems this new standard's purpose could be to mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for third party management of security services provided to registered entities. This standard would codify the requirements around how registered entities can securely make use of third party monitoring services.

As part of this project, Texas RE would then recommend modifying the definition of EACMS to specify that EACMS are owned by registered entities. This modification to the definition would then unambiguously exclude third party entities from being required to comply with the other CIP standards.

Likes 0	
Dislikes 0	
Response	

8. The V5TAG document request the SDT to “Clarify the IRA definition to address the placement of the phrase “using a routable protocol” in the definition and clarity with respect to Dial-up Connectivity.” Therefore, the SDT proposes modifications to the IRA definition and CIP-005 Requirement R2. These modifications will clarify scenarios where Interactive Remote Access applies to serial only devices. Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification. (CIP-005 Technical Rationale pages 7, 19-21, 27, and 33-37).

Jenifer Holmes - Alliant Energy Corporation Services, Inc. - 4 - MRO,RF	
Answer	No
Document Name	
Comment	
Alliant supports MRO NSRF's comments.	
Likes 0	
Dislikes 0	
Response	
Trevor Tidwell - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	No
Document Name	
Comment	
See comment #10 regarding R2.1	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No
Document Name	
Comment	
Remote access client has no location specified. A user could use a remote access client locally. This does not address system-to-system similar to CIP-013, and is inconsistent with CIP-013 in regards to system-to-system vs IRA.	
Likes 0	

Dislikes 0

Response

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

Answer	No
Document Name	

Comment

With respect to Interactive Remote Access, ERCOT requests clarification as to whether the definition should be limited to only solutions using a remote access client. This appears to be very narrow and may exclude future technologies. The IRA definition and Requirement R2 do not appear to have been updated to specifically address dial-up. The removal of specifics can be misleading, especially where an entity might not consider dial-up capability to align with “remote access client.”

Likes 0

Dislikes 0

Response

Bruce Reimer - Manitoba Hydro - 1,3,5,6

Answer	No
Document Name	

Comment

We disagree with the IRA modifications since the current IRA definition has already covered the serial only devices and devices outside of ESP, but just CIP-005 R2 has not addressed that yet except CIP-004 R5.1. In the current IRA definition: “User-initiated access by a person employing a remote access client or other remote access technology using a routable protocol…”, the IRA definition only states the user-initiated access using a routable protocol and doesn’t say all communication sessions need to be routable. Also it doesn’t say the Cyber Asset that is accessible by a remote client has to be within ESP. For instance, when a device serially connected to a terminal server and it can be accessible by a remote client, it meets IRA definition, but current CIP-005-5 R2 doesn’t apply since R2 only apply to the cyber asset within ESP. However, for CIP-004 R5.1, it requires to revoke IRA access to High and medium impact BCS and associated EACMS and PACS, it implies EACMS or PACS may have IRA access even though they are not within an ESP. Given that current IRA definition has covered the serial only devices and devices outside of ESP, we only need to modify the applicable systems in CIP-005 R2 to address these devices. We suggest changing the applicable systems in CIP-005 R2 without changing the requirements as follows:

“High Impact BES Cyber Systems and their associated EACM, PACS and PCA

Medium Impact BES Cyber Systems and their associated EACM, PACS and PCA”

Likes 0

Dislikes 0

Response

Teresa Cantwell - Lower Colorado River Authority - 1,5	
Answer	No
Document Name	
Comment	
The proposed language does not provide clarity to serial only devices as they (serial or dial-up) is not called out in R2.	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	
We agree with EEI's comments on the IRA definition in Question 1. The clarity requested by the SAR can be provided by changing the phrase to "using a routable or dial-up protocol." We ask the SDT to respect the scope of the SAR, and propose that if the SDT desires to clarify scenarios where IRA includes serially connected devices and security controls for these devices, this would be more appropriately handled by a future SAR requesting authorization to do so.	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Network and Security Technologies - 1 - NA - Not Applicable	
Answer	No
Document Name	
Comment	
N&ST believes the proposed modification of "IRA" has been watered down to the point where it basically defines "Interactive Remote Access" as remote access that's interactive. While we concur with removing as much "requirements-like" language from Glossary definitions, we believe the revised definition should retain the information that "IRA" is access to a BES Cyber System or associated applicable system and that it is initiated from outside the ESP or ESZ where the system being accessed is located.	
Likes 0	
Dislikes 0	

Response

Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5

Answer	No
Document Name	CIP 005_Q8 Diagram.pdf

Comment

Tri-State does not agree. The removal of the ERC characteristic from the definition of IRA will bring into scope several types of serial communications links that should not be defined as having IRA.

Several examples include:

- The RTU owned by entity “A” has ERC and IRA. There is also a serial communications link between the RTU owned by entity “A” and an RTU owned by entity “B” inside the substation control house. Under the new IRA definition the RTU owned by entity “B” has an IRA link from entity “A”.
- The RTU in a substation control house has a serial communications link to the control center. At the control center the serial communications link is connected to the SCADA network. Under the new IRA definition this RTU has IRA.
- The RTU owned by entity “A” inside a substation control house with a serial communications to a control center owned by entity “B”. At the control center owned by entity “B”, the serial communications link is converted to routable protocol and connected to the SCADA network. Under the new IRA definition this RTU owned by entity “A” has IRA to the SCADA network owned by entity “B”.
- An RTU in a substation control house with IRA has a serial link to a cyber asset in the substation yard. Under the new IRA definition the cyber asset in the control house yard has IRA.

We believe the risk is at the initial point where Ethernet and serial merge. Current requirements require authentication which mitigate the risk. This change to IRA does not provide additional protection but does significantly increase scope. By increasing scope we divert limited resources that would be better used at higher risk areas.

In addition, IRA for serial communications may bring into scope the IP-to-Serial connections from an EMS (front-end processor) application server down to the RTU at a substation. One could argue that an EMS user has IRA to the RTU from the EMS front-end processor server. This communication should be excluded from the IRA definition and this situation needs to be addressed by the SDT. See the uploaded diagram for further details:

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 1,3,6

Answer	No
Document Name	

Comment

As written, the definition of IRA can apply to an RDP connection from one asset inside of an ESP to another asset inside of the same ESP since a User is initiating access and employing a remote access client. This would render R2.1 impossible to follow for a majority of RDP connections in a given system. We propose that the language about the connection not originating from a IS, within an ESP or at an access point should remain to clarify that point.	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2 - MRO,SERC,RF	
Answer	No
Document Name	
Comment	
Interactive Remote Access: Request clarification of whether the definition should be limited to only solutions using a remote access client. This appears to be very narrow and may exclude future technologies. The IRA definition and Requirement R2 does not appear to have been updated to specifically address dial-up. The removal of specifics can be misleading, especially where an entity may not consider dial-up capability to align with “remote access client."	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
See EEI’s response to Question 1 above.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - MRO, Group Name Westar-KCPL	
Answer	No
Document Name	

Comment	
Westar / Kansas City Power & Light support Edison Electric Institute’s (EEI) response to Question 8.	
Likes 0	
Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,5,6 - SERC, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
Duke Energy does not generally agree with the modifications to the IRA defintion and CIP-005 Requirement R2. The definition removes "using routable protocol" and incorporates IP to serial conversion scenarios or serial only scenarios. Since serial connections can now be treated as IRA, this may cause a burden on the business units who support serial connected devices.	
Likes 0	
Dislikes 0	
Response	
Jennifer Wright - Sempra - San Diego Gas and Electric - 1,3,5	
Answer	No
Document Name	
Comment	
SDG&E supports EEI’s comments submitted on our behalf.	
Likes 0	
Dislikes 0	
Response	
Michael Puscas - ISO New England, Inc. - 2	
Answer	No
Document Name	
Comment	

The new definition is ambiguous and opens up a broad discussion of what a remote access client is. The new definition does not provide clarity. In addition, the definition is not backwards compatible.	
Likes 0	
Dislikes 0	
Response	
James Brown - California ISO - 2 - WECC	
Answer	No
Document Name	
Comment	
Regarding the Interactive Remote Access definition: Request clarification of whether the definition should be limited to only solutions using a remote access client. This appears to be very narrow and may exclude future technologies. The IRA definition and Requirement R2 does not appear to have been updated to specifically address dial-up. The removal of specifics can be misleading, especially where the entity might not consider dial-up capability to align with “remote access client.”	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1,3,5,6	
Answer	No
Document Name	
Comment	
The Exelon companies agree with the comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Chinedu Ochonogor - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	No
Document Name	
Comment	

AZPS believes this scenario may lead to the determination that serial assets utilizing a session termination gateway may be incorrectly subject to requirements intended for ERC assets. This will lead to unnecessary effort in conforming to standards that have no additional security benefit, e.g. CIP007-6 R1.1.	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
We agree with EEI’s comments on the IRA definition in Question 1. The clarity requested by the SAR can be provided by changing the phrase to “using a routable or dial-up protocol.” We ask the SDT to respect the scope of the SAR, and propose that if the SDT desires to clarify scenarios where IRA includes serially connected devices and security controls for these devices, this would be more appropriately handled by a future SAR requesting authorization to do so.	
Likes 0	
Dislikes 0	
Response	
Kent Feliks - AEP - 3,5	
Answer	No
Document Name	
Comment	
Please see AEP’s response to Question #1	
Likes 0	
Dislikes 0	
Response	
Andy Crooks - SaskPower - 1,3,5,6,9 - MRO	
Answer	No

Document Name	
Comment	
We agree with EEI’s comments on the IRA definition in Question 1. The clarity requested by the SAR can be provided by simply changing the phrase to “using a routable or dial-up protocol.” We ask the SDT to respect the scope of the SAR, and propose that if the SDT desires to clarify scenarios where IRA includes serially connected devices and security controls for these devices, this would be more appropriately handled by a future SAR requesting authorization to do so.	
Likes 0	
Dislikes 0	
Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	
We agree with EEI’s comments on the IRA definition in Question 1. The clarity requested by the SAR can be provided by simply changing the phrase to “using a routable or dial-up protocol.” We ask the SDT to respect the scope of the SAR, and propose that if the SDT desires to clarify scenarios where IRA includes serially connected devices and security controls for these devices, this would be more appropriately handled by a future SAR requesting authorization to do so.	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	No
Document Name	
Comment	
Oncor supports EEI's comment.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	

Answer	No
Document Name	
Comment	
Interactive Remote Access: Request clarification of whether the definition should be limited to only solutions using a remote access client. This appears to be very narrow and may exclude future technologies. The IRA definition and Requirement R2 does not appear to have been updated to specifically address dial-up. The removal of specifics can be misleading, especially where entity might not consider dial-up capability to align with “remote access client.”	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern requests the SDT take steps to ensure that the scope of IRA is clear and doesn’t bring in cyber assets not currently covered under this definition. For example, today the IRA definition implies remote access “into an ESP”, yet EACMS and PACS are not required to be in an ESP today. By virtualizing EACS or PACS, does this create IRA to those asset types if they are required to be in an ESZ? Is all “remote” access into an ESZ going to be considered IRA going forward for virtualized EACS and PACS, even if those assets aren’t on the same SCI as a h/m BES Cyber System? Or if they are ONLY hosted on SCI with other EACS or PACS, respectively? These types of questions appear to be questions and confusion as to the intended applicability of requirements to specific virtualized systems that the SDT should help clarify in subsequent rounds of commenting/balloting.	
Likes 0	
Dislikes 0	
Response	

Andrea Barclay - Georgia System Operations Corporation - 3,4	
Answer	Yes
Document Name	
Comment	
GSOC/OPC provides the following comments for the SDT’s review and consideration: • To ensure that the definitions remain neutral to a particular implementation method, GSOC/OPC recommends that the SDT revise the definition of Interactive Remote Access to include “or other remote access technology.” • GSOC/OPC is concerned about the expansion of definitions to address serial to IP connectivity without the inclusion of proposed implementation timelines/timeframes.	
Likes 0	
Dislikes 0	
Response	
Greg Davis - Georgia Transmission Corporation - 1	
Answer	Yes
Document Name	
Comment	
· To ensure that the definitions remain neutral to a particular implementation method, GTC recommends that the SDT revise the definition of Interactive Remote Access to include “or other remote access technology.” · GTC is concerned about the expansion of definitions to address serial to IP connectivity without the inclusion of proposed implementation timelines/timeframes.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Pacific Gas and Electric Company - 1,3,5 - WECC	
Answer	Yes
Document Name	
Comment	

PG&E agrees the proposed modifications correctly address the risks of Interactive Remote Access (IRA) using connection methods other than “a routable protocol” which is absent from the current CIP-005-5 and -6 Standards. IRA access using Dial-up, serial, or IP-to-Serial connection methods have the same risk as those employing a routable protocol.

Likes 0	
Dislikes 0	

Response

Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC

Answer	Yes
Document Name	

Comment

City Light recognizes the request to address “routable protocol” and “Dial-up Connectivity” but does not agree that this revision is the time and place to do so. The proposed changes to “routable protocol” and “Dial-up Connectivity” may have significant impact to entities, and no justification has been provided about whatever is the security concern driving the proposed changes. These changes also are likely to be lost in all the other changes aimed at accommodating virtualization. For these reasons, City Light strongly urges that all changes regarding “routable protocol” and “Dial-up Connectivity” be struck from this revision and proposed separately. They are worthy of attention on their own, not as part of this even larger, and largely different, effort.

It could be as simple as preparing for comments (and perhaps ballot) a separate proposed version of CIP-005, that includes only the proposed changes to “routable protocol” and “Dial-up Connectivity,” without any of proposed virtualization changes.

Such a change may also promote acceptance of the changes proposed in support of virtualization, by removing any chance for ***NO*** *ballots based on concern about these unconnected changes.*

Likes 0	
Dislikes 0	

Response

Gladys DeLaO - CPS Energy - 1,3,5

Answer	Yes
Document Name	

Comment

Recommend the SDT provide clarification to the IRA definition as it creates confusion and does not appear to address Dial-Up Connectivity. Will Entities be provided a phased in consideration for existing architecture and the implantation guidelines be reflective of the phased in approach?

Likes 0	
Dislikes 0	

Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Cleco Corporation - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
See EEI Comments.	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1,3,5,6	
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	
Aubrey Short - FirstEnergy - FirstEnergy Corporation - 1,3,4, Group Name Aubrey Short, On Behalf of:	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Boody - Lakeland Electric - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Davis Jelusich - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Public Utility District No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
faranak sarbaz - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Scott Langston - Tallahassee Electric (City of Tallahassee, FL) - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Neil Swearingen - Salt River Project - 1,3,5,6 - WECC	
Answer	
Document Name	
Comment	
Not Applicable to the High Impact Control Centers.	
Likes 0	
Dislikes 0	
Response	

9. The SDT is proposing modifications to CIP-005 Requirement R1. Do you agree with these changes? Please provide comments to support your response. (CIP-005 Technical Rational pages 22-32).

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	
We cannot agree until the concerns posed in Questions 1 thru 8 are addressed.	
Likes 0	
Dislikes 0	
Response	
Bruce Reimer - Manitoba Hydro - 1,3,5,6	
Answer	No
Document Name	
Comment	
We disagree with modifications to CIP-005 R1 (See our comments in question 1 & 3). · For R1.1, if SDT still wants network layer protection for EACMS and PACS, we suggest changing the CIP-005 R1.1 applicable systems to include EACMS and PACS. · For R1.2, if STD intends to allow inbound and outbound access control either at network perimeter level or local device level, the applicable system should be changed as follows: o Electronic Security Perimeter o High Impact BES Cyber Systems and their associated EACM, PACS and PCA o Medium Impact BES Cyber Systems and their associated EACM, PACS and PCA	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	

Comment	
ERCOT offers the following items for consideration: Part 1.1 Measure: An example of evidence may include, but is not limited to, a list of all ESPs or ESZs with all uniquely identifiable applicable systems. Add in “Cyber Assets connected via a routable protocol within each ESP or Cyber Assets and virtual Cyber Assets contained within the ESZ.” Part 1.2: Regarding the exclusion of time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE), this needs to be clarified to address situations where communication is coming into a BCS from a remote location. It appears that some sort of “rule” would be required for this communication. Part 1.3: Break the exclusion away from the requirement to add emphasis. See 1.2. Part 1.6 Measure: Enforcing authentication looks to be a new requirement created within a measure. The requirement and measure do not align.	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	
Please see Southern’s response to previous questions.	
Likes 0	
Dislikes 0	
Response	
Trevor Tidwell - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	No
Document Name	
Comment	

For R1.1 we disagree with PACS and EACS hosted on SCI being in scope. A PACS or EACS that is virtualized is not at any higher risk than the physical counterpart that does not have a requirement to have communications to and from controlled. As stated in comment #4 if the concern is PACS or EACS hosted on SCI that also hosts HIBCS or MIBCS then they are covered by definition as an associated PCA. Per comment #3 we believe ESP can be retired and thus the requirement language could drop ESP.

For R1.2 we agree with the premise. Again, ESP could probably be dropped from Applicable Systems.

The structure of R1.1 and R1.2 punish entities that have defense in depth with a larger perimeter and then host-based or zone firewalls deployed. Under the proposed requirement if an ESZ within another ESP or ESZ was not properly configured with access permissions yet the larger perimeter or zone was then it is still a violation. The standard needs to be objective based of requiring logical access permissions to HIBCS, MIBCS, and associated PCAs. In the defense in depth model if at least one of the perimeter or zones are configured correctly then the objective is accomplished. Under the proposed CIP requirement if one is but another isn’t then it is a violation when in fact there was no risk to the Bulk Electric System. Supporting the defense in depth model encourages entities to deploy zones within zones to reduce compliance risk and increase security. Not supporting the defense in depth model will create a driver for entities to reduce compliance risk by having only one zone. While compliance risk has been accomplished the security of the Bulk Electric System suffers because of single point of failure encouraged by the compliance risk. Proposed R1.2 is still prescriptive not objective based. A way to address the issue could be to have R1.2 have the Applicable Systems of HIBCS, MIBCS and associated PCA and SCI. The requirement would be “At least one ESP or ESZ protecting the Applicable System, require inbound or outbound logical access permissions, including the reason for granting access, and deny all other logical access by default. The access permissions can exclude time-sensitive protection or control functions….” This would allow entities to have defense in depth but only need to prove that at least one of the layers had protections in place.

We agree with the premise of R1.3. This is a gap in CIP-012.

We disagree with the applicable systems in R1.4. If physical PACS and EACS do not have Dial-Up Connectivity requirements then why do the virtualized PACS and EACS have such requirements. Again as stated before PACS or EACS sharing the same SCI as HIBCS or MIBCS are also by definition PCAs.

For R1.5 we agree with the requirement but disagree with the Applicable Systems. This should have the same Applicable Systems as proposed R1.2 for conformity purposes.

For R1.6 it is unclear what risk the SDT is trying to address. Why are management systems of SCI hosting HIBCS or MIBCS only called out. A physical BCA could have a baseboard management controller. Is there a reason its management system doesn’t have similar restrictions? Management systems do not exist only on virtual infrastructure. Also as mentioned before it is unclear what the SDT means by management systems. We strongly urge the SDT to make this a defined term. For example SCADA is typically managed from within the same GUI operators use and cannot be separated. More clarification is needed for this requirement.

Likes 0	
Dislikes 0	

Response

Jenifer Holmes - Alliant Energy Corporation Services, Inc. - 4 - MRO,RF	
Answer	No
Document Name	
Comment	
Alliant supports MRO NSRF's comments.	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF	
Answer	No
Document Name	
Comment	
All CIP standards impacted by virtualization should be updated concurrently. The efforts for the entities to adopt these changes would be significant.	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	
Reclamation recommends if replacing Electronic Security Perimeter with Logical Isolation, this term should be added to the NERC Glossary of Terms. Logical Isolation is not a NERC defined term and has not been added as a new definition within this standard revision proposal.	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Cleco Corporation - 1,3,5,6 - SERC	

Answer	No
Document Name	
Comment	
See EEI Comments.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	
SWG offers the following items for consideration. • Part 1.1 Measure: An example of evidence may include, but is not limited to, a list of all ESPs or ESZs with all uniquely identifiable applicable systems. Add in "Cyber Assets connected via a routable protocol within each ESP or Cyber Assets and virtual Cyber Assets contained within the ESZ." • Part 1.2: Regarding the exclusion of time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE), this needs to be clarified to address situations where communication is coming into a BCS from a remote location. It appears that some sort of "rule" would be required for this communication. • Part 1.3: Break the exclusion away from the requirement to add emphasis. Look at 1.2. • Part 1.6 Measure: Enforcing authentication looks to be a new requirement created within a measure. The requirement and measure do not align.	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	No
Document Name	
Comment	
Oncor supports EEI's comment.	
Likes 0	
Dislikes 0	

Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	
We cannot agree until the concerns posed in Questions 1 thru 8 are addressed.	
Likes 0	
Dislikes 0	
Response	
Andy Crooks - SaskPower - 1,3,5,6,9 - MRO	
Answer	No
Document Name	
Comment	
We cannot agree until the concerns posed in Questions 1 thru 8 are addressed.	
Likes 0	
Dislikes 0	
Response	
Kent Feliks - AEP - 3,5	
Answer	No
Document Name	
Comment	
Please see AEP’s response to Question #1	
Likes 0	
Dislikes 0	
Response	

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

Answer	No
Document Name	

Comment

Revise Requirement R1, Part 1.1 to, “All applicable systems shall reside within one or more, or on the logical perimeter of defined ESPs or ESZs.”

Likes 0

Dislikes 0

Response

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

Internet Protocol (IP) is not the only risk that should be addressed. While it is the dominant routable protocol in modern use, multiple other routable protocols exist (for example, IPX, Appletalk, etc.), as well as “layer 2” non-routable protocols that nonetheless provide a capability for conveying malicious code and infiltrating exploitable data.

Also, the R1 table title needs to be updated, from ESP to Logical Isolation.

Likes 0

Dislikes 0

Response

Davis Jelusich - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Public Utility District No. 1 of Chelan County

Answer	No
Document Name	

Comment

CHPD cannot agree with the changes to R1 at this time. With the current wording, it is difficult to realize implementation and successful compliance of the proposed changes without additional clarification of the new terminology and its application to other standards. Additionally, CHPD believes that the current definition for Shared Cyber Infrastructure discourages the use of virtualization for BES Cyber 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 RSC no NGrid and Eversource	
Answer	No
Document Name	
Comment	
Part R1.2 – request clarification. There seems to be a gap between R1.2's logical access permission and data diodes; because data diodes do not use/need logical access permission. How can an Entity pass an audit while using data diodes? Part 1.2 and 1.3 – we request removing the IEC 61850 language from the Requirement since that other non-NERC Standard could change on its own. We suggest moving these exemptions into this Standards Exemptions Section (4.2.3) Part R1.4 – the new Requirement remove the need for a mitigation plan. The Entity only needs to provide evidence the system is not capable. While we agree with intent of removing TFEs, we suggest these new words are less secure Part 1.6 – request clarification. We believe the Requirement wants to say that the Intermediate Systems and the BES Cyber Systems must be on different virtual machine hosts.	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
We cannot agree until the concerns posed in Questions 1 thru 8 are addressed.	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	

The addition of "routable Internet Protocol (IP) communications" to eliminate storage transport protocols, does not take into account that there are known attacks on these protocols that could impact the systems utilizing these storage protocols.	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1,3,5,6	
Answer	No
Document Name	
Comment	
The Exelon companies agree with the comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1,3	
Answer	No
Document Name	
Comment	
See Eversource response to Question 1.	
Likes 0	
Dislikes 0	
Response	
James Brown - California ISO - 2 - WECC	
Answer	No
Document Name	
Comment	
CAISO offers the following items for consideration;	

- Part 1.1 Measure: An example of evidence may include, but is not limited to, a list of all ESPs or ESZs with all uniquely identifiable applicable systems. Add in “Cyber Assets connected via a routable protocol within each ESP or Cyber Assets and virtual Cyber Assets contained within the ESZ.”
- Part 1.2: Regarding the exclusion of time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE), this needs to be clarified to address situations where communication is coming into a BCS from a remote location. It appears that some sort of “rule” would be required for this communication.
- Part 1.3: Break the exclusion away from the requirement to add emphasis. Look at 1.2.
- Part 1.6 Measure: Enforcing authentication looks to be a new requirement created within a measure. The requirement and measure do not align.

Likes 0	
Dislikes 0	

Response

Michael Puscas - ISO New England, Inc. - 2

Answer	No
Document Name	

Comment

R1 is potentially duplicative of CIP-006 R1.10. A review should be performed to ensure that there is no overlap and that the requirement is necessary.

For Part 1.1: The language under “Measures” currently states “[a]n example of evidence may include, but is not limited to, a list of all ESPs or ESZs with all uniquely identifiable applicable systems.” The following should be added: “Cyber Assets connected via a routable protocol within each ESP or Cyber Assets and virtual Cyber Assets connected within the ESZ.”

For Parts 1.2 and 1.3: Excluding communications using protocol IEC TR-61850-90-5 R-GOOSE is inappropriate. Perhaps use the capability of the system in this instance.

For Part 1.3: Including the CIP-012 exclusion within the requirement language overly complicates the requirement. Exclusions should be listed in the Exemptions section. CIP-012 is written without the applicability section and this requirement is asset based.

For Parts 1.1, 1.4, and 1.5: It’s confusing to have protections applied to virtualized assets but not applied to the physical assets with the same classification (i.e. PACS hosted on SCI, EACS hosted on SCI, PACS, & EACS).

For Part 1.6: The language under “Measures” includes enforcing authentication, but that is not in the requirement. Thus, “authentication” should be deleted from the measure. Also, the term “management plane” comes up in the requirement statement itself, but it is only defined in the Technical Rationale. Please consider adding either a definition of “management plane” or include specification of management and data planes as part of the SCI definition to support compliance with CIP-005-7 R1.6. At a minimum, each should be defined if they are gong be part of the requirement. This could be accomplished by adding something like the following to the SCI definition: “This includes its management systems that support configuration of policy for sharing of CPU, memory, and storage. This also includes the management plane that supports carrying instructions and status for sharing of CPU, memory, and storage.”

Likes 0	
Dislikes 0	

Response	
Jennifer Wright - Sempra - San Diego Gas and Electric - 1,3,5	
Answer	No
Document Name	
Comment	
SDG&E supports EEI’s comments submitted on our behalf.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - MRO, Group Name Westar-KCPL	
Answer	No
Document Name	
Comment	
Westar / Kansas City Power & Light support Edison Electric Institute’s (EEI) response to Question 9.	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
See EEI’s response to Question 1 above.	
Likes 0	
Dislikes 0	
Response	

Bobbi Welch - Midcontinent ISO, Inc. - 2 - MRO,SERC,RF

Answer	No
Document Name	

Comment

MISO offers the following items for consideration.

Part 1.1 Measure: An example of evidence may include, but is not limited to, a list of all ESPs or ESZs with all uniquely identifiable applicable systems. Add in “Cyber Assets connected via a routable protocol within each ESP or Cyber Assets and virtual Cyber Assets contained within the ESZ.”

Part 1.2: Regarding the exclusion of time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE), this needs to be clarified to address situations where communication is coming into a BCS from a remote location. It appears that some sort of “rule” would be required for this communication.

Part 1.3: Break the exclusion away from the requirement to add emphasis. Look at 1.2.

Part 1.6 Measure: Enforcing authentication looks to be a new requirement created within a measure. The requirement and measure do not align.

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 1,3,6

Answer	No
Document Name	

Comment

According to how we interpret the new R1.1, any PAC or EAC that is virtualized will have to be placed inside of an ESP or ESZ, but the physical PACs and EACs do not have that same requirement. We believe that this creates a discrepancy in protection requirements between virtual and physical PCs. We propose that if SCI devices host BCAs or PCAs then the SDT should clarify this in the definition. Currently it applies to SCI that host VCAs inside and outside the ESP.

Likes 0	
Dislikes 0	

Response

Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5

Answer	No
Document Name	

Comment

No, Tri-State does not agree with CIP-005-7 R1.6.

Regarding 1.6 we would like more clear definitions to better understand the description of management systems, management plane, and data plane. Would like examples.

As stated in the measures of CIP-005-7 R1.6, a hypervisor could be the management system, which would essentially share CPU, Memory, Disk and network resources with the hosting VMs if there is no traditional “management system.” In some cases, the hosting platform is a multi-purpose operating system such as Windows or Linux. The same argument could be applied to the containers.

Likes 0	
Dislikes 0	

Response

Greg Davis - Georgia Transmission Corporation - 1

Answer	No
Document Name	

Comment

GTC provides the following comments for the SDT’s review and consideration:

· In the Measures column for R1.1, GTC recommends capitalizing “applicable system” for consistency with previous column and other sections within the standard.

· In the Measures column for R1.2, the “each access rule” revision could be interpreted as an expansion of responsibilities. Where more than 1 rule is grouped together to form the access policy to be effected, the revised requirement could be interpreted to require a “reason” be assigned to each line in a grouping as opposed to the overall rule for the access policy resulting from the grouping. To ensure that the reliability standards present the “what,” and not the “how,” GTC recommends that the SDT review this language closely and clarify the intent. An example clarification is provided below for the SDT’s consideration:

An example of evidence may include, but is not limited to, architectural diagrams that detail how network communication is limited and a list of rules (firewall, access control lists, software defined policies, etc.) that demonstrate that only permitted access is allowed and that each access rule or policy (as applicable) has a documented reason

· Relative to R1.3, the language in the requirement too closely mirrors the language in the exception, which could result in ambiguity between what is excluded and what is included in applicability. GTC recommends that the SDT consider clarification.

Likes 0	
Dislikes 0	

Response

Roger Fradenburgh - Network and Security Technologies - 1 - NA - Not Applicable

Answer	No
Document Name	
Comment	

N&ST notes the proposed wording in Part 1.1 opens the possibility of defining a BCS that comprises BCAs in different ESPs or ESZs. We believe the SDT needs to better articulate the benefits of allowing this and should also address what the Technical Rationale document refers to as the risk of “side channel” attacks.

N&ST also notes that making virtualized EACS devices subject to R1 Part 1.1 would preclude using one to provide access control for a conventional, IP-based ESP.

Likes 0	
Dislikes 0	
Response	

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

Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Andrea Barclay - Georgia System Operations Corporation - 3,4

Answer	Yes
Document Name	
Comment	

GSOC/OPC provides the following comments for the SDT’s review and consideration:

- In the Measures column for R1.1, GSOC/OPC recommends capitalizing “applicable system” for consistency with previous column and other sections within the standard.

- In the Measures column for R1.2, the “each access rule” revision could be interpreted as an expansion of responsibilities. Where more than 1 rule is grouped together to form the access policy to be effected, the revised requirement could be interpreted to require a “reason” be assigned to each line in a grouping as opposed to the overall access policy resulting from the grouping. To ensure that the reliability standards present the “what,” and not the “how,” GSOC/OPC recommends that the SDT review this language closely and clarify the intent. An example clarification is provided below for the SDT’s consideration:

An example of evidence may include, but is not limited to, architectural diagrams that detail how network communication is limited and a list of rules (firewall, access control lists, software defined policies, etc.) that demonstrate that only permitted access is allowed and that each access rule **or policy (as applicable)** has a documented reason

- Relative to R1.3, the language in the requirement too closely mirrors the language in the exception, which could result in ambiguity between what is excluded and what is included in applicability. GSOC/OPC recommends that the SDT consider clarification.

Likes 0	
Dislikes 0	

Response

Gladys DeLaO - CPS Energy - 1,3,5

Answer	Yes
Document Name	

Comment

1. Existing implementations that have mixed trust may require work to align trust levels once the new requirement goes live. Will Entities be provided a phased in consideration for existing architecture and the implantation guidelines be reflective of the phased in approach?

2. The requirement reads as if the isolation model can be only ESP or ESZ. Is it possible to implement a blended model, assuming all requirements are met for both implementations, or is it exclusive? It can be envisioned where both would come in to play for certain migration scenarios.   Is it possible that a Cyber Asset may appear in two or more ESZ, assuming identical trust level, or is a Cyber Asset restricted to only one ESZ?

There should be considerations for all CIP standards impacted by virtualization be updated concurrently to ensure efforts to make the necessary modifications to existing architecture by the entity.

Likes 0	
Dislikes 0	

Response

Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC

Answer	Yes
Document Name	

Comment

City Light generally supports the proposed R1 modifications, with the exceptions discussed above under Questions 2-7, and the overarching concerns discussed in Questions 1 and 13

Likes 0	
Dislikes 0	

Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	Yes
Document Name	
Comment	
While we understand the need to identify an Electronic Access Point is no longer the only model for addressing network access control with the proposed updates, if a firewall performs the "logical isolation of an ESZ or ESP", we are not sure how it can also reside within the defined ESP. Part 1.1 requires, if we understand the definition of Shared Cyber Infrastructure correctly (to include existing firewall that are associated with an EAP), that those firewalls (considered SCIs) must "reside within one or more defined ESPs or ESZs." Additionally, for Part 1.6, since Shared Cyber Infrastructure includes existing firewalls, it would be helpful to define or expand on what "that hosts BES Cyber Systems" means for those already existing firewalls (non-virtual). As tedious as it might sound, adding words such as "that hosts", without explicitly expressing what the intent of the word is, causes issues with the entities and the regions. It would be prudent to get away from terms can be construed in different ways or that can change the execution of the requirement depending on how they are interpreted.	
Likes 0	
Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,5,6 - SERC, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy generally agrees with the modifications to CIP-005 Requirement R1.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Pacific Gas and Electric Company - 1,3,5 - WECC	
Answer	Yes
Document Name	
Comment	

PG&E agrees with the modifications and change in approach to “logical isolation” since it would apply to the current implementation of CIP-005 (backward compatibility) and the proposed modifications to clearly allow for the use of virtual technology.	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5	
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	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Scott Langston - Tallahassee Electric (City of Tallahassee, FL) - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
faranak sarbaz - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chinedu Ochonogor - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Neil Swearingen - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Boody - Lakeland Electric - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aubrey Short - FirstEnergy - FirstEnergy Corporation - 1,3,4, Group Name Aubrey Short, On Behalf of:	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	

Part 1.1 - Texas RE noticed R1.1 is not a requirement to create ESPs or ESZs. Part 1.1 requires that entities place their applicable systems within a defined ESP or ESZ. The creation of the ESP or ESZ is an inferred requirement. Texas RE recommends there be a specific requirement for entities to create and/or define ESPs and/or ESZs. Texas RE recommends the language to be modified to "Define/Create and implement ESPs or ESZs for all applicable systems". Additionally, Texas RE suggests PACS and EACS not hosted on SCI should be included in this requirement.

Part 1.2 – If the drafting team chooses not to modify Part 1.1 to explicitly require the creation of ESPs and ESZs, Texas RE recommends modifying Part 1.2 to the following. Texas RE proposes that the applicable systems in R1.2 be defined as:

Electronic Security Perimeters and Electronic Security Zones in which one or more of the following reside:

High Impact BES Cyber Systems and their associated:

PCA

SCI

PACS hosted on SCI

EACS hosted on SCI

Medium Impact BES Cyber Systems connected to a network via routable protocol and their associated:

PCA

SCI

PACS hosted on SCI

EACS hosted on SCI

Part 1.4 – Texas RE recommends PACS and EACS not hosted on SCI also be included in this requirement since they are just as important for security as PACS and EACS hosted on SCI.

Part 1.5 states "Have one or more methods for detecting known or suspected malicious routable Internet Protocol (IP) communications to or from ESPs or ESZs." Texas RE disagrees that detection of malicious communications is restricted to routable IP communications. Most modern IPS and IPS sensors inspect Layer 2 (non-routable) and Layer 3 (routable) traffic, and include deep packet inspection. There are layer 2 attacks such as MAC address flooding, DHCP server spoofing, Man-in-the-middle attacks, and IP host spoofing that should be monitored. Texas RE recommends the language to be modified to "Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications to or from ESPs or ESZs.

The Technical Rationale on page 28 states "The use of the phrase "routable Internet Protocol (IP) communications" is intended to eliminate internal storage transport protocols including, but not limited to Fibre Channel, iSCSI, and InfiniBand from the scope of this requirement as well as serial communications." However, Fibre Channel and iSCSI can both operate at layer 3 of the OSI Model using routable protocol (TCP/IP).

Part 1.5 – Texas RE recommends PACS and EACS not hosted on SCI also be included in this requirement since they are just as important for security as PACS and EACS hosted on SCI.

Part 1.6 states “Management systems may only share CPU, memory, or ESZ or ESP with other management systems and the management plane.” On page 11 of the Technical Rationale there is the statement: “This inclusion is intended to ensure that devices that provide logical isolation for an ESZ or ESP, and therefore have an associated risk, have protection for the **associated management systems (management plane)** as required by Part 1.6.” Texas RE seeks clarification on the use of the words “management systems” and “management plane”. The SDT may consider defining these term(s) to improve clarity and reduce ambiguity.

Likes 0	
Dislikes 0	

Response

10. The SDT is proposing modifications to CIP-005 Requirement R2. Do you agree with these changes? Please provide comments to support your response. (CIP-005 Technical Rationale pages 33-37).

Jenifer Holmes - Alliant Energy Corporation Services, Inc. - 4 - MRO,RF

Answer	No
Document Name	

Comment

Alliant supports MRO NSRF's comments.

Likes 0	
Dislikes 0	

Response

Trevor Tidwell - PNM Resources - Public Service Company of New Mexico - 1,3

Answer	No
Document Name	

Comment

First some entities have over declared ESPs (those without any BCS) so remote access from those ESPs do not have to traverse an Intermediate System. The language change to R2 main would affect these entities.

For R2.1 we agree with the addition of SCI to the applicable systems. However there a a couple of problems. The first is regarding IRA itself. The new IRA definition is “User-initiated access by a person employing a remote access client.” The requirement is to ensure IRA (per R2 main originating outside the ESP or ESZ) is through an Intermediate System. Does this mean TCAs are no longer allowed? A TCA can be outside the ESP or ESZ if it is a stand-alone device cabled to a BCA, or associated PCA or SCI. The TCA could employee software the allows access to the BCA or associated PCA or SCI. This could be considered Interactive Remote Access as the TCA employed a remote access client. Consider having an exclusion in R2 main of “for all remote access that originates from outside of any of the entities’ ESP’s or ESZ’s containing high or medium impact BES Cyber Systems or associated SCI *excluding directly connected TCAs*.”

The other problem is with MIBCS. The webinar mentioned the change was to include those MIBCS that were serial but elsewhere in the communication path had a serial to IP conversion. Some technicians use test sets or other devices to troubleshoot the communication to RTUs, HMIs, and data concentrators. Typically this is done on site. It is unclear with the proposed definition how this troubleshooting tool could still be used in a compliant manner. The access is user-initiated using a client tool and it isn’t within the ESP or ESZ and it isn’t through an Intermediate System. Typically, this work is done on the SCADA port using a SCADA protocol (i.e. DNP 3.0, Modbus, Series V, Conitel). These ports are typically restricted to just the SCADA protocol and do not provide remote access to actually reconfigure the device. This may be a problem with the current standard but it is more evident in the proposed standard. A suggestion would to be revise the proposed IRA definition to clarity what the remote access client can access or modify like the configuration of the device.

We agree with proposed R2.2 and R2.3.

For R2.4 and R2.5, again we disagree with PACS and EACS hosted on SCI being included in Applicable Systems. As stated, before PACS or EACS sharing the same SCI as HIBCS or MIBCS are also by definition PCAs. The purpose of CIP-005 is “To protect BES Cyber Systems against compromise by allowing only known and controlled communication to and from the system and logically isolating all other communication.” The purpose does not include a statement about protecting communication to PACS and EACS hosted on SCI. Again, if the PACS and EACS do not share SCI with a HIBCS or MIBCS then what is the concern. If there is a concern, then both physical and virtual need to be protected. Otherwise it is already address as those PACS and EACS that share SCI with HIBCS or MIBCS are also by definition PCAs.

We disagree with R2.6. This is beyond the stated purpose of CIP-005. “To protect BES Cyber Systems against compromise by allowing only known and controlled communication to and from the system and logically isolating all other communication.” The purpose is not to protect IS from compromise such as side channel attacks which the rationale indicates this requirement addresses. Why are only IS called out to prevent side channel attacks? Why are EACS and PACS hosted on SCI not also called out? The risks identified on page 37 of the rationale are not any that impact a BCS or even the BES itself, but only the Intermediate System. Thus, it should not be a Bulk Electric System Reliability Standard.   Also, it is unclear how an IS can even be within an ESZ or ESP.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

While Southern supports the recommendations made by the V5TAG to include dial-up connectivity whenever such connectivity is used for Interactive Remote Access, the use of the proposed new terms ESZ and SCI need to be clarified and modified as discussed in our response to previous questions.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

ERCOT offers the following items for consideration:

R2: The leading requirement could be clearer. ERCOT suggests the SDT consider “Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts in *CIP-005-7 Table R2 –Remote Access Management,* per system capability.” The remaining language should be addressed in the applicability or requirement language in the table.

Part 2.1: Consider “User-initiated access by a person employing a remote access client.” Revision of the definition may be necessary to address non-traditional remote access methods that people might not recognize. The requirement does not specify what you accessing with IRA.

Part 2.2: The lack of a definition for confidentiality and integrity could lead to inconsistency of interpretation and implementation. ERCOT suggests the SDT consider adding more clarity to the requirement language.

Part 2.4: Should this include all EACS and PACS to align to the FERC direction of future supply chain modifications?

Part 2.5: Should this include all EACS and PACS to align to the FERC direction of future supply chain modifications?

Part 2.6: ERCOT requests the SDT clarify why storage was not included in the requirement scope. It appears that an Intermediate System can now be in the same ESP or ESZ as the BES Cyber Systems they are protecting. Is this intentional?

Likes 0	
Dislikes 0	

Response

Bruce Reimer - Manitoba Hydro - 1,3,5,6

Answer	No
Document Name	

Comment

We disagree with modifications to CIP-005 R2 (See our comments in question 8).

Likes 0	
Dislikes 0	

Response

Teresa Cantwell - Lower Colorado River Authority - 1,5	
Answer	No
Document Name	
Comment	
The current term of “encryption” provides confidentiality and integrity. Calling these out separately could cause challenges to demonstrate compliance.	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 3,4	
Answer	No
Document Name	
Comment	
GSOC/OPC is concerned that the use of “remote access client” in the definition for Interactive Remote Access may unnecessarily limit the use of available remote access technologies. To ensure that the requirement focusses on the “what” and not the “how,” GSOC/OPC recommends the addition of “or other remote access technology to the current use of “remote access client.” Similarly, GSOC/OPC is concerned that in R2.2, the use of the term “the client” may also be unnecessarily limiting or technology-specific. Accordingly, GSOC/OPC recommends that SDT revise R2.2 and suggests the following example language: Protect the confidentiality and integrity of Interactive Remote Access between the **remote access client or technology** and the Intermediate System.	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	
We cannot agree until the concerns posed in Questions 1 thru 8 are addressed.	
Likes 0	
Dislikes 0	

Response

Greg Davis - Georgia Transmission Corporation - 1

Answer	No
Document Name	

Comment

GTC is concerned that the use of “remote access client” in the definition for Interactive Remote Access may unnecessarily limit the use of available remote access technologies. To ensure that the requirement focusses on the “what” and not the “how,” GTC recommends the addition of “or other remote access technology to the current use of “remote access client.” Similarly, GTC is concerned that in R2.2, the use of the term “the client” may also be unnecessarily limiting or technology-specific. Accordingly, GTC recommends that SDT revise R2.2 and suggests the following example language:

Protect the confidentiality and integrity of Interactive Remote Access between the remote access client or technology and the Intermediate System.

Likes 0	
Dislikes 0	

Response

Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5

Answer	No
Document Name	

Comment

Tri-State does not agree. R2 includes wording for “all remote access” and we believe it should not be all-inclusive. R2 should be only applicable to routable communication.

Additionally, we have the same disagreement to these changes as our response to question #2. Regarding Intermediate Systems in R2.6, the standard needs to allow for situations where a traditional “management system” is not used.

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 1,3,6

Answer	No
Document Name	

Comment

As written, R2.1 requires SCI access to go through an IS. Since SCI includes firewalls, you would be required to limit access to the firewall to an IS only. Technically, firewalls are the measure most would use to limit down the access. Due to a firewall's location on the perimeter of the ESP, it is not easy to limit what devices have access to it without adding a secondary device in front of it.

Likes 0	
Dislikes 0	

Response

Bobbi Welch - Midcontinent ISO, Inc. - 2 - MRO,SERC,RF

Answer	No
Document Name	

Comment

MISO offers the following items for consideration.

R2: Clarify the leading requirement. Proposed language: “Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts in *CIP-005-7 Table R2 –Remote Access Management,* per system capability.” The remaining language should be addressed in the applicability or requirement language in the table.

Part 2.1: Consider “User-initiated access by a person employing a remote access client.” May need to work the definition to address non-traditional remote access methods that people might not recognize. The requirement does not specify what you accessing with IRA.

Part 2.2: Lack of definition of confidentiality and integrity could lead to inconsistency of interpretation and implementation. Consider adding more clarity to the requirement language.

Part 2.4: Should this include all EACS and PACS to align to the FERC direction of future supply chain modifications?

Part 2.5: Should this include all EACS and PACS to align to the FERC direction of future supply chain modifications?

Part 2.6: Please clarify why storage was not included in the requirement scope. In reading this, it appears that an Intermediate System can now be in the same ESP or ESZ as the BES Cyber Systems they are protecting. Is this intentional? In addition, significant architectural work may be required by some entities to comply with this.

Likes 0	
Dislikes 0	

Response

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

Answer	No

Document Name	
Comment	
While EEI supports the recommendations made by the V5TAG to include dial-up connectivity whenever such connectivity is used for Interactive Remote Access, the use of the proposed new terms ESZ and SCI need to be clarified as discussed in our response to Question 1.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - MRO, Group Name Westar-KCPL	
Answer	No
Document Name	
Comment	
Westar / Kansas City Power & Light support Edison Electric Institute’s (EEI) response to Question 10.	
Likes 0	
Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,5,6 - SERC, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
Duke Energy does not generally agree with the modifications to CIP-005 Requirement R2. CIP-005/Part 2.1 - Per definition of Interactive Remote Access, if the user is employing a remote access client even though the individual is initiating the request from within an ESP, it is considered IRA and needs to go through Intermediate Systems. This creates extra burden on the entities. CIP-005/Part 2.3 - This requirement requires multi-factor authentication to Intermediate System. This may be reaching outside of the CIP scope (for example, the situation where an individual is simply accessing the intermediate system without needing to access BES Cyber Asset or Virtual Cyber Assets).	
Likes 0	
Dislikes 0	
Response	

Jennifer Wright - Sempra - San Diego Gas and Electric - 1,3,5

Answer	No
Document Name	

Comment

SDG&E supports EEI’s comments submitted on our behalf.

Likes 0	
Dislikes 0	

Response

Michael Puscas - ISO New England, Inc. - 2

Answer	No
Document Name	

Comment

For Parts 2.1, 2.4, and 2.5: All of the requirements should have the same applicable systems; in addition, the acronyms used within the requirements should be spelled out.

For Part 2.6: Part 2.6 is incompatible with consolidation efforts as it requires separate SCI for IS. This prescribes technology without providing protective value. Part 2.6 should be removed to allow consolidation of IS with other classification on an SCI.

Likes 0	
Dislikes 0	

Response

James Brown - California ISO - 2 - WECC

Answer	No
Document Name	

Comment

CAISO offers the following items for consideration;

- R2: The leading requirement could use revision to be clearer. Consider, “Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts in *CIP-005-7 Table R2 –Remote Access Management,* per system capability.” The remaining language should be addressed in the applicability or requirement language in the table.
- Part 2.1: Consider “User-initiated access by a person employing a remote access client.” May need to work the definition to address non-traditional remote access methods that people might not recognize. The requirement does not specify what you’re accessing with IRA.

- Part 2.2: Lack of definition of confidentiality and integrity could lead to inconsistency of interpretation and implementation. Consider adding more clarity to the requirement language.
- Part 2.4: Should this include all EACS and PACS to align to the FERC direction of future supply chain modifications?
- Part 2.5: Should this include all EACS and PACS to align to the FERC direction of future supply chain modifications?
- Part 2.6: Please clarify why storage was not included in the requirement scope. In reading this, it appears that an Intermediate System can now be in the same ESP or ESZ as the BES Cyber Systems they are protecting. Is this intentional? In addition, significant architectural work may be required by some entities to comply with this.

Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1,3	
Answer	No
Document Name	
Comment	
While Eversource supports the recommendations made by the V5TAG to include dial-up connectivity whenever such connectivity is used for Interactive Remote Access, we do not support the use of the proposed new terms ESZ and SCI as discussed in our response to Question 1.	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1,3,5,6	
Answer	No
Document Name	
Comment	
The Exelon companies agree with the comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
We cannot agree until the concerns posed in Questions 1 thru 8 are addressed.	
Likes 0	
Dislikes 0	
Response	
Davis Jelusich - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Public Utility District No. 1 of Chelan County	
Answer	No
Document Name	
Comment	
CHPD agrees with the changes proposed for R2.1, R2.2, R2.3, R2.4, and R2.5. CHPD does not agree with the inclusion of language in R2.6. The proposed R2.6 language to require CPU and memory to be shared only with other VCA Intermediate Systems discourages virtualization of Intermediate Systems. CHPD recommends removing “may only share CPU, memory” from the requirement language, but agrees that dedicating an ESZ/ESP to Intermediate Systems is appropriate.	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
There is little risk difference between “Interactive” remote access and “System-to-System” remote access. In either case, strong methods of authentication, integrity, and non-repudiation controls are highly advisable. The concept of a real-time “live hack” popularized by movie “hackers” is generally a fallacy while in reality it requires highly coordinated scripting activities that leverage compromised trusted systems to execute exploits that are pre-staged by the threat actor. The benefit of the doubt that current CIP standards extend to supposedly trusted system-to-system communications is misplaced.	
Likes 0	
Dislikes 0	

Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	No
Document Name	
Comment	
There is inconsistency between Requirement, R2 Part 2.1 and Requirement, R2 Part 2.6. Requirement R2, Part 2.1 is to, “Ensure that Interactive Remote Access is through an Intermediate System that is not inside an applicable ESP or ESZ” and R2 Part 2.6 requirement is, “IS may only share CPU, memory, or ESZ or ESP with other IS”. So, an Intermediate System must be outside an ESP or ESZ, per Requirement, R2.1, therefore, Requirement, R2.6 should be revised as follows: “Intermediate Systems can only share CPU and memory with other Intermediate Systems”.	
Likes 0	
Dislikes 0	
Response	
Kent Feliks - AEP - 3,5	
Answer	No
Document Name	
Comment	
AEP is unable to agree with the proposed modifications to CIP-005 R2 at this time due to the need for clarity around some of the new proposed terms. Please see AEP’s response to Question #1.	
Likes 0	
Dislikes 0	
Response	
Andy Crooks - SaskPower - 1,3,5,6,9 - MRO	
Answer	No
Document Name	
Comment	
We cannot agree until the concerns posed in Questions 1 thru 8 are addressed.	
Likes 0	
Dislikes 0	

Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	
We cannot agree until the concerns posed in Questions 1 thru 8 are addressed.	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	No
Document Name	
Comment	
Oncor supports EEI's comment.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	
SWG offers the following items for consideration. • R2: The leading requirement could use revision to be clearer. Consider, “Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts in *CIP-005-7 Table R2 –Remote Access Management,* per system capability.” The remaining language should be addressed in the applicability or requirement language in the table. • Part 2.1: Consider “User-initiated access by a person employing a remote access client.” May need to work the definition to address non-traditional remote access methods that people might not recognize. The requirement does not specify what you accessing with IRA. • Part 2.2: Lack of definition of confidentiality and integrity could lead to inconsistency of interpretation and implementation. Consider adding more clarity to the requirement language.	

- Part 2.4: Should this include all EACS and PACS to align to the FERC direction of future supply chain modifications?
- Part 2.5: Should this include all EACS and PACS to align to the FERC direction of future supply chain modifications?
- Part 2.6: Please clarify why storage was not included in the requirement scope. In reading this, it appears that an Intermediate System can now be in the same ESP or ESZ as the BES Cyber Systems they are protecting. Is this intentional? In addition, significant architectural work may be required by some entities to comply with this.

Likes 0

Dislikes 0

Response

Clay Walker - Cleco Corporation - 1,3,5,6 - SERC

Answer	No
Document Name	

Comment

See EEI Comments.

Likes 0

Dislikes 0

Response

Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF

Answer	No
Document Name	

Comment

All CIP standards impacted by virtualization should be updated concurrently. The efforts for the entities to adopt these changes would be significant.

Likes 0

Dislikes 0

Response

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

Answer	No
Document Name	

Comment

Likes 0	
Dislikes 0	
Response	
Michael Johnson - Pacific Gas and Electric Company - 1,3,5 - WECC	
Answer	Yes
Document Name	
Comment	
PG&E agrees with the modifications on the removal of the prescriptive language in Part 2.2, making it more objective-based, and the enhanced security due to the Interactive Remote Access definition modifications which would now cover serial and dial-up connectivity.	
Likes 0	
Dislikes 0	
Response	
Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
City Light generally supports the proposed R2 modifications, with the exception of scope change as discussed above under Question 8, and the overarching concerns discussed in Questions 1 and 13.	
Likes 0	
Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1,3,5	
Answer	Yes
Document Name	
Comment	
There should be considerations for all CIP standards impacted by virtualization be updated concurrently to ensure efforts to make the necessary modifications to existing architecture by the entity.	

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no NGrid and Eversource

Answer	Yes
Document Name	

Comment

R2 – the new Requirement remove the need for a mitigation plan. The Entity only needs to provide evidence the system is not capable. While we agree with intent of removing TFEs, we suggest these new words are less secure.

Part 2.1 – request clarification. How are TCAs covered?

Part 2.3 – for improved comprehension, we suggest that Part 2.3 borrow these words from Part 2.2 – “between the client and the Intermediate System”

Part 2.6 – request clarification. We believe the Requirement wants to say that the Intermediate Systems and the BES Cyber Systems must be on different virtual machine hosts.

Likes 0	
Dislikes 0	

Response

Jesus Sammy Alcaraz - Imperial Irrigation District - 1,3,5,6

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Roger Fradenburgh - Network and Security Technologies - 1 - NA - Not Applicable

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aubrey Short - FirstEnergy - FirstEnergy Corporation - 1,3,4, Group Name Aubrey Short, On Behalf of:	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Boody - Lakeland Electric - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Neil Swearingen - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chinedu Ochonogor - APS - Arizona Public Service Co. - 1,3,5,6	
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, Group Name ACES Standard Collaborations	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
faranak sarbaz - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Langston - Tallahassee Electric (City of Tallahassee, FL) - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	

Comment

Part 2.1 - The proposed language in R1.1 states “All applicable systems shall reside within one or more defined ESPs or ESZs.

The applicable systems are listed as:

High Impact BES Cyber Systems and their associated:

PCA

SCI

PACS hosted on SCI

EACS hosted on SCI

And

Medium Impact BES Cyber Systems connected to a network via routable protocol and their associated:

PCA

SCI

PACS hosted on SCI

EACS hosted on SCI

Texas RE agrees with the language of this requirement. The requirement, however, is potentially problematic when combined with the language in R2.1 which states “Ensure that Interactive Remote Access is through an Intermediate System that is not inside an applicable ESP or ESZ.” Some entities choose to host their Intermediate Systems on Virtual Cyber Assets. An Intermediate System will meet the definition of EACS. For those Intermediate Systems that are virtualized they will meet the definition of EACS hosted on SCI. R1.1 requires that EACS hosted on SCI reside within one or more defined ESPs or ESZs. R2.1 requires that an IS used for IRA is not inside an applicable ESP or ESZ. At best, this is a clarity issue where it is not immediately obvious that the ESP or ESZ the Intermediate System is residing within is not an “applicable” ESP or ESZ. At worst, this causes a scenario where the only acceptable Intermediate System is one that is not virtualized. Texas RE does not believe this is the SDT's intent.

To address this, Texas RE proposes that the verbiage “that is not inside an applicable ESP or ESZ” be removed from R2.1. R2.1 would then read as “Ensure that Interactive Remote Access is through an Intermediate System.” The proposed language in R2.6, “IS may only share CPU, memory, or ESZ or ESP with other IS.”, would ensure the intention behind “that is not inside an applicable ESP or ESZ” in R2.1 is still being met.

Part 2.2 - The addition of “confidentiality and integrity” is an improvement over using just the word “encryption”. Encryption may provide confidentially but not integrity. For example, encryption with digital signatures would provide both. Texas RE recommends the language to be modified to “*For all*

Interactive Remote Access sessions, protect the confidentiality and integrity by utilizing encryption that terminates at an Intermediate System” or similar language.

The Technical Rationale states the following in regards to R2.2: the language “Protect the confidentiality and integrity of Interactive Remote Access between the client and the Intermediate System” prevents outdated encryption methods from being utilized. Texas RE disagrees that this requirement language prevents the use of outdated encryption methods. Outdated encryption methods provide more than zero protection and therefore would meet the language in this requirement.

Alternatively, if the language in this requirement is determined to allow the CEAs the judgement on whether or not a specific encryption technology is “good enough” this can lead to inconsistent enforcement across the regions.

Texas RE proposes that the SDT define a new term, Strong Encryption Standard. Strong Encryption Standard would be defined as “An Encryption Standard with a security strength of 112 bits or higher.” 112 bits was chosen as that is the minimum encryption strength permitted under NIST SP 800-175B, Section 3.4. As NIST deprecates weaker key strengths the expectation is the SDT would update the definition of Strong Encryption Standard to match the minimum strength recommended by NIST.

In addition to this new term, a new requirement would be drafted, similar in nature to CIP-007-6 R3.3.

R# - For the protections implemented in Part 2.2 that use encryption, use a Strong Encryption Standard.

This language would balance prescription with flexibility. CEAs would have a bright-line criteria to determine whether or not an encryption algorithm is acceptable to use, but at the same time registered entities would have the flexibility of choosing the encryption standard that is best for their environment. Texas RE recognizes that not all encryption algorithms are of equal strength, and some encryption algorithms may be insecure despite meeting the required 112 bit security strength. Texas RE would not be opposed to the SDT modifying the proposed definition of Strong Encryption Standard to include or reference a blacklist of encryption algorithms that are not acceptable to be used, but this may be overly burdensome for the amount of benefit it provides.

Part 2.3 – While it does not object to the proposed language in Part 2.3, Texas RE notes that the proposed language in R2.3 may have unintended consequences that drive a certain architecture type. A number of entities use multiple systems in order to comply with this requirement. For example, an entity may normally be blocked from remotely accessing their Intermediate System. The entity logs into a separate system using multi-factor authentication and they are now allowed to remotely access the Intermediate System.

Under that architecture, if the separate system is unavailable, the entity can still make use of the Intermediate System by physically accessing the Intermediate System and remotely accessing their applicable BCS (this is possible because the current IRA definition excludes remote access that originates from an Intermediate System).

Under the proposed language in R2 and R2.3 entities would be required to use multi-factor authentication when directly accessing the Intermediate System if they intend to use the Intermediate System to remotely access an applicable system from R2.1. This provides an overall improvement to security, but does introduce compliance risk if the Intermediate System is needed when MFA is unavailable.

Part 2.6 - Texas RE notes that the existing definition of ESP “The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol.” and the proposed verbiage in requirement R2.6 “IS may only share CPU, memory, or ESZ or ESP with other IS” means that it is not possible for an Intermediate System to be located within an ESP. An Intermediate System is an EACS. If the “ESP” is only allowed to be populated with other EACS then the network will not contain any BCS. If the “ESP” does not contain any BCS then the “ESP” does not actually meet the definition of ESP. If the SDT intends to allow Intermediate Systems to be located within ESPs then the definition of ESP or the verbiage in R2.6 will need to be modified. Texas RE recommends modifying the definition of ESP to no longer include BCS as a scoping mechanism or to explicitly state that Intermediate Systems must be located within an ESZ. As Intermediate Systems are currently forbidden from being located within an ESP, explicitly requiring the Intermediate System to be located within a defined ESZ will achieve the SDT’s goal while having a minimal impact on registered entities. This, combined with R2.6’s requirement that Intermediate Systems can only share ESZ with other Intermediate Systems would ensure that the Intermediate Systems are both isolated and protected.

Texas RE notes that on page 36 of the Technical Rationale, there are extra bullet points in Parts 2.4 and 2.5, Applicable Systems column.

Likes 0	
Dislikes 0	

Response

11. Backwards Compatibility: What level of effort is required to migrate from existing definitions to new definitions on existing virtualized architecture?	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE does not have comments on this question.	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	
Document Name	
Comment	
The level of effort can be greatly reduced if “or ESP” is removed from the SCI definition and from the Requirements of R1.6. Including ESPs poses a backwards compatibility challenge; see Question 2 response.	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 3,4	
Answer	
Document Name	
Comment	
GSOC/OPC is supportive of making modifications to enable the standards to progress to a more technology agnostic model. To facilitate this transition, an implementation period of at least 24 months is recommended to ensure that these changes related to virtualization can be implemented efficiently and effectively. However, GSOC supports a more rapid pace for the revisions associated with the splitting of the PACS/PAMS and EAMS/EACS definitions as it is currently prohibiting the adoption of controls that would increase the security of BCAs and prompt adoption would foster overall security.	
Likes 0	

Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5	
Answer	
Document Name	
Comment	
Fairly significant as almost every internal process will need modification	
Likes 0	
Dislikes 0	
Response	
Bruce Reimer - Manitoba Hydro - 1,3,5,6	
Answer	
Document Name	
Comment	
We disagree with all new definitions since they all can be covered by the current definitions.	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	
Document Name	
Comment	
None.	
Likes 0	
Dislikes 0	

Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	
Document Name	
Comment	
The level of effort required to accommodate these changes could be significant, but could be lessened by consideration of proposed changes provided in our responses to previous questions.	
Likes 0	
Dislikes 0	
Response	
Trevor Tidwell - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	
Document Name	
Comment	
The effort to the proposed changes without any modification are high because of virtualized PACS and EACS being brought into scope even if they don’t share SCI with HIBCS or MIBCS. The IRA revisions also require more time to determine the impacts as the webinar added a twist with the revelation that the IP to serial conversion was in scope.	
Likes 0	
Dislikes 0	
Response	
Jenifer Holmes - Alliant Energy Corporation Services, Inc. - 4 - MRO,RF	
Answer	
Document Name	
Comment	
Alliant supports MRO NSRF's comments.	
Likes 0	
Dislikes 0	

Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1,3,5,6	
Answer	
Document Name	
Comment	
There will be some effort for our current architecture, since we are already utilizing virtualization. However, the level of effort necessary to develop plans, policies, procedures, and to document their application under revised CIP Standards, would be substantial. Although not as extensive as that required for the CIP v5 transition, utilities seeking to utilize virtualization in their BCS environments will need be prepared for a major effort to revise and validate their suite of CIP compliance policies, procedures, and document.	
Likes 0	
Dislikes 0	
Response	
Scott Langston - Tallahassee Electric (City of Tallahassee, FL) - 1,3,5	
Answer	
Document Name	
Comment	
N/A - no existing virtualized architecture.	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	
Document Name	
Comment	
Each change to a standard creates additional work for an entity to evaluate its processes, revise where appropriate, implement the changes, and retrain employees, which is not cost-effective. The proposed changes to the CIP standards will have significant impacts on entities and will require substantial resources to implement. The proposed changes go beyond simply updating technology and/or documentation; they constitute a culture shift comparable to the CIP v5 transition. Entities must implement processes to achieve an understanding of new terms, buy in to their use, and change the culture to	

employ new terms. Entities must be provided enough time to determine the effects of the revised requirements and definitions, develop adequate processes, and train personnel appropriately to implement quality practices that improve BES reliability.	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	
Document Name	
Comment	
Very little effort to migrate.	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Cleco Corporation - 1,3,5,6 - SERC	
Answer	
Document Name	
Comment	
See EEI Comments.	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	
Document Name	
Comment	
Minimal work will be required for our existing environment to document compliance for the R1.6; however, if we choose to implement virtual firewalls, there will be additional work required to implement the changes and document compliance.	

Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	
Document Name	
Comment	
SWG Comment: New definitions do not pose significant issue. Implementation of CIP-005 may pose issues with entities who must re-architect virtual infrastructure to meet the new verbiage. This is no small task and should be allowed adequate time.	
Likes 0	
Dislikes 0	
Response	
faranak sarbaz - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	
Document Name	
Comment	
Based on preliminary assessment, the level of effort required is moderate. However, additional guidance on implementation and audit approach is needed in order to make a full evaluation.	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	
Document Name	
Comment	
The effort appearss to be substantial; therefore, adequate time should be allowed to adapt a new architecture landscape.	
Likes 0	

Dislikes 0	
Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	
Document Name	
Comment	
The level of effort can be greatly reduced if “or ESP” is removed from the SCI definition and from the Requirements of R1.6. Including ESPs poses a backwards compatibility challenge; see Question 2 response.	
Likes 0	
Dislikes 0	
Response	
Andy Crooks - SaskPower - 1,3,5,6,9 - MRO	
Answer	
Document Name	
Comment	
The level of effort can be greatly reduced if “or ESP” is removed from the SCI definition and from the Requirements of R1.6. Including ESPs poses a backwards compatibility challenge; see Question 2 response.	
Likes 0	
Dislikes 0	
Response	
Kent Feliks - AEP - 3,5	
Answer	
Document Name	
Comment	
AEP is of the opinion that the effort required would be considerably high. It is difficult to say, however, without clarification of the ESZ definition.	
Likes 0	
Dislikes 0	

Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	
Document Name	
Comment	
The level of effort is significant with backwards compatibility even if little or no virtualization is in use, because all processes must be reviewed and updated to accommodate current and future (inevitable) use of virtual systems. CenterPoint Energy analyzed the project just for the High Impact BES Cyber Systems with the assumption of having existing staff (that are already tasked with other duties) dedicate 3 hours per day to the effort. Based upon this assumption and the time estimates for the associated tasks, this project will take two experienced analysts more than two years to complete the work.	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	
Document Name	
Comment	
To the extent an entity leverages new technologies the effort may be high.	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	
Document Name	
Comment	
BPA believes the SDT has done an admirable job of preserving nested capabilities and backwards compatibility. While it will entail significant effort to migrate, it is justifiable effort.	
Likes 0	

Dislikes 0

Response

Davis Jelusich - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Public Utility District No. 1 of Chelan County

Answer

Document Name

Comment

CHPD believes that this language requires a significant amount of effort due to the lack of specific BCA scoping language in the SCI definition. Migrating to this language, as written, would require CHPD to classify additional Cyber Assets that perform no BES functions.

Likes 0

Dislikes 0

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no NGrid and Eversource

Answer

Document Name

Comment

There should be full compatibility that the existing CIP terminology and definitions should be acceptable going forward.

Likes 0

Dislikes 0

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer

Document Name

Comment

The level of effort can be greatly reduced if “or ESP” is removed from the SCI definition and from the Requirements of R1.6. Including ESPs poses a backwards compatibility challenge; see Question 2 response.

Likes 0

Dislikes 0

Response	
Gladys DeLaO - CPS Energy - 1,3,5	
Answer	
Document Name	
Comment	
As we understand the redefinition, little to no effort will be required to maintain the existing paradigm. However, this will require a major effort to rearchitect the interaction between the devices and defining the policies that would supersede the existing ACLs that currently permit or restrict traffic to a policy-based system. Any migration will best be implemented in conjunction with a major system overhaul/refresh. Will Entities be provided a phased in consideration for existing architecture and the implantation guidelines be reflective of the phased in approach?	
Likes 0	
Dislikes 0	
Response	
Chinedu Ochonogor - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	
Document Name	
Comment	
While the changes are intended to allow for backward compatibility for currently implemented technology a significant effort is still needed for process/program updates as well as asset assessment procedures and device classification methods in order to adopt the new definitions. This effort should not be overlooked when pinpointing the implementation timeline for these new changes.	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1,3,5,6	
Answer	
Document Name	
Comment	
The Exelon companies agree with the comments submitted by EEI that while the effort appears to be substantial, the clarification of ESZ may lessen the effort.	

Likes 0	
Dislikes 0	

Response

Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC

Answer	
Document Name	

Comment

City Light considers that the level of effort would be mixed, with minimal to moderate effort on the technical side and extensive effort on the compliance and documentation side.

Minimal effort would be required for existing BES Cyber Systems themselves. There would likely be marginally additional level of effort required for designing and deploying the upgrade of BES Cyber Systems planned for calendar year 2020 and beyond. Beyond that, any additional technical effort brought about by upgrading to a virtualized architecture likely would be negligible.

However, the level of effort necessary to develop plans, policies, procedures, and to document their application under revised CIP Standards, would be substantial. Although not as extensive as that required for the CIP v5 transition, utilities seeking to utilize virtualization in their BCS environments—and that would be almost all of them—will need be prepared for a major effort to revise and validate their suite of CIP compliance policies, procedures, and documents. City Light anticipates that such an effort (for virtualization throughout all applicable CIP Standards) could require about a year of dedicated effort. Significant expense likely also would be incurred for external consultant support.

Likes 0	
Dislikes 0	

Response

Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates

Answer	
Document Name	

Comment

Overall, we believe that migrating from existing definitions to a majority of the new definitions in existing virtualized and non-virtualized environments will require a small amount of effort. However, we do feel that the term “Shared Cyber Infrastructure” and how the requirements are applied to those assets, will require a significant amount of work.

Likes 0	
Dislikes 0	

Response

Quintin Lee - Eversource Energy - 1,3	
Answer	
Document Name	
Comment	
Definitely impactful but not substantial. See Eversource response to Question 7.	
Likes 0	
Dislikes 0	
Response	
Neil Swearingen - Salt River Project - 1,3,5,6 - WECC	
Answer	
Document Name	
Comment	
Based on the current budget/costs/resources for our High Impact Control Centers, the level of effort involved in a developing new processes, design/modification of network architecture, and the research and development needed in order to support new tools - 36 months or more would be needed.	
Likes 0	
Dislikes 0	
Response	
James Brown - California ISO - 2 - WECC	
Answer	
Document Name	
Comment	
New definitions do not pose significant issue. Implementation of CIP-005 may pose issues with entities who must re-architect virtual infrastructure to meet the new verbiage. This is no small task and adequate time should be allowed.	
Likes 0	
Dislikes 0	
Response	

Michael Puscas - ISO New England, Inc. - 2	
Answer	
Document Name	
Comment	
The effort required would be very significant because in several instances there is no backwards compatibility.	
Likes 0	
Dislikes 0	
Response	
Jennifer Wright - Sempra - San Diego Gas and Electric - 1,3,5	
Answer	
Document Name	
Comment	
SDG&E supports EEI’s comments submitted on our behalf.	
Likes 0	
Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,5,6 - SERC, Group Name Duke Energy	
Answer	
Document Name	
Comment	
Duke Energy is currently assessing the impact of migrating from the existing definition to the new definition on existing virtualized architecture.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - MRO, Group Name Westar-KCPL	

Answer	
Document Name	
Comment	
Westar / Kansas City Power & Light support Edison Electric Institute’s (EEI) response to Question 11.	
Likes 0	
Dislikes 0	
Response	
Patricia Boody - Lakeland Electric - 1,3,5,6	
Answer	
Document Name	
Comment	
LAK believes that the actual question is not just the level of effort to migrate from existing to new definitions for backwards compatibility. For entities who need to maintain the existing terms and moving toward new definitions, they will likely need to address their entire CIP program, from start to finish. Even adopting the new terms and new requirements as entities move toward more virtualization will require updates to CIP-002 programs to ensure that the devices are identified and categorized appropriately. The new requirements (not just for CIP-005, but the conforming changes and nuances of the changes to the standards based on new and revised glossary terms) will be just as dramatic to implement as CIP Version 5. While LAK believes that it is the right way to go, LAK has concerns that it will take considerable effort, both in terms of time and energy as well as in dollars, to implement. We do not believe that industry will be able to adopt it and incorporate the new definitions and changes to a single set of the CIP suite of standards such as CIP-005-6 without overhauling the entire CIP program (including training and security awareness as well as the more technical security based standards)	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	
Document Name	
Comment	
The effort appears to be substantial; however, with the clarification of ESZ, it may help lessen the effort.	
Likes 0	
Dislikes 0	

Response

Bobbi Welch - Midcontinent ISO, Inc. - 2 - MRO,SERC,RF

Answer	
Document Name	

Comment

MISO Comment: The proposed new definitions on existing virtualized architecture do not pose any significant issues. In contrast, CIP-005-7 as currently written is not directly Backwards Compatible and, as such, has the potential to pose significant issues for entities who must re-architect virtual infrastructure to comply with the new verbiage. For this reason, MISO recommends the Implementation Plan for CIP-005-7 allow adequate time for entities to come into compliance with the new standard; i.e. 36 months.

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 1,3,6

Answer	
Document Name	

Comment

In our transmission operations control centers we are removing all Virtual infrastructure so effort would be non-existent. However, for our RSA and AMAG these will need to be relocated to an ESP and split into two sets of systems for Medium and High sites.

This will be a very low to low effort for our generation fleet.

Likes 0	
Dislikes 0	

Response

Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5

Answer	
Document Name	

Comment

Significant level of effort due to issues with inclusion of serial connectivity. As previously stated in the answer to question #2, we may need additional hardware/infrastructure to comply with the current draft.

Likes 0

Dislikes 0

Response

Michael Johnson - Pacific Gas and Electric Company - 1,3,5 - WECC

Answer

Document Name

Comment

PG&E indicates the following:

1 – For CIP-002, PG&E does not foresee any backward compatibility issues since virtualization is currently lightly used. It does appear the effort to record the new Cyber Asset types (i.e. EACS, EAMS, PAMS, VCA, etc..) will require internal process modifications and some yet to be determined administrative effort to verify they are identified and documented as virtualization is expanded.

2 – For CIP-005, similar to the above CIP-002 input, PG&E does not foresee any backward compatibility issues since virtualization is currently lightly used within the BCS environment. There is a concern about the creation of the proper documentation to demonstrate compliance with the different connectivity/communication methods to be allowed. With the expansion of definitions and potential methods to meet the protection objectives, it is very possible evidence can be created that an Audit Team would deem insufficient. This is especially true for some of the newer technology that Audit Teams do not have experience with.

Recommendation - PG&E recommends the SDT work on guidance for the generation of proper evidence to help reduce differences in interruption.

Likes 0

Dislikes 0

Response

Aubrey Short - FirstEnergy - FirstEnergy Corporation - 1,3,4, Group Name Aubrey Short, On Behalf of:

Answer

Document Name

Comment

The document has made significant effort to maintain compatibility with CIP-005-6.

Likes 0

Dislikes 0

Response

Greg Davis - Georgia Transmission Corporation - 1

Answer	
Document Name	
Comment	
GTC is supportive of making modifications to its program in order for the standards to progress to a more technology agnostic model. We recommend that at least 24 months be permitted to make these changes related to virtualization. However, we also request that the splitting of the EAMS and EACS definition occur promptly as it is currently prohibiting the adoption of controls that would increase the security of BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Network and Security Technologies - 1 - NA - Not Applicable	
Answer	
Document Name	
Comment	
N&ST believes the SDT’s efforts to maintain “backward compatibility” that will not force entities with existing, non-virtualized environments to make any significant changes have been largely successful. N&ST believes the impact on entities that are presently utilizing highly virtualized networking and computing environments could, depending on their detailed configurations, range from minor to fairly significant.	
Likes 0	
Dislikes 0	
Response	

12. The SDT posted a draft CIP-005-7 Technical Rationale document to explain the basis behind these proposed changes. Please provide any additional comments on this document	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1,3,5,6	
Answer	
Document Name	
Comment	
No additional comments	
Likes 0	
Dislikes 0	
Response	
Jenifer Holmes - Alliant Energy Corporation Services, Inc. - 4 - MRO,RF	
Answer	
Document Name	
Comment	
Alliant supports MRO NSRF's comments.	
Likes 0	
Dislikes 0	
Response	
Trevor Tidwell - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	
Document Name	
Comment	
Most of our comments are addressed in other comments. The rationale does not appear to have any outstanding errors, but most of the focus was on the actual requirements. The rationale will need to be revised if modifications are made.	
Likes 0	
Dislikes 0	
Response	

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

Answer

Document Name

Comment

Southern applauds the SDT for the hard work in the development of the draft CIP-005-7 Technical Rationale document that provides thorough descriptions of the proposed changes and visual organization of these newly proposed concepts. Additional clarification on new Glossary Terms and revisions to existing terms will help bring the industry closer to continued forward progress towards enhanced security and reliability through these new risk-based approaches.

Likes 0

Dislikes 0

Response

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

Answer

Document Name

Comment

None.

Likes 0

Dislikes 0

Response

Bruce Reimer - Manitoba Hydro - 1,3,5,6

Answer

Document Name

Comment

In our view, if all virtual devices are identified properly, they will fall within the definition of BCA, EACMS, or PACS, the logical isolation may not be needed since all CIP Cyber Asset are protected by the current CIP requirements.

Likes 0

Dislikes 0

Response

Teresa Cantwell - Lower Colorado River Authority - 1,5

Answer	
Document Name	

Comment

None.

Likes 0	
Dislikes 0	

Response

Andrea Barclay - Georgia System Operations Corporation - 3,4

Answer	
Document Name	

Comment

GSOC/OPC requests additional clarity regarding the intent of the last paragraph on p. 26 of the Technical Rationale document relative to the explanation of the interaction between CIP-012 and CIP-005 super-ESP concept.

Likes 0	
Dislikes 0	

Response

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5

Answer	
Document Name	

Comment

We agree with EEI's comments and appreciate the hard work done by the SDT in the development of the draft CIP-005-7 Technical Rationale document believing that it provides a thorough description of the proposed changes.

If the SDT should decide to revise the document, we would request enlargement of the diagrams on pp. 20-21, additional annotation of the components, and color coding of the lines with respect to serial and routable protocol for greater clarity.

To help entities interpret the diagrams for their systems, the location Alpha scenarios should be updated to show the following:

A single unit for a plant DCS system – where the system could be local routable with serial conversion then out, or routable end to end

Substations where the end point devices are serial connected BCS (all diagrams depict blue-line connectivity that implies local routable connectivity – this could be true with some systems in the substations) Provide clarity where a “protocol break” vs IP to serial conversion pass-through occurs in the diagrams. Previous guidance suggests that this changes whether ERC exists or not. The differences between High and Medium Impact applications Make it clearer where “system-to-system” communications is occurring.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE included comments on the Technical Rationale in its answers to #9 and #10.	
Likes 0	
Dislikes 0	
Response	
Greg Davis - Georgia Transmission Corporation - 1	
Answer	
Document Name	
Comment	
GTC requests additional clarity regarding the intent of the last paragraph on p. 26 of the Technical Rationale document relative to the explanation of the interaction between CIP-012 and CIP-005 super-ESP concept.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Pacific Gas and Electric Company - 1,3,5 - WECC	

Answer

Document Name

Comment

PG&E indicates the Technical Rationale document does provide good information on the modifications and their impact. There is a great deal of information contained with the document which requires multiple readings and back-and-forth referencing between some sections to fully understand the impacts. PG&E believes the magnitude of the modifications necessitate the current condition of the document and does not have any recommendations for improvement in its presentation.

Recommendation - As noted in PG&E Question 2 input, we recommend if SCI of different impact ratings cannot share the same CPU and memory, it be clearly indicated within the Technical Rationale document.

Likes 0

Dislikes 0

Response

Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5

Answer

Document Name

Comment

The diagrams do not clearly depict the demarcation points between the hypervisors, management system and SCI. In addition, the diagrams do not provide examples where there is no separate management system and the built-in features of hypervisors are used to manage the SCI. In such scenarios, it appears that accessing the hypervisor directly would not comply with CIP-005-7 R1.6. Also, see Tri-State's other comments regarding defining management systems, management plane, data plane and providing examples.

On page 7 of the Technical Rationale, the sentence “The reliance on “using a routable protocol” has been removed to incorporate IP to serial conversion scenarios to serial only Cyber Assets” is inconsistent with the removal of ERC from the revised definition of IRA. The SDT could change it to: “If a serial is converted to IP before leaving the substation.”

Likes 0

Dislikes 0

Response

Bobbi Welch - Midcontinent ISO, Inc. - 2 - MRO,SERC,RF

Answer

Document Name

Comment

None

Likes 0	
Dislikes 0	

Response

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

Answer	
Document Name	

Comment

EEI appreciates the hard work done by the SDT in the development of the draft CIP-005-7 Technical Rationale document, believing that it provides a thorough description of the proposed changes. However, EEI member companies recommend clarifying the new NERC Glossary Terms along with revisions to existing terms while not creating new compliance obligations for entities that do not use a virtualization.

Likes 0	
Dislikes 0	

Response

Patricia Boody - Lakeland Electric - 1,3,5,6

Answer	
Document Name	

Comment

LAK believes that the Technical Rationale is a good start but may need additional explanations for some of the concepts (for example R Parts 2.4 and Part 2.5 related to system-to-system remote access). We appreciated the extension of time to review all documentation; however, other obligations prevented LAK from a detailed review of the TR document.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - MRO, Group Name Westar-KCPL

Answer	
Document Name	

Comment

Westar / Kansas City Power & Light support Edison Electric Institute’s (EEI) response to Question 12.	
Likes 0	
Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,5,6 - SERC, Group Name Duke Energy	
Answer	
Document Name	
Comment	
Duke Energy does not have any additional comments at this time.	
Likes 0	
Dislikes 0	
Response	
Jennifer Wright - Sempra - San Diego Gas and Electric - 1,3,5	
Answer	
Document Name	
Comment	
SDG&E supports EEI’s comments submitted on our behalf.	
Likes 0	
Dislikes 0	
Response	
Michael Puscas - ISO New England, Inc. - 2	
Answer	
Document Name	
Comment	
The Technical Rationale goes further than the requirements. For example, the Technical Rational explains what “affinity” means, but that is not included in the requirements. Concepts such as “affinity” should be included in the requirements, not just in the Technical Rationale.	

Likes 0	
Dislikes 0	
Response	
James Brown - California ISO - 2 - WECC	
Answer	
Document Name	
Comment	
No additional comments on the technical rationale document.	
Likes 0	
Dislikes 0	
Response	
Neil Swearingen - Salt River Project - 1,3,5,6 - WECC	
Answer	
Document Name	
Comment	
SRP has no additional comments.	
Likes 0	
Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	
Document Name	
Comment	
We appreciate the SDT’s work on this document. It provides valuable information and guidance to entities on the updated requirements.	
Likes 0	
Dislikes 0	

Response	
Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	
Document Name	
Comment	
Great job! City Light recognizes the hard work by the SDT and appreciates the effort to explain and clarify the proposed modifications.	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1,3,5,6	
Answer	
Document Name	
Comment	
The Exelon companies agree with the EEI recommendation to clarify the NERC Glossary Terms so as not create new compliance obligations for entities that do not use virtualization.	
Likes 0	
Dislikes 0	
Response	
Chinedu Ochonogor - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	
Document Name	
Comment	
AZPS would like to see more explanation in the technical rational on how virtualized networking should be considered. Software defined networking needs more emphasis in the use with virtualized system. AZPS believes this is needed as we implement the zero trust security architecture in accordance with the CIP requirements.	
Likes 0	
Dislikes 0	

Response

Gladys DeLaO - CPS Energy - 1,3,5

Answer	
Document Name	

Comment

Request for additional information to be contained in the Technical Rationale document are included in our response to previous questions.

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	
Document Name	

Comment

We agree with EEI comments and appreciate the hard work done by the SDT in the development of the draft CIP-005-7 Technical Rationale document believing that it provides a thorough description of the proposed changes.

If the SDT should decide to revise the document, we would request enlargement of the diagrams on pp. 20-21, additional annotation of the components, and color coding of the lines with respect to serial and routable protocol for greater clarity.

To help entities interpret the diagrams for their systems, the location Alpha scenarios should be updated to show the following:

A single unit for a plant DCS system – where the system could be local routable with serial conversion then out, or routable end to end

Substations where the end point devices are serial connected BCS (all diagrams depict blue-line connectivity that implies local routable connectivity – this could be true with some systems in the substations)

Provide clarity where a “protocol break” vs IP to serial conversion pass-through occurs in the diagrams. Previous guidance suggests that this changes whether ERC exists or not.

The differences between High and Medium Impact applications

Make it clearer where “system-to-system” communications is occurring.

Likes 0	
Dislikes 0	

Response

Davis Jelusich - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Public Utility District No. 1 of Chelan County	
Answer	
Document Name	
Comment	
CHPD believes that it would be useful to include examples of successful compliance of the proposed changes. The current wording makes it difficult to realize implementation of virtualized BES Cyber Systems in a mixed-trust environment. Examples should directly identify controls that can be applied to enable the use of CIP and non-CIP devices within the same virtual environment.	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	
Document Name	
Comment	
BPA largely agrees with the Technical Rationale, and the case for virtualization changes is supported by literally incalculable benefit. The TR does a good job with the basics; there is justification far beyond what can be captured in a single white paper or on this comment form.	
Likes 0	
Dislikes 0	
Response	
Kent Feliks - AEP - 3,5	
Answer	
Document Name	
Comment	
AEP is appreciative of the efforts of the SDT in not only the standard modifications but also the Technical Rationale document. We also recommend providing some clarification surrounding the ESZ definition as well as ensuring new compliance obligations are not created for those who do not use virtualization currently.	
Likes 0	
Dislikes 0	
Response	

Andy Crooks - SaskPower - 1,3,5,6,9 - MRO

Answer	
Document Name	

Comment

We agree with EEI comments.

EEI appreciates the hard work done by the SDT in the development of the draft CIP-005-7 Technical Rationale document believing that it provides a thorough description of the proposed changes.

If the SDT should decide to revise the document, we would request enlargement of the diagrams on pp. 20-21, additional annotation of the components, and color coding of the lines with respect to serial and routable protocol for greater clarity.

To help entities interpret the diagrams for their systems, the location Alpha scenarios should be updated to show the following:

> A single unit for a plant DCS system – where the system could be local routable with serial conversion then out, or routable end to end
>
> Substations where the end point devices are serial connected BCS (all diagrams depict blue-line connectivity that implies local routable connectivity – this could be true with some systems in the substations)
>
> Provide clarity where a “protocol break” vs IP to serial conversion pass-through occurs in the diagrams. Previous guidance suggests that this changes whether ERC exists or not.
>
> The differences between High and Medium Impact applications
>
> Make it clearer where “system-to-system” communications is occurring.

Likes 0	
Dislikes 0	

Response

Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	
Document Name	

Comment

We agree with EEI comments.

EEI appreciates the hard work done by the SDT in the development of the draft CIP-005-7 Technical Rationale document believing that it provides a thorough description of the proposed changes.

If the SDT should decide to revise the document, we would request enlargement of the diagrams on pp. 20-21, additional annotation of the components, and color coding of the lines with respect to serial and routable protocol for greater clarity.

To help entities interpret the diagrams for their systems, the location Alpha scenarios should be updated to show the following:

A single unit for a plant DCS system – where the system could be local routable with serial conversion then out, or routable end to end

Substations where the end point devices are serial connected BCS (all diagrams depict blue-line connectivity that implies local routable connectivity – this could be true with some systems in the substations)

Provide clarity where a "protocol break" vs IP to serial conversion pass-through occurs in the diagrams. Previous guidance suggests that this changes whether ERC exists or not.

The differences between High and Medium Impact applications

Make it clearer where "system-to-system" communications is occurring.

Likes 0	
Dislikes 0	

Response

faranak sarbaz - Los Angeles Department of Water and Power - 1,3,5,6

Answer	
Document Name	

Comment

No additional comments.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	
Document Name	

Comment

None.

Likes 0	
Dislikes 0	

Response

Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	
Document Name	
Comment	
No additional comments.	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Cleco Corporation - 1,3,5,6 - SERC	
Answer	
Document Name	
Comment	
See EEI Comments.	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	
Document Name	
Comment	
No Additional Comments.	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	

Document Name	
Comment	
Reclamation appreciates the time and effort put into producing the CIP-005-7 Technical Rationale and believes it is a needed document to provide the framework for the revised CIP-005-7 standard.	
Likes 0	
Dislikes 0	
Response	

13. Provide any additional comments for the SDT to consider, if desired

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	
Document Name	

Comment

In regards to filling out the evidence request spreadsheet, registered entities that are already implementing virtualization now must identify and adjust for new terms. Registered entities that are currently using virtualized environments list the host (hypervisor) as a CA (BCA, EACMS, PACS, PCA, etc.) and include the VMs.

Likes 0	
Dislikes 0	

Response

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5

Answer	
Document Name	

Comment

We agree with EEI comments:

“EEI notes many improvements over the previous virtualization proposal, however we remain concerned over the level of change to the CIP Standards: new, revised, and retired Glossary Terms; new and revised CIP-005 Requirements. To address these concerns, EEI suggests the SDT take another approach to virtualization by offering clear alternatives in the Standards—options—much like a decision box or if / then statements.

For example: If you use virtual, then take path B; if not, continue with path A’s existing requirements. We believe such an approach would provide an easier transition.”

We submit as a possible solution to backwards compatibility the precedent established by the PRC-005-2 Implementation Plan, whereby an Entity could choose to remain compliant with PRC-005-1.1b on a component by component basis until it elected PRC-005-2, or was required to by the 100% compliance implementation date.

For CIP-005-7, the Implementation Plan could include language such as: “Each Responsible Entity shall maintain documentation to demonstrate compliance with either CIP-005-6 (according to the Glossary Terms as defined prior to the conforming changes driven by CIP-005-7) or CIP-005-7 (or subsequent versions), but not both, for a given ESP or ESZ.”

Likes 0	
Dislikes 0	

Response

Andrea Barclay - Georgia System Operations Corporation - 3,4	
Answer	
Document Name	
Comment	
GSOC/OPC is concerned that the list of Applicable Systems identified in Section 4 of CIP-005 is not reflective of the “systems” listed within the requirements table. The requirements table and Section 4 of the standard should reflect/list the same potential “Applicable Systems” as applicable across and within the standard. Accordingly, GSOC/OPC recommends that the SDT review this discrepancy and make the revisions necessary to ensure consistency. Further, GSOC/OPC is concerned that some of the “systems” listed as “Applicable Systems” within the requirements table are not necessarily systems and, therefore, do not necessarily easily lend themselves to identification of a particular asset or system. For this reason, such classification may result in each Responsible Entity attempting to “translate” such system into a set of associated assets, e.g., ESP and ESZ. Such translation could vary greatly by and amongst Responsible Entities as well as the ERO and its auditors. GSOC/OPC recommends that the SDT review these revisions to the “Applicable Systems” column to ensure that the objective and applicability is clear, unambiguous, and feasible. GSOC/OPC notes that the use of terms versus associated acronyms is inconsistent in the proposed draft of CIP-005, e.g., use of “IS” versus use of “Intermediate System.” GSOC/OPC recommends the SDT evaluate the proposed draft for consistent usage of acronyms versus defined terms. Finally, GSOC/OPC notes that there was not an update to or an indication of review of VSLs or VRFs. It is recommended that such review occur to ensure that they remain consistent with the requirements of CIP-005.	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5	
Answer	
Document Name	
Comment	
None.	
Likes 0	
Dislikes 0	
Response	
Bruce Reimer - Manitoba Hydro - 1,3,5,6	
Answer	
Document Name	

Comment

We disagree with the proposed changes. In our view, current CIP requirements can apply to virtualization environment smoothly without significant changes. Given that the CIP compliance program today works fairly smoothly by implementing the existing requirements, any changes of requirements and definitions beyond virtualization shouldn’t be targeted such as network layer protection for EACMS and PACS proposed in CIP-005-7 R1. SDT should focus on how to resolve CIP compliance in the virtualization environment without prohibiting the new technology rather than try to change the requirements for the defense in depth since it is not the driver for this project. Resulting from our comments in the above questions, as long as the Cyber Asset definition are modified to include virtual devices, most of existing CIP V5 requirements would apply to virtualization environment seamlessly.

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 of Edison Electric Institute.

Likes 0

Dislikes 0

Response

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

Answer

Document Name

Comment

The new CIP-005 standard provides more clarity around the use of virtual infrastructure and virtual machines, but will require 2-3 years for some companies to implement – this is not a like to like change.

ERCOT suggests spelling out acronyms in all requirement parts in order to ensure they are clearly understood.

Removable Media: Examples were removed. However, examples were still listed for Transient Cyber Asset. ERCOT believes Examples are very helpful.

PAMS and PACS: Based on the implementations, mounted hardware or devices might not actually be mounted exactly at the Physical Security Perimeter. ERCOT suggests the SDT consider rewording.

Likes 0	
Dislikes 0	

Response

Trevor Tidwell - PNM Resources - Public Service Company of New Mexico - 1,3

Answer	
Document Name	

Comment

SDT needs to remember that some technologies are not virtualization specific. The idea of an ESZ and policies can apply to physical systems today. Windows has Windows Firewall and Group Policy can push out policies for those host-based firewalls. This means an operator workstation with a Window Firewall enabled could be a BCA and EACS and SCI under the proposed definitions. Those workstations also have a single network address but across usually two NICS. If that is the case then under proposed CIP-005 R1.6 what is the management system for that operator workstation? If it is the same NICS used for SCADA and other typical operations tasks then there can be no separation of that management plane.

Some of the new requirements still have a prescriptive rather than objective bent. Please try to word the requirements to give entities an objective to met rather than the SDT determine the risk and prescribe the solution. Instead define the risk and the objective regarding the risk. This is what we attempted to do in comment #5, “Have a means to reduce risk of a VCA utilizing CPU, memory, or storage in a way that prevents other VCAs from having access to those resources.”

Again we understand the effort the SDT has put into this and this is not an easy task. We hope the comments help the SDT towards its goals of more objective rather than prescriptive requirements that addresses all the items before the SDT.

Likes 0	
Dislikes 0	

Response

Jenifer Holmes - Alliant Energy Corporation Services, Inc. - 4 - MRO,RF

Answer	
Document Name	

Comment	
Alliant supports MRO NSRF's comments.	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1,3,5,6	
Answer	
Document Name	
Comment	
No additional comments	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	
Document Name	
Comment	
Reclamation recommends that electronic isolation distinguish between system protection levels along with BES and non-BES. An Electronic Security Zone (ESZ) could become a risk to BES Cyber Systems when stretched to corporate business enclaves through virtual machine hyper jumping from a lower trust business network. Mixed trust environments on shared infrastructure between CIP Applicable Systems and corporate business networks could also introduce unnecessary risk to the BES. All shared infrastructure needs to be protected at the highest level of identified system that resides on it.	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	
Document Name	

Comment	
None	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Cleco Corporation - 1,3,5,6 - SERC	
Answer	
Document Name	
Comment	
See EEI Comments. Also, the language used in the CIP-005-7 R1.6 and R2.6 requirements is confusing. The use of multiple "or" statements makes the requirements difficult to interpret. Also, the term "management plane" is not defined, but is referenced twice in the standard.	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	
Document Name	
Comment	
No additional comments.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	

Document Name

Comment

The new CIP-005 standard provides more clarity around use of virtual infrastructure and virtual machines but will require 2-3 years for some companies to implement – this is not a like to like change. It is somewhat noteworthy that many entities have already implemented virtual infrastructure and are able to comply, even under audit scrutiny, to the current wording of the standards. As such, the SWG believes current approved and implemented versions of the standards allow and support virtualization with no change.

General comment: Spell out acronyms in all requirement parts to ensure clear understanding.

Removable Media: Examples were removed. However, examples were still listed for Transient Cyber Asset. Examples are very helpful.

PAMS and PACS: Based on the implementations, mounted hardware or devices might not actually be mounted exactly at the Physical Security Perimeter. Consider rewording this.

Likes 0

Dislikes 0

Response

faranak sarbaz - Los Angeles Department of Water and Power - 1,3,5,6

Answer

Document Name

Comment

No additional comments.

Likes 0

Dislikes 0

Response

Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer

Document Name

Comment

We agree with EEI comments:

“EEI notes many improvements over the previous virtualization proposal, however we remain concerned over the level of change to the CIP Standards: new, revised, and retired Glossary Terms; new and revised CIP-005 Requirements. To address these concerns, EEI suggests the SDT take another approach to virtualization by offering clear alternatives in the Standards—options—much like a decision box or if / then statements.

For example: If you use virtual, then take path B; if not, continue with path A’s existing requirements. We believe such an approach would provide an easier transition.”

We submit as a possible solution to backwards compatibility the precedent established by the PRC-005-2 Implementation Plan, whereby an Entity could choose to remain compliant with PRC-005-1.1b on a component by component basis until it elected PRC-005-2, or was required to by the 100% compliance implementation date.

For CIP-005-7, the Implementation Plan could include language such as: “Each Responsible Entity shall maintain documentation to demonstrate compliance with either CIP-005-6 (according to the Glossary Terms as defined prior to the conforming changes driven by CIP-005-7) or CIP-005-7 (or subsequent versions), but not both, for a given ESP or ESZ.”

Likes 0	
Dislikes 0	

Response

Andy Crooks - SaskPower - 1,3,5,6,9 - MRO

Answer	
Document Name	

Comment

We agree with EEI comments:

“EEI notes many improvements over the previous virtualization proposal, however we remain concerned over the level of change to the CIP Standards: new, revised, and retired Glossary Terms; new and revised CIP-005 Requirements. To address these concerns, EEI suggests the SDT take another approach to virtualization by offering clear alternatives in the Standards—options—much like a decision box or if / then statements.

For example: If you use virtual, then take path B; if not, continue with path A’s existing requirements. We believe such an approach would provide an easier transition.”

We submit as a possible solution to backwards compatibility the precedent established by the PRC-005-2 Implementation Plan, whereby an Entity could choose to remain compliant with PRC-005-1.1b on a component by component basis until it elected PRC-005-2, or was required to by the 100% compliance implementation date.

For CIP-005-7, the Implementation Plan could include language such as: “Each Responsible Entity shall maintain documentation to demonstrate compliance with either CIP-005-6 (according to the Glossary Terms as defined prior to the conforming changes driven by CIP-005-7) or CIP-005-7 (or subsequent versions), but not both, for a given ESP or ESZ.”

Likes 0	
Dislikes 0	

Response

Kent Feliks - AEP - 3,5

Answer	

Document Name	
Comment	
Many improvements made in this proposal are noted over the previous version. However, the proposed terms and requirement modifications need some clarification. AEP suggests taking an approach to these modifications that involves offering alternatives to virtualization within the standard. We understand it can be difficult to provide a new path for virtualization while also maintaining existing requirements, but we feel that both are needed.	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
Davis Jelusich - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Public Utility District No. 1 of Chelan County	
Answer	
Document Name	
Comment	
CHPD believes that it would be useful to see how these proposed changes are going to be applied to the other standards, particularly CIP-007 and CIP-010. It is difficult to identify how our existing workflows will change under the proposed changes.	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	

Document Name

Comment

As mentioned above, the proposed changes will bring auditing challenges for auditors as each policy based environment vendor will have differing approaches as well as modules, tools, monitoring, etc. to present policies versus existing environments with firewalls which can be presented uniformly (source, destination, port). We feel prior to approval(s), a standardized and approved audit approach should be published to the industry for auditing policy based environments.

Likes 0

Dislikes 0

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no NGrid and Eversource

Answer

Document Name

Comment

Comments on the Definitions

Shared Cyber Infrastructure (SCI) - we recommend changing from “Programmable electronic devices whose compute, storage” to “Programmable electronic devices whose processing resources”

Transient Cyber Asset (TCA)

- Should some TCA/VCA (Virtual Cyber Asset) be considered BCA (BES Cyber Asset)?
- We request a use case to better understand this standardized configuration
- Request clarification. Since the TCA needs to connect to a SCI, that forces the SCI to comply. What does the SCI comply with?

Protected Cyber Asset (PCA) – request confirmation that “shared compute resources” means other virtualized instances on the same SCI hypervisor

EACS (Electronic Access Control System) & EAMS (Electronic Access Monitoring System) – we request keeping the old term / definition / applicability EACMS in addition to these two new terms / definitions / applicability. We suggest that the Entity has the flexibility to use any of these three terms / definitions / applicability to avoid forcing Entities in to costly, large changes to their documentation and training, etc.

ESZ (Electronic Security Zone) – we recommend changing from “A segmented section of a network that contains systems and components to create a logical isolation” to “is a network that is logically isolated” because the network is logically isolated, a segment is not. The network does not “contain systems and components to create a logical isolation.”

PSP (Physical Security Perimeter) – we recommend changing from “The physical border at which access is controlled.” to “The border at which physical access is controlled.”

Comments on the Standard – Exemptions

4.2.3 - request clarification. Will these Exemptions apply to all CIP Standards?

4.2.3.3 – request clarification since this new exemption is not consistent with CIP-006 R10 to physically protect communication lines between PSPs (Physical Security Perimeter)

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	
Document Name	

Comment

We agree with EEI comments:

“EEI notes many improvements over the previous virtualization proposal, however we remain concerned over the level of change to the CIP Standards: new, revised, and retired Glossary Terms; new and revised CIP-005 Requirements. To address these concerns, EEI suggests the SDT take another approach to virtualization by offering clear alternatives in the Standards—options—much like a decision box or if / then statements.

guidance suggests that this changes whether ERC exists or not.

The differences between High and Medium Impact applications

Make it clearer where “system-to-system” communications is occurring.

Provide any additional comments for the SDT to consider, if desired.

Comments:

We agree with EEI comments:

“EEI notes many improvements over the previous virtualization proposal, however we remain concerned over the level of change to the CIP Standards: new, revised, and retired Glossary Terms; new and revised CIP-005 Requirements. To address these concerns, EEI suggests the SDT take another approach to virtualization by offering clear alternatives in the Standards—options—much like a decision box or if / then statements.

For example: If you use virtual, then take path B; if not, continue with path A’s existing requirements. We believe such an approach would provide an easier transition.”

We submit as a possible solution to backwards compatibility the precedent established by the PRC-005-2 Implementation Plan, whereby an Entity could choose to remain compliant with PRC-005-1.1b on a component by component basis until it elected PRC-005-2, or was required to by the 100% compliance implementation date.

For CIP-005-7, the Implementation Plan could include language such as: “Each Responsible Entity shall maintain documentation to demonstrate compliance with either CIP-005-6 (according to the Glossary Terms as defined prior to the conforming changes driven by CIP-005-7) or CIP-005-7 (or subsequent versions), but not both, for a given ESP or ESZ.”

Likes 0	
Dislikes 0	

Response

Gladys DeLaO - CPS Energy - 1,3,5

Answer	
Document Name	

Comment

There should be considerations for all CIP standards impacted by virtualization be updated concurrently to ensure efforts to make the necessary modifications to existing architecture by the entity. Additionaly, ensure all new terms are defined.

Likes 0	
Dislikes 0	

Response

Chinedu Ochonogor - APS - Arizona Public Service Co. - 1,3,5,6

Answer	
Document Name	

Comment

The full impact of the proposed definition changes is difficult to assess without also reviewing the proposed changes to CIP-007 and CIP-010. AZPS would like to have the ability to comment on these definition changes along with the CIP-007 and CIP-010 commenting periods. AZPS appreciates and supports the work invested in modifying these requirements. The transparent nature the SDT has taken to relay the intent and need for change has not gone unnoticed.

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer	
Document Name	
Comment	
Consider rewording CIP-005 R1 P1.6 and R2 P2.6 for better clarity.	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1,3,5,6	
Answer	
Document Name	
Comment	
The Exelon companies appreciate the opportunity to comment on this important topic and the good work being done by the SDT. We also however agree with the EEI comments expressing concern that absent additional clarification the proposed version may create unnecessary burden for registered entities that are not planning to deploy virtualization.	
Likes 0	
Dislikes 0	
Response	
Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	
Document Name	
Comment	
City Light again commends the SDT on their persistence and effort to tackle this tough challenge. *One gap that we would like to see addressed by the SDT is guidance to demonstrate consistency of the proposed virtualization modifications for High and Medium assets with use of virtualization at Low assets under CIP-003-7 R2 Attachment 1 Section 3 Electronic Security. As much as possible, please be sure the approaches proposed here do not directly conflict with the extensive guidance about electronic access provided to support CIP-003-7.* *City Light also asks that any new security requirements for existing physical BCS and associated devices be removed from this proposed Standard and be discussed and balloted separately. To minimize scope creep, we request that the risks be quantified and presented that justify these expanded non-virtualization requirements, those that add new security controls beyond the conceptual changes necessary to accommodate virtualization in the CIP standards.*	

Likewise, City Light asks that other non-virtualization concepts, such as the changes to treatment of routable connectivity and Dial-up Connectivity be treated in a separate comment period and proposal. We appreciate the efforts of the SDT to identify the location and nature of non-virtualization changes in this material and comment form, but we feel all non-virtualization changes should be treated separately. The modifications for virtualization are a big enough lift on their own, they and should not be combined (and confused) with other unrelated changes.

City Light also recommends that the SDT strongly recommend that NERC conduct a pilot program to evaluate the CIP modifications for virtualization, because of the many changes and new definitions that are required in the existing Standards. Such a pilot program could be similar to the one conducted in all regions as part of (and prior to) the CIP v5 transition.

City Light requests that the phrase "that could lead to misoperation or instability in the BES" be restored to the Purpose statement of proposed CIP-005-7. This phrase is an essential scoping statement necessary to identify the applicability of the controls of CIP-005.

Finally, we note the incorrect punctuation for (presumably) the plural of acronyms as used throughout this comment form, the proposed CIP-005-7, and supporting materials. For instance, the plural of "VCA" is "VCAs," not "VCA's" as used above. "VCA's" is the possessive form, and by context that is not what is intended in the draft documents.

Likes 0	
Dislikes 0	

Response

Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates

Answer	
Document Name	

Comment

Overall, we support the updates to CIP-005. However, there are several instances where verbiage is focused almost solely on virtualization, and we see opportunities where entities might be confused as to whether it applies to existing, non-virtualized infrastructure and, if it does apply, confusion on how it would apply. Additionally, there appears to be a significant amount of change to documentation and evidence that will impact entities with no virtualized environment or virtualized environments that are segmented are in compliance today. While some of this might be unavoidable, it would be prudent of the SDT to continue to actively consider how to make updates to the standards without placing a large burden on entities that would like to "stay the way they are today."

Likes 0	
Dislikes 0	

Response

Quintin Lee - Eversource Energy - 1,3

Answer	
Document Name	

Comment

Eversource notes many improvements over the previous virtualization proposal, however we remain concerned over the level of change to the CIP Standards: new, revised, and retired Glossary Terms; new and revised CIP-005 Requirements. To address these concerns, Eversource suggests the SDT take another approach to virtualization by offering clear alternatives in the Standards—options—much like a decision box or if / then statements.

For example: If you use virtual, then take path B; if not, continue with path A's existing requirements. We believe such an approach would provide an easier transition

Likes 0	
Dislikes 0	

Response

Neil Swearingen - Salt River Project - 1,3,5,6 - WECC

Answer	
Document Name	

Comment

SRP has no additional comments.

Likes 0	
Dislikes 0	

Response

James Brown - California ISO - 2 - WECC

Answer	
Document Name	

Comment

The new CIP-005 standard provides more clarity around use of virtual infrastructure and virtual machines but will require 2-3 years for some companies to implement – this is not a like to like change. It is somewhat noteworthy that many entities have already implemented virtual infrastructure and are able to comply, even under audit scrutiny, to the current wording of the standards. As such, the CAISO believes current approved and implemented versions of the standards allow for virtualization. These changes would guide the adoption of virtualized environments, but any changes need to be backward compatible to support existing solutions.

General comment: Spell out acronyms in all requirement parts to ensure clear understanding.

Removable Media: Examples were removed. However, examples were still listed for Transient Cyber Asset. Examples are very helpful.

PAMS and PACS: Based on the implementations, mounted hardware or devices might not actually be mounted exactly at the Physical Security Perimeter. Consider rewording this.

Likes 0	

Dislikes 0	
Response	
Jennifer Wright - Sempra - San Diego Gas and Electric - 1,3,5	
Answer	
Document Name	
Comment	
SDG&E supports EEI’s comments submitted on our behalf.	
Likes 0	
Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,5,6 - SERC, Group Name Duke Energy	
Answer	
Document Name	
Comment	
Duke Energy does not have any additional comments at this time.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - MRO, Group Name Westar-KCPL	
Answer	
Document Name	
Comment	
Westar / Kansas City Power & Light support Edison Electric Institute’s (EEI) response to Question 13.	
Likes 0	
Dislikes 0	
Response	

Patricia Boody - Lakeland Electric - 1,3,5,6	
Answer	
Document Name	
Comment	
LAK realizes that the SDT is not yet developing an implementation plan. LAK recommends that the SDT consider these changes and the implications of major overhaul of existing CIP programs when developing the proposal for an implementation plan. LAK also recommends that NERC establish another group similar to the v5TAG for a pilot implementation of the revised standards.	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	
Document Name	
Comment	
EEI notes many improvements over the previous virtualization proposal, however the new, revised, and retired Glossary Terms; new and revised CIP-005 Requirements need to be further clarified. While the proposed changes achieve many of the desired goals (i.e., more broadly enabled virtualization), there remains some concerns that those changes may create unnecessary burden for registered entities that are not planning to deploy virtualization. For this reason, we ask the SDT to look for additional opportunities to better clarify how both solutions can be achieved to address the broad needs of the Industry.	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2 - MRO,SERC,RF	
Answer	
Document Name	
Comment	
The proposed CIP-005-7 standard as currently written provides more clarity around use of virtual infrastructure and virtual machines and could require up to 3 years for some companies to implement. This does not equate to Backwards Compatibility as the standard does not allow entities to continue to operate "as is;" i.e. with no changes. In addition, a recent noteworthy observation is that multiple entities have implemented virtual infrastructure and have been found to be in compliance following an audit under the current version of the standards. As such, MISO recommends the SDT consider	

retaining the current approved and implemented versions of the standards "as is" and update the Technical Rationale and Justification document to describe how the standards support the implementation of virtualization with no change.

General comment: Spell out acronyms in all requirement parts to ensure clear understanding.

Removable Media: Examples were removed. However, examples were still listed for Transient Cyber Asset. Examples are very helpful.

PAMS and PACS: Based on the implementations, mounted hardware or devices might not actually be mounted exactly at the Physical Security Perimeter. Consider rewording this to allow for flexibility in location.

Likes 0	
Dislikes 0	

Response

Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5

Answer	
Document Name	

Comment

Please update the NERC Project Tracking Spreadsheet with a full list of standards that will be affected by these changes. In addition to what is listed, please add CIP-008, CIP-009, and CIP-011. In the future, consider adding CIP-013 due to the expectation of future versions including EACMS and firewalls.

There is an issue with this online comment form where it has not saved our Yes/No responses accurately and will not allow for manual changes. We have tried to provide context in each question to show whether Tri-State agrees with the modifications or not.

Likes 0	
Dislikes 0	

Response

Michael Johnson - Pacific Gas and Electric Company - 1,3,5 - WECC

Answer	
Document Name	

Comment

PG&E provides the following:

1 - PG&E submits the following concern regarding the proposed modification to the Physical Security Perimeter (PSP) definition:

Removal of the Cyber Asset types to be protected will lead to interpretation differences between Registered Entities and Audit Team on what should be physically protected. What is not indicated in the Technical Rationale document for the PSP modification is the method of indicating the Cyber Assets to be protected. PG&E assumes this will be done using appropriate modifications to the Applicable Systems column for each CIP-006 Requirement Part when those modifications are posted for comment.

If the above is not correct how Cyber Assets to be protected will be indicated, please indicate in later comment postings how those Cyber Assets will be indicated.

Likes 0	
Dislikes 0	

Response

Greg Davis - Georgia Transmission Corporation - 1

Answer	
Document Name	

Comment

GTC is concerned that the list of Applicable Systems identified in Section 4 of CIP-005 is not reflective of the "systems" listed within the requirements table. The requirements table and Section 4 of the standard should reflect/list the same potential "Applicable Systems" as applicable across and within the standard. Accordingly, GTC recommends that the SDT review this discrepancy and make the revisions necessary to ensure consistency.

Further, GTC is concerned that some of the "systems" listed as "Applicable Systems" within the requirements table are not necessarily systems and, therefore, do not necessarily easily lend themselves to identification of a particular asset or system. For this reason, such classification may result in each Responsible Entity attempting to "translate" such system into a set of associated assets, e.g., Electronic Security Perimeter and Electronic Security Zone. Such translation could vary greatly by and amongst Responsible Entities as well as the ERO and its auditors. GTC recommends that the SDT review these revisions to the "Applicable Systems" column to ensure that the objective and applicability is clear, unambiguous, and feasible.

GTC notes that the use of terms versus associated acronyms is inconsistent in the proposed draft of CIP-005, e.g., use of "IS" versus use of "Intermediate System." GTC recommends the SDT evaluate the proposed draft for consistent usage of acronyms versus defined terms.

Finally, GTC notes that there was not an update to or an indication of review of VSLs or VRFs. It is recommended that such review occur to ensure that they remain consistent with the requirements of CIP-005.

Likes 0	
Dislikes 0	

Response