Comment Report

Project Name:	2016-02 Modifications to CIP Standards | Concepts for Virtualization and Definitions
Comment Period Start Date:	10/6/2017
Comment Period End Date:	11/2/2017
Associated Ballots:	

There were 48 sets of responses, including comments from approximately 141 different people from approximately 94 companies representing 10 of the Industry Segments as shown in the table on the following pages.

Questions

1. Do you agree that the proposed change to the Cyber Asset definition makes it inclusive of both physical and virtual devices, including treatment of each virtual machine and hypervisor? If you do not agree, please provide rationale to support your position.

2. Do you agree that the term programmable in the Cyber Asset definition does not need further clarification at this time? If yes, please provide rationale to support your position.

3. If programmable does need further clarification, how would you prefer it to be addressed? Use comments to detail necessary definition changes or guidance that could be developed.

4. Do you agree with the proposed definition of Centralized Management Systems (CMS)? If not, please provide rationale to support your position.

5. Do you agree that the proposed definition of ESZ more adequately applies to proper isolation of multi-instance environments, regardless of OSI layer? If not, please provide a rationale to support your position.

6. Do you agree that the proposed definition of ESZ would aid the development of future CIP Standards by providing a more relevant level of separation? If not, please provide a rationale to support your position.

7. Do you agree that the proposed CIP-005 Requirement R1, Part 1.6 provides sufficient security controls for the high and medium impact BES Cyber Systems residing in a multi-instance environment and their associated CMS to reduce the stated risks inherent to virtualization? If not, please provide a rationale to support your position.

8. Do you agree that the proposed CIP-005 Requirement R1, Part 1.7 provides a necessary security control to the high and medium impact BES Cyber Systems residing in a multi-instance environment and their associated CMS(s) to reduce risks inherent to virtualization? If not, please provide a rationale to support your position.

9. Do you agree that the proposed CIP-005 Requirement R1, Part 1.8 provides sufficient security control to reduce the risks associated with shared multi-instance environments? If not, please provide a rationale to support your position.

10. The SDT asserts that the proposed CIP-005 Requirement 1, Part 3.1 provides additional security controls for remote access when performing CMS functions. These are necessary to reduce the risk associated with remote access to multi-instance environments. Do you agree with this assertion? If not, please provide a rationale to support your position.

11. Should the gap between Interactive Remote Access and system-to-system communication that was exposed by the examination of the risks inherent to virtualization be addressed for systems other than high and medium impact BES Cyber Systems residing in a multi-instance environment and their associated CMS? If not, please provide a rationale to support your position.

12. The SDT asserts that the new proposed CIP-004 Requirement R4, Part 4.5, provides additional security control to the electronic and unescorted physical access to multi-instance environment processes which reduces the “too much privilege” risk inherent to virtualization which has been identified. Do you agree with this assertion? If not, please provide a rationale to support your position.

13. Do you agree with the SDT’s assertion that the definition of EACMS is too broad and does not differentiate the capabilities and risk(s) of the systems that fall within that definition scope? If not, please provide rationale to support your position.

14. Do you agree that the language of the proposed definitions of EACS provides better consistency and clarity to the CIP Standards? If not, please provide rationale to support your position and alternative language.

15. Do you agree that the language of the proposed definitions of EAG provides better consistency and clarity to the CIP Standards? If not, please provide rationale to support your position and alternative language.

16. Do you agree that the current compliance requirements related to EACMS monitoring systems are precluding or discouraging solutions that could reduce risk to security and reliability? Please provide your rationale in support or against this assertion.

17. Should the security requirements for the access control portion of the EACMS to be different from the monitoring portion of the EACMS? If you do, please provide your rationale.

18. Should CIP-011 Requirement R2 scope be expanded to include designated storage locations for access monitoring systems? If not, please provide rationale to support your position.

19. Do you agree with assignment of CIP Standard requirements to each of the EACS, EAG, and CMS categories as presented in the table above? If not, please provide rationale to support your position.

20. As the standards today do not prohibit the use of virtualization technologies, do you support an approach where no changes are made to the CIP Standards in response to the virtualization issue identified by the V5 TAG? Please provide a rationale to support your position.

21. Is your organization in support of Concept 1: Modifications to allow use of secure multi-instance? Please provide rationale to support your position.

22. Is your organization in support of Concept 2: Modifications to the EACMS definition? Please provide rationale to support your position.

23. Is your organization in support of Concept 3: Compliance Guidance? Please provide rationale to support your position.

24. If you have additional comments that you have not provided in response to the questions above, please provide them here.

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim	1,3,4	RF	FirstEnergy Corporation	Aaron Ghdooshim	FirstEnergy - FirstEnergy Corporation	4	RF
					Aubrey Short	FirstEnergy - FirstEnergy Corporation	1	RF
					Theresa Ciancio	FirstEnergy - FirstEnergy Corporation	3	RF
					Robert Loy	FirstEnergy - FirstEnergy Solutions	5	RF
					Ann Ivanc	FirstEnergy - FirstEnergy Solutions	6	RF
Southern Company - Southern Company Services, Inc.	Brandon Cain	1,3,5,6	FRCC,MRO,NPCC,SERC,SPP RE,Texas RE,WECC	Southern Company	Katherine Prewitt	Southern Company - Southern Company Services, Inc.	1	SERC
					R. Scott Moore	Southern Company - Alabama Power Company	3	SERC
					William D. Shultz	Southern Company - Southern Company Generation	5	SERC
					Jennifer Sykes	Southern Company - Southern Company Generation and Energy Marketing	6	SERC
Florida Municipal Power Agency	Brandon McCormick	3,4,5,6	FRCC	FMPA	Tim Beyrle	City of New Smyrna Beach Utilities Commission	4	FRCC
					Jim Howard	Lakeland Electric	5	FRCC

					Lynne Mila	City of Clewiston	4	FRCC
					Javier Cisneros	Fort Pierce Utilities Authority	3	FRCC
					Randy Hahn	Ocala Utility Services	3	FRCC
					Don Cuevas	Beaches Energy Services	1	FRCC
					Jeffrey Partington	Keys Energy Services	4	FRCC
					Tom Reedy	Florida Municipal Power Pool	6	FRCC
					Steven Lancaster	Beaches Energy Services	3	FRCC
					Mike Blough	Kissimmee Utility Authority	5	FRCC
					Chris Adkins	City of Leesburg	3	FRCC
					Ginny Beigel	City of Vero Beach	3	FRCC
Tennessee Valley Authority	Brian Millard	1,3,5,6	SERC	Tennessee Valley Authority	Scott, Howell D.	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
Duke Energy	Colby Bellville	1,3,5,6	FRCC,RF,SERC	Duke Energy	Doug Hils	Duke Energy	1	RF
					Lee Schuster	Duke Energy	3	FRCC
					Dale Goodwine	Duke Energy	5	SERC
					Greg Cecil	Duke Energy	6	RF
Midcontinent ISO, Inc.	David Francis	2,3	FRCC,MRO,NPCC,RF,SERC,SPP RE,Texas RE,WECC	SRC + SWG	Gregory Campoli	New York Independent System Operator	2	NPCC

					Mark Holman	PJM Interconnection, L.L.C.	2	RF
					Charles Yeung	Southwest Power Pool, Inc. (RTO)	2	SPP RE
					Terry BIlke	Midcontinent ISO, Inc.	2	RF
					Elizabeth Axson	Electric Reliability Council of Texas, Inc.	2,3	Texas RE
					Ben Li	IESO	1	MRO
					Drew Bonser	SWG	NA - Not Applicable	NA - Not Applicable
					Darrem Lamb	CAISO	2	WECC
					Matt Goldberg	ISONE	2	NPCC
Public Utility District No. 1 of Chelan County	Janis Weddle	1,3,5,6		Chelan PUD	Haley Sousa	Public Utility District No. 1 of Chelan County	5	WECC
					Joyce Gundry	Public Utility District No. 1 of Chelan County	3	WECC
					Jeff Kimbell	Public Utility District No. 1 of Chelan County	1	WECC
DTE Energy - Detroit Edison Company	Karie Barczak	3,4,5		DTE Energy - DTE Electric	Jeffrey Depriest	DTE Energy - DTE Electric	5	RF
					Daniel Herring	DTE Energy - DTE Electric	4	RF
					Karie Barczak	DTE Energy - DTE Electric	3	RF
Associated Electric Cooperative, Inc.	Mark Riley	1,3,5,6		AECI & Member G&Ts	Mark Riley	Associated Electric Cooperative, Inc.	1	SERC
					Brian Ackermann	Associated Electric Cooperative, Inc.	6	SERC
					Brad Haralson	Associated Electric	5	SERC

						Cooperative, Inc.		
					Todd Bennett	Associated Electric Cooperative, Inc.	3	SERC
					Michael Bax	Central Electric Power Cooperative (Missouri)	1	SERC
					Adam Weber	Central Electric Power Cooperative (Missouri)	3	SERC
					Ted Hilmes	KAMO Electric Cooperative	3	SERC
					Walter Kenyon	KAMO Electric Cooperative	1	SERC
					Stephen Pogue	M and A Electric Power Cooperative	3	SERC
					William Price	M and A Electric Power Cooperative	1	SERC
					Mark Ramsey	N.W. Electric Power Cooperative, Inc.	1	SERC
					Kevin White	Northeast Missouri Electric Power Cooperative	1	SERC
					Skyler Wiegmann	Northeast Missouri Electric Power Cooperative	3	SERC
					John Stickley	NW Electric Power Cooperative, Inc.	3	SERC
					Jeff Neas	Sho-Me Power Electric Cooperative	3	SERC
					Peter Dawson	Sho-Me Power Electric Cooperative	1	SERC

Seattle City Light	Paul Haase	1,3,4,5,6	WECC	Seattle City Light	Pawel Krupa	Seattle City Light	1	WECC
					Dana Wheelock	Seattle City Light	3	WECC
					Hao Li	Seattle City Light	4	WECC
					Mike Haynes	Seattle City Light	5	WECC
					Bud Freeman	Seattle City Light	6	WECC
					Paul Haase	Seattle City Light	1,3,4,5,6	WECC
					Ginette Lacasse	Seattle City Light	1,3,4,5,6	WECC
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	RSC no ISO-NE NYISO NextERA Con-Ed and HQ	Guy V. Zito	Northeast Power Coordinating Council	10	NPCC
					Randy MacDonald	New Brunswick Power	2	NPCC
					Wayne Sipperly	New York Power Authority	4	NPCC
					Glen Smith	Entergy Services	4	NPCC
					Brian Robinson	Utility Services	5	NPCC
					Bruce Metruck	New York Power Authority	6	NPCC
					Alan Adamson	New York State Reliability Council	7	NPCC
					Edward Bedder	Orange & Rockland Utilities	1	NPCC
					David Burke	Orange & Rockland Utilities	3	NPCC
					Michele Tondalo	UI	1	NPCC
					Laura Mcleod	NB Power	1	NPCC
					David Ramkalawan	Ontario Power Generation Inc.	5	NPCC

					Quintin Lee	Eversource Energy	1	NPCC
					Paul Malozewski	Hydro One Networks, Inc.	3	NPCC
					Helen Lainis	IESO	2	NPCC
					Sean Bodkin	Dominion - Dominion Resources, Inc.	6	NPCC
					Michael Schiavone	National Grid	1	NPCC
					Michael Jones	National Grid	3	NPCC
PSEG	Sean Cavote	1,3,5,6	NPCC,RF	PSEG REs	Tim Kucey	PSEG - PSEG Fossil LLC	5	NPCC
					Karla Barton	PSEG - PSEG Energy Resources and Trade LLC	6	RF
					Jeffrey Mueller	PSEG - Public Service Electric and Gas Co.	3	RF
					Joseph Smith	PSEG - Public Service Electric and Gas Co.	1	RF
Southwest Power Pool, Inc. (RTO)	Shannon Mickens	2	SPP RE	SPP Standards Review Group	Shannon Mickens	Southwest Power Pool Inc.	2	SPP RE
					Mike Buyce	City Utilities of Springfield	1,4	SPP RE
					Steven Keller	Southwest Power Pool Inc.	2	SPP RE
PPL - Louisville Gas and Electric Co.	Shelby Wade	3,5,6	RF,SERC	Louisville Gas and Electric Company and Kentucky Utilities Company	Charles Freibert	PPL - Louisville Gas and Electric Co.	3	SERC
					Dan Wilson	PPL - Louisville Gas and Electric Co.	5	SERC
					Linn Oelker	PPL - Louisville Gas and Electric Co.	6	SERC

1. Do you agree that the proposed change to the Cyber Asset definition makes it inclusive of both physical and virtual devices, including treatment of each virtual machine and hypervisor? If you do not agree, please provide rationale to support your position.

Joel Charlebois - AESI - Acumen Engineered Solutions International Inc. - 5

Answer	No
Document Name	

Comment

The proposed wording in the second sentence of the revised definition may still lead to some instances of inconsistent interpretation or application of the definition. It would be preferable to specifically use both of the terms “physical” and “virtual” in the second sentence, consistent with their use in the first sentence of the definition.

Suggested language for the second sentence: “Each virtual machine and physical host is a distinct device.”

Likes 0	
Dislikes 0	

Response

Richard Kinas - Orlando Utilities Commission - 3,5

Answer	No
Document Name	

Comment

- OUC has identified Concerns over the proposed definition to address virtual Cyber Assets including physical/hardware as many standards/requirements do not apply to a virtual device. For example, there are no physical i/o ports so the application of port locks (CIP-007-6 R1.2) does not exist in a virtual environment.
- The SDT should address the future proofing of the definition that will apply to all types of virtualized environments including storage, servers, switches, firewalls, routers, etc.
- The definition must take into consideration a virtual machine running on a virtual machine.
- The original terms “hardware, software and data” implied a physical device, with hardware and data residing within it. Within a virtual environment, the Virtual hosts (at the physical threshold) will be comprised of “hardware, software and data” while the virtual guests will be comprised of “software and data” however they may or may not be comprised of hardware. Virtual hosts not existing at the physical threshold may or may have physical aspects.
- We suggest that a different type of Cyber System be identified within the standards to address all infrastructure required to run the BES Cyber Asset/BES Cyber System in a virtual environment. We considered that the hypervisor becomes more impactful and may need even higher level of security controls. The BES Cyber System would continue to be those BCS that perform control & operation of the BES.
- If a follow-on sentence must be included in a definition, then the definition is not sufficient.
- If the second sentence must be retained then the clarification should make it clear that a virtual machine is by definition a Cyber Asset and not just a distinct device. However Hypervisors by their unique functioning, must include additional baseline information to ensure that the “entire system” remains stable, such as configuration information related to partitioning hardware, etc. used to prevent resource starvation.
- The requirement around baseline information is different between virtual hosts (infrastructure) and virtual guest/physical guests (BES Cyber Assets/Systems). With virtual hosts configuration information is critical and must be monitored to ensure that risks specific to virtual environments such as resource starvation are not modified without knowledge.

Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	No
Document Name	
Comment	
The criteria or additional clarification for ”programmable” should be detailed in this definition.	
Likes 0	
Dislikes 0	
Response	
Brandon McCormick - Florida Municipal Power Agency - 3,4,5,6 - FRCC, Group Name FMPA	
Answer	No
Document Name	2016-02_Virtualization_Unofficial Comment Form_FMPA_comments.docx
Comment	
Please see attached comments	
Likes 0	
Dislikes 0	
Response	
Robert Ganley - Long Island Power Authority - 1	
Answer	No
Document Name	
Comment	
The interchanged use of the word Virtual Machine vs. Virtual Device can be misleading. The definition should be consistent for clarity.	

Cyber Asset: A programmable electronic physical device or virtual machine, including the hardware, software, and data in the device or asset. Each physical host and each virtual machine are considered distinct Cyber Assets.	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
CenterPoint Energy Houston Electric, LLC ("CenterPoint Energy") does not agree with the proposed change to the Cyber Asset definition. The current definition covers virtual machines. Additionally, using the term "virtual device" without a corresponding definition may unintentionally broaden the scope of applicability. For example, it is not clear whether a container would be considered a "virtual device" alongside a virtual machine or a virtual local area network.	
Likes 0	
Dislikes 0	
Response	
Don Schmit - Nebraska Public Power District - 1,3,5	
Answer	No
Document Name	
Comment	
We agree with the comments submitted by the APPA.	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	

Comment	
N&ST supports the intent of the proposed change but believes the revised definition needs more clarity, particularly with regard to the word, “host.” Suggested wording: ”A programmable electronic physical or virtual device, including the hardware, software, and data in the device. Each virtual device, commonly referred to as a virtual machine, and the underlying hardware and operating system that serve as the host for one or more such virtual machines are to be considered distinct Cyber Assets."	
Likes 0	
Dislikes 0	
Response	
Chantal Mazza - Hydro-Qu?bec TransEnergie - 2 - NPCC	
Answer	No
Document Name	
Comment	
Request clarification on the term ”host” and how it relates to hypervisor. Consider removing this last sentence (Each virtual machine and host is a distinct device.) and move into the guidance.	
Likes 0	
Dislikes 0	
Response	
John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	No
Document Name	
Comment	
Tacoma Power supports comments submitted by APPA.	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	No
Document Name	

Comment

APPA does not agree that the proposed change is inclusive and believes that there is a better way to include both physical and virtual devices. Therefore, public power proposes the following:

“Programmable electronic devices, including the hardware, software, and data in those devices.
Virtualized systems or devices are distinct devices.”

This proposed change would help in “future-proofing” the definition.

Likes 0	
Dislikes 0	

Response

David Francis - Midcontinent ISO, Inc. - 2,3 - MRO,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG

Answer	No
Document Name	

Comment

The SWG offers the following comments.

- The original definition does not exclude the use of virtualization, therefore it should be read to be inclusive of virtual systems. This is supported by the ***Security Guideline for the Electricity Sector: Identifying Critical Cyber Assets*** published in 2010. It states that Cyber Assets to be considered under CIP-002-1 include, at a minimum, “hardware platforms running virtual machines or virtual storage”.
- The addition of “physical or virtual” does not add clarity to the definition.
- The question uses the term “hypervisor”, but the definition uses “host”. Please ensure consistency of the terms. Hypervisor is the more commonly understood term.
- If the SDT is determined to revise the definition in this manner, we recommend “Each virtual machine and each host is a distinct and separate device” to provide more clarity about the treatment of each guest and host.
- ERO-endorsed implementation guidance would be a more appropriate means to address the treatment of the hardware, software, and data and provide examples of implementation.
- Virtual system cannot be categorized as “electronic” due to the fact that they have no measureable electronic output. Virtual systems simply mimic an electronic device.

Likes 0	
Dislikes 0	

Response

Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs

Answer	No
Document Name	
Comment	
The interchanged use of the word Virtual Machine vs. Virtual Device can be misleading. The definition should be consistent for clarity. Cyber Asset: A programmable electronic physical device or virtual machine, including the hardware, software, and data in the device or asset. Each physical host and each virtual machine are considered distinct Cyber Assets.	
Likes 0	
Dislikes 0	
Response	
Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - FRCC,MRO,WECC,Texas RE,SERC,SPP RE, Group Name Southern Company	
Answer	No
Document Name	
Comment	
In a VDI environment, there may be no persistent virtual device; in some cases, only an image may exist that is then spun up at the point in time it is needed. Given the definition above, all programmable electronic devices consisting of a virtualized host would be classified as a Cyber Asset, regardless of the persistence of a virtual machine on the host that may or may not be used in the context of Applicable System. The asset hosting the virtualized host would be, itself, a completely separate Cyber Asset. Consider changing this part of the proposed definition “Each virtual machine and host is a distinct device.” to read “Each virtual device is distinct from it’s host(ing) device.”	
Likes 0	
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
ERCOT signs on to the SRC comments and provides the following additional descriptive detail on the SRC’s comments, as well as responses for Questions #18 and #20. ERCOT does not see the value of modifying the definition of Cyber Asset as noted in the comment form. The addition of the words “physical or virtual” does not add clarity to the definition. Virtual systems cannot be categorized as “electronic” due to the fact that they have no measureable electronic output. Virtual systems simply mimic an electronic device. ERCOT also notes that the current approved definition does not exclude the use of	

virtualization, therefore it should be read to be inclusive of virtual systems. This is supported by the ***Security Guideline for the Electricity Sector: Identifying Critical Cyber Assets*** published in 2010. It states that Cyber Assets to be considered under CIP-002-1 include, at a minimum, “hardware platforms running virtual machines or virtual storage”.

In lieu of modifications to the definition of Cyber Asset, ERCOT recommends ERO-endorsed implementation guidance as a more appropriate means to address the treatment of the hardware, software, and data comprising a virtual Cyber Assets. ERCOT recommends drafting of examples of implementation through such guidance. Examples will aid industry in understanding the ways that virtual technologies can be implemented in a complaint manner.

Although we do not support modifications to the definition, if the SDT is determined to revise the definition in this manner ERCOT requests that the SDT ensure consistency of the terms. The question uses the term “hypervisor”, but the definition uses “host”. Hypervisor is the more commonly understood term, rather than host. We recommend the language be modified as, “Each virtual machine and each host is a distinct and separate device” to provide more clarity about the treatment of each guest and host.

Likes 0	
Dislikes 0	

Response

Wendy Center - U.S. Bureau of Reclamation - 1,5

Answer	No
Document Name	

Comment

Reclamation recommends the proposed definition of Cyber Asset be changed:

from: A programmable electronic physical or virtual device, including the hardware, software, and data in the device

to: A microprocessor-based device, including the hardware and software in the device, that is programmable by the end user or contains firmware/BIOS that is updatable by the end user in the field.

Inclusions:

1. Devices that can be “flash” updated by end user personnel, such as programmable logic controllers, distributed control system controllers, and other similar devices.

2. Virtual Machines

3. Workstations

4. Servers

Reclamation also recommends adding the following terms to the NERC Glossary of Terms:

Virtual Machine (VM) – An operating system (OS) or application environment that is installed on software, which imitates dedicated hardware. Each Virtual Machine is a distinct Cyber Asset on the Host Machine.

Host Machine – A physical Cyber Asset used to run one or more Virtual Machines.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE

Answer	No
Document Name	

Comment

The proposed Cyber Asset definition:

Adds Implementation and Compliance Complexity. The following terms, incorporated into the definition, are ambiguous and will necessitate creating additional glossary terms:

- virtual device,
- virtual machine, and
- virtual host.

Creates uncertainty that increases the opportunity for unintended negative consequences. For example, it is unclear if the proposed network virtualization definition establishes a scenario where VLAN on a switch becomes its own virtual device.

If the SDT concludes action is necessary, please consider the following:

A programmable electronic physical or virtual devices, including the hardware, software, and data in those devices. Each virtual machine and host is a distinct device.

Likes 0	
Dislikes 0	

Response

Ronald Donahey - TECO - Tampa Electric Co. - 1,3,5,6

Answer	No
Document Name	

Comment

- TEC has identified concerns over the proposed definition to address virtual Cyber Assets including physical/hardware as many standards/requirements do not apply to a virtual device. For example, there are no physical i/o ports so the application of port locks (CIP-007-6 R1.2) does not exist in a virtual environment. The definition must take into consideration a virtual machine running on a virtual machine.
- The original terms “hardware, software and data” implied a physical device, with hardware and data residing within it. Within a virtual environment, the Virtual hosts (at the physical threshold) will be comprised of “hardware, software and data” while the virtual guests will be comprised of “software and data” however they may or may not be comprised of hardware. Virtual hosts not existing at the physical threshold may or may have physical aspects.
- If a follow-on sentence must be included in a definition, then the definition is not sufficient.
- If the second sentence must be retained then the clarification should make it clear that a virtual machine is by definition a Cyber Asset and not just a distinct device. However Hypervisors by their unique functioning, must include additional baseline information to ensure that the “entire system” remains stable, such as configuration information related to partitioning hardware, etc. used to prevent resource starvation.
- The SDT should address the future proofing of the definition that will apply to all types of virtualized environments including storage, servers, switches, firewalls, routers, etc.
- We suggest that a different type of Cyber System be identified within the standards to address all infrastructure required to run the BES Cyber Asset/BES Cyber System in a virtual environment. We considered that the hypervisor becomes more impactful and may need even higher level of security controls. The BES Cyber System would continue to be those BCS that perform control & operation of the BES.
- The requirement around baseline information is different between virtual hosts (infrastructure) and virtual guest/physical guests (BES Cyber Assets/Systems). With virtual hosts configuration information is critical and must be monitored to ensure that risks specific to virtual environments such as resource starvation are not modified without knowledge.

Likes 0

Dislikes 0

Response

Paul Haase - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light

Answer	No
Document Name	

Comment

Seattle City Light appreciates the efforts of the SDT to tackle this difficult question, and agrees with concept of the change. However, City Light is concerned about details fo the definition. As such, City Light support APPA's comments about the proposed new Cyber Asset definition.

Likes 0

Dislikes 0

Response

Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC

Answer	No
Document Name	
Comment	
Definition does not use appropriate terminology such as host and guest. Consider addressing each virtual machine as a distinct asset instead of a ‘device’.	
Likes 0	
Dislikes 0	
Response	
Daniel Grinkevich - Con Ed - Consolidated Edison Co. of New York - 1,3,5,6	
Answer	No
Document Name	
Comment	
The current definition already addresses both virtual and physical assets.	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	

Comment

Yes, the proposed change to the Cyber Asset definition makes it inclusive of both physical and virtual “devices,” but the proposed change introduces new problems for compliance.

One use of virtualization that has been observed in the field is in the area of virtual desktops for Control Center operator consoles. In the observed case, a “base image” is instantiated each time a user logs in, thus giving each user a fresh system for each shift. The base image is kept up to date as required by CIP-007-6, etc. Because the Cyber Asset is considered to be the physical device on which the virtualization software runs, the changes effected by each new instance of the base image are simply data changes that are logged by log in/log out monitoring. If each new instance is required to be treated as a new Cyber Asset, per the proposed definition, then each individual instance must be documented with baselines (CIP-010-2 R1), an active vulnerability assessment (CIP-010-2 R3 Part 3.3), etc. This will prove unworkable.

The present definition permits wide flexibility in the use of virtualization technologies for BES Cyber Systems, EACMS, and PACS, as long as each VM is protected at the same level as the hardware device it is capable of running on.

Likes 0	
Dislikes 0	

Response

Russell Noble - Cowlitz County PUD - 3,5

Answer	Yes
Document Name	

Comment

Cowlitz PUD agrees the proposed Cyber Asset definition will be inclusive. However, it may be over inclusive of devices that are not vulnerable to “network or internet” remote access. We believe the generic definition of “cyber” currently identifies computer based electronic devices that execute program instructions (code) from a memory medium, of which is living in an environment that allows modification via code execution. Electronic devices requiring physical manipulation, such as contact connections or replacement of hardware, to modify or replacement for upgrade should be excluded as they are not subject to circular code on code modification. The term “programmable electronic device” is subject to future definitional changes, and results in uncertain compliance interpretations. In agreement with APPA’s comment, we believe the definition of Cyber Asset should be restricted to a distinct virtual ***entity*** or physical device.

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	
TVA requests the SDT consider removing the sentence “Each virtual machine and host is a distinct device.” The term “virtual machine” carries significant connotations and potential for confusion. For example, a virtualized network switch may not be called a virtual machine, it may be a virtual router instance, virtual firewall instance, or a virtual device context. Each are somewhat analogous to the term virtual machine. However, calling out virtual machine specifically may hinder understanding.	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
BPA agrees that the proposed change to the Cyber Asset definition makes it inclusive of physical and virtual devices. However, the term *programmable electronic device* is NERC specific and not relevant to Cyber Security definitions in broader industry. Continued use of the term is unnecessary.	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	
The SPP Standards Review Group would suggest that the drafting team provides clarity on the term “host” that’s associated with the proposed definition. At this point, there is some confusion about the applicability on how the term could be used. Question: If a registered entity has a server farm, how would a host be defined in that particular situation?	
Likes 0	
Dislikes 0	
Response	

Aaron Austin - AEP - 3,5	
Answer	Yes
Document Name	
Comment	
AEP believes the proposed definition provides an applicability umbrella that enables responsible entities to scope their obligations effectively. But request that if “host” and “hypervisor” are synonymous terms, that a clarification be added to the definition or compliance guidance.	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Alliant Energy agrees, assuming that "host" is equal to "hypervisor." We also have a general request that terms are used consistently throughout the requirements, definitions, and rationale/guidance. The definition of "Cyber Asset" should clarify what is meant by "host" - the question refers to "virtual machine and hypervisor" but the definition refers to "virtual machine and host." The second sentence of the definition should be clarified as to whether the virtual machine and hypervisor are different entities. Unless these updates are aimed specifically for hypervisors, we suggest avoiding using that specific terminology and instead suggest to use a more generic reference like "mulit-instance OS."	
Likes 0	
Dislikes 0	
Response	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
“Host” is inherently obvious: It supports one or more virtualized components. “Hypervisor” is the ambiguous, implementation specific term that should not be used. Suggest that use of the term “hypervisor” be entirely avoided.	

Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Downey - Peak Reliability - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Janis Weddle - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Chelan PUD	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bob Case - Black Hills Corporation - 1 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4, Group Name FirstEnergy Corporation	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shelby Wade - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lauren Price - ATCO Electric - 1 - MRO,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8,9 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Tolo - Unisource - Tucson Electric Power Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE would like to clarify that the virtual machine and host are one Cyber Asset as the virtual machine cannot operate without the host machine. This shared relationship means that neither can be separate Cyber Assets. For example, if a virtual machine has been identified as a BES Cyber Asset (BCA); the host machine that runs the virtual machine is also a BCA; which also applies to PACS, EACMS, and PCAs. Texas RE is concerned that treating the virtual machine and its host as separate Cyber Assets can cause mixed-trust virtual environments; the host runs CIP and corporate virtual machines. CIP controls are only being applied to the CIP virtual machine and not its host; even though the host "*if rendered unavailable, degraded, or misused*" can impact the CIP and corporate virtual machines.	
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 ISO-NE NYISO NextERA Con-Ed and HQ	
Answer	
Document Name	
Comment	

No consensus Request clarification on the term ”host” and how it relates to hypervisor. Consider removing this last sentence (Each virtual machine and host is a distinct device.) and move into the guidance	
Likes 0	
Dislikes 0	
Response	

2. Do you agree that the term programmable in the Cyber Asset definition does not need further clarification at this time? If yes, please provide rationale to support your position.

Paul Haase - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light	
Answer	No
Document Name	
Comment	
City Light believes programmable should be clarified to clearly differentiate between configurable hardware (which was not envisioned to be in scope in the original CIP v5 or in the never-published NERC guidance, and should be in scope now) and devices that execute easily modified instructions. The risks presented by configurable hardware are much less than those from truly programmable devices, and they should not be lumped together.	
Likes 0	
Dislikes 0	
Response	
Ronald Donahey - TECO - Tampa Electric Co. - 1,3,5,6	
Answer	No
Document Name	
Comment	
• Since it is the configuration of the Virtual Hosts software that implements many of the security controls that will be implemented in a virtual environment, for Virtual Hosts it is more important to identify the configuration as opposed to the programmability as the defining criteria.	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	
Reclamation recommends that any clarification of the term programmable be contained within the definition of Cyber Asset. Refer to the recommended definition of Cyber Asset in the response to Question 1.	
Likes 0	

Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
Comments: As noted in question 1, ERCOT does not support modifying the definition of Cyber Asset unless a modification to address “programmable” provides clarity to address risk and aids in cyber asset identification across all entities. There is a risk of inconsistency of definition across the industry if the term is not defined. If there is not an ERO-wide benefit, it should remain up to the entity to define the term for their own purposes. Implementation guidance should not be used to define a term. It is an illustration of a way to comply. This is fundamentally different from the authoritative purpose of a definition. Implementation guidance should not be used to define the scope of the assets as a foundation of a standard.	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	No
Document Name	
Comment	
Comments: While we believe we know what a programmable device is in the sense of those devices that could be modified with malware, or which should have change control around upgrade processes, we still wouldn't mind greater clarity to assure there is no misinterpretation as to what is in scope for compliance.	
Likes 0	
Dislikes 0	
Response	
Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	No
Document Name	
Comment	

The definition of the word programmable means a device is capable of being programed via electronic code or configuration changes. A dip switch should not consider an electronic programmable device since a physical action is required to change the setting. However, there may be critical devices/equipment that are considered Non-programmable but can have an adverse effect on the a BES Cyber System (i.e. Net Gear –Non-managed Switches, or similar).	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	No
Document Name	
Comment	
Texas RE recommends clarifying the definition by adding a description for programmable: "*A programmable (able to be provided with coded instructions) electronic device (physical or virtual), including the hardware, software, and data in those devices*."	
Likes 0	
Dislikes 0	
Response	
David Francis - Midcontinent ISO, Inc. - 2,3 - MRO,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG	
Answer	No
Document Name	
Comment	
• Programmable should be defined if it provides clarity of risk and aids in cyber asset identification across all entities. It not, it can be up to the entity to define it for their own purposes. There is a risk of inconsistency of definition across the industry if the term is not defined. • Implementation guidance should not be used to define a term. It is an illustration of a way to comply. This is fundamentally different from the authoritative purpose of a definition. Implementation guidance should not be used to define the scope of the assets as a foundation of a standard.	
Likes 0	
Dislikes 0	
Response	

Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
Duke Energy requests clarification as to what “data” should be evaluated. The drafting team should consider inserting the term “configuration” in front of the word “data” which we feel would clear up some ambiguity.	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
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	No
Document Name	
Comment	
TVA requests additional clarity for the term “programmable”; The ERO Enterprise-endorsed guidance does not sufficiently resolve issues with the term programmable.	
Likes 0	
Dislikes 0	
Response	
Don Schmit - Nebraska Public Power District - 1,3,5	

Answer	No
Document Name	
Comment	
The lack of a definition can lead to either over or under classification of devices. It is currently up to the entity to decide. Auditors may have a different definition which can lead to a violation and devices unprotected for a period of time. Lack of a NERC definition can lead to inconsistencies between Regional Entities.	
Likes 0	
Dislikes 0	
Response	
Robert Ganley - Long Island Power Authority - 1	
Answer	No
Document Name	
Comment	
The definition of the word programmable means a device is capable of being programed via electronic code or configuration changes. A dip switch should not consider an electronic programmable device since a physical action is required to change the setting. However, there may be critical devices/equipment that are considered Non-programmable but can have an adverse effect on the a BES Cyber System (i.e. Net Gear –Non-managed Switches, or similar)	
Likes 0	
Dislikes 0	
Response	
Bob Case - Black Hills Corporation - 1 - WECC	
Answer	No
Document Name	
Comment	
Need to differentiate physical configurability, from electronically programmable.	
Likes 0	
Dislikes 0	
Response	

Janis Weddle - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Chelan PUD	
Answer	No
Document Name	
Comment	
There is still a gray area where it is questionable on whether a device is programmable or not. Most would agree a device that is configured by DIP switches is not programmable. But functionally, a device that takes settings via software, but has no field-changeable executable code is no different, and it is unclear if such a device would be considered “programmable”. Another area of question would be live OS virtual machines. These devices are read-only and the executable code cannot be altered.	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	No
Document Name	
Comment	
Given that currently most responsible entities have their own interpretation about programmable, pleased detail what "programmable" means in the Cyber Asset definition.	
Likes 0	
Dislikes 0	
Response	
Richard Kinas - Orlando Utilities Commission - 3,5	
Answer	No
Document Name	
Comment	
• There are concerns that without definition of programmable, the scope of standards may be expanded to devices that do not meet the qualifications of BES Cyber Assets. • Since it is the configuration of the Virtual Hosts software that implements many of the security controls that will be implemented in a virtual environment, for Virtual Hosts it is more important to identify the configuration "configurable" as opposed to the programmability as the defining criteria.	
Likes 0	
Dislikes 0	

Response

Joel Charlebois - AESI - Acumen Engineered Solutions International Inc. - 5

Answer	No
Document Name	

Comment

There are a few varying interpretations of the term programmable being used by the industry. Even the referenced ERO Enterprise-endorsed Implementation Guidance which is a Lessons Learned document, indicates that different Entities were interpreting the term differently. Also, the ERO Enterprise-endorsed Implementation Guidance, as the reference suggests, is meant as guidance, and not meant to be the only way to be compliant.

In addition, Entities who fail to document their own definition of programmable in their BES Cyber System Categorization process or methodology, and even Entities who do document their own definition of programmable, are subject to auditor interpretation of the term, which can be different than the Entity’s interpretation.

Likes 0	
Dislikes 0	

Response

Teresa Cantwell - Lower Colorado River Authority - 1,5

Answer	No
Document Name	

Comment

Does “programmable” mean the ability to run custom code and the ability to make pre-defined configuration changes? Or does the ability to make configuration changes only fit the meaning of “programmable”? Please provide language clarifying electronically programmable language (e.g. not changes via dip switches).

Likes 0	
Dislikes 0	

Response

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group

Answer	No
Document Name	

Comment

Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4, Group Name FirstEnergy Corporation	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3,5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Daniel Grinkevich - Con Ed - Consolidated Edison Co. of New York - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
No comment.	
Likes 0	
Dislikes 0	
Response	

Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE	
Answer	Yes
Document Name	
Comment	
The term “programmable” in the Cyber Asset definition does not need further clarification. The ERO endorsed Implementation Guidance clarifies the intent by explaining the various capability attributes that should be used to determine programmability.	
Likes 0	
Dislikes 0	
Response	

Aaron Austin - AEP - 3,5	
Answer	Yes
Document Name	
Comment	
AEP believes the current definition and the proposed definition allow entities to define “Programmable” for their context. It provides flexibility for asset identification.	
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 ISO-NE NYISO NextERA Con-Ed and HQ	
Answer	Yes
Document Name	
Comment	
Some entities have built their own definition of “programmable” into their compliance program. A NERC term that varies from their definition could have significant impact on their compliance program. Since this is a hypothetical scenario, it is impossible to know if the impact would be to add or remove BES CA’s. Therefore, it is also impossible to know if this would negatively or positively impact cyber security.	
Likes 0	
Dislikes 0	
Response	

Lauren Price - ATCO Electric - 1 - MRO,RF	
Answer	Yes
Document Name	
Comment	
ATC agrees that the term programmable in the Cyber Asset definition does not need further clarification at this time based on the following rationale. ATC closely monitored the SDT's prior attempts to define and provide guidance on this term. In addition, during earlier revisions to the standards, the SDT's formal responses to previous comments about this term have provided ATC adequate visibility into, and understanding of, the SDT's intent for the term. ATC had leveraged available information and guidance to formulate a methodology that assures programmable devices are considered for evaluation, and we have been able to provide clarity within our implementation through the use of our internally defined the term(s) Electronically Programmable and Mechanically Configurable. This approach provides our Subject Matter Experts with a uniform understanding of the term programmable that is consistent with the SDT's intent for the term thereby obviating the need for the SDT to further clarify it within the regulation.	
Likes 0	
Dislikes 0	
Response	
Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - FRCC,MRO,WECC,Texas RE,SERC,SPP RE, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern agrees, given the ERO Enterprise-endorsed Implementation Guidance that exists on the term "programmable", that the flexibility currently given Responsible Entities to internally evaluate and defend asset capabilities against the defined term provides adequate clarification at this time.	
Likes 0	
Dislikes 0	
Response	
Shelby Wade - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company	
Answer	Yes
Document Name	
Comment	

While there can still be some confusion on the term programmable, the guidance document provides the needed information.	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
AZPS agrees that the term programmable in the Cyber Asset definition does not need further clarification at this time. AZPS supports the revision of the definition to specifically address physical and virtual devices.	
Likes 0	
Dislikes 0	
Response	
Chantal Mazza - Hydro-Qu?bec TransEnergie - 2 - NPCC	
Answer	Yes
Document Name	
Comment	
Some entities have built their own definition of “programmable” into their compliance program. A NERC term that varies from their definition could have significant impact on their compliance program. Since this is a hypothetical scenario, it is impossible to know if the impact would be to add or remove BES CA’s. Therefore, it is also impossible to know if this would negatively or positively impact cyber security.	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	

There is existing guidance on the term programmable; therefore, there is no further need to clarify the term at this time.	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
The definition of “programmable electronic device” by the examples in the BES Cyber Assets Lessons Learned document is sufficient to mitigate most of the risk posed by the devices in question. Additional fine-tuning of devices not identified as BES Cyber Assets can be accomplished on a case-by-case basis by audit teams in the field.	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
N/A	
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	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Tolo - Unisource - Tucson Electric Power Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8,9 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brandon McCormick - Florida Municipal Power Agency - 3,4,5,6 - FRCC, Group Name FMPA	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Downey - Peak Reliability - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	
Document Name	
Comment	
No comment at this time	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	

Answer	
Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	

3. If programmable does need further clarification, how would you prefer it to be addressed? Use comments to detail necessary definition changes or guidance that could be developed.	
Teresa Cantwell - Lower Colorado River Authority - 1,5	
Answer	
Document Name	
Comment	
Definition in Glossary. Distinction between providing parameters vs selecting pre-configured options - clarification between programmable and configurable.	
Likes 0	
Dislikes 0	
Response	
Joel Charlebois - AESI - Acumen Engineered Solutions International Inc. - 5	
Answer	
Document Name	
Comment	
As there are still varying interpretations of the term programmable, and the ERO Enterprise-endorsed Implementation Guidance is simply meant as guidance and not the only way to be compliant, there should be a NERC defined glossary term established and industry accepted definition for programmable	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	

Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Richard Kinas - Orlando Utilities Commission - 3,5	
Answer	
Document Name	
Comment	
I would suggest that a separate definition is created to address infrastructure. With Infrastructure identifying configuration as opposed to programmability as criteria. If infrastructure is associated with BES Cyber Assets and could impact the BES Cyber Asset 15minute test then it must be identified and protected.	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	
Document Name	
Comment	
We suggest adding the following wording in the definition: “A programmable device means an electronic device with a microprocessor-based circuit board, and an operating system or firmware, where an I/O port is used for programming the device. DIP switches do not qualify as an I/O port.”	
Likes 0	

Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	
Janis Weddle - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Chelan PUD	
Answer	
Document Name	
Comment	
The term programmable needs to be removed and a more specific phrase needs to be used to clarify the boundary between non-Cyber Assets and Cyber Assets.	
Likes 0	
Dislikes 0	
Response	
Bob Case - Black Hills Corporation - 1 - WECC	
Answer	
Document Name	
Comment	
Need to differentiate physical configurability, from electronically programmable.	
Likes 0	
Dislikes 0	
Response	

Russell Noble - Cowlitz County PUD - 3,5

Answer	
Document Name	

Comment

Cowlitz PUD agrees in part with BPA that the term programmable should be retired. We differ in that the definitional objective is not clear. We believe there are four concepts requiring clear identification: A computational device or entity that:

1. Autonomously reads code assembled into a set of instructions (a program) to process data;
2. Uses a memory medium to contain the code and data using read and write actions;
3. Communicates with like or similar devices to exchange code and/or data;
4. And, installs and modifies its programs by executing a program.

Concerning "virtual devices," we believe this to be confusing. Rather, we propose BPA's use of "entity" or "virtual machine" Thus, a Cyber Asset is a “discrete device” that is contained within a physical cabinet with visible ports, or a discrete ***virtual entity or machine*** with hidden virtual ports logically contained in a "discrete device." Further, we are not confident that guidance is sufficient to convey the above in a manner that protects stakeholders from contrary audit standard requirement interpretation.

Likes 0	
Dislikes 0	

Response

Robert Ganley - Long Island Power Authority - 1

Answer	
Document Name	

Comment

The definition should be inclusive of programmable and non-programmable in order to capture all cyber assets that can impact the BES CS’s.

Likes 0	
Dislikes 0	

Response

Don Schmit - Nebraska Public Power District - 1,3,5

Answer	
Document Name	

Comment

We recommend a definition that the device meets all of the criteria below:

- A device that has a microprocessor and field-updateable firmware or software.
  - “Field-Updatable” would include devices that have a management port, web interface, or any external interface that would allow the introduction of a firmware, software or logic update.
  - If the device’s case is sealed in such a way that would require it to be damaged to gain access to the chipset or internal ports then the device is to be considered to be not Field-Updatable.

Likes 0	
Dislikes 0	

Response

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

Answer	
Document Name	

Comment

TVA requests the SDT clarify the intent as requested by the V5 TAG.

Likes 0	
Dislikes 0	

Response

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

Answer	
Document Name	

Comment

BPA believes that industry understands the term programmable as described in SDT Considerations for V5 Posting: “an electronic device which can execute a sequence of instructions loaded to it through software or firmware, and configuration of an electronic device is included in programmable.” The capability of being modified exists for every independent executable entity such as virtual machines or hypervisor hosts. Associated controls to prevent unauthorized or unintended modification apply to all independent executable entities because vulnerabilities may exist in either entity and are not reduced without protecting both individually.

Likes 0	
Dislikes 0	

Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	
Document Name	
Comment	
Duke Energy agrees that additional clarity is needed. The guidance document referenced by the SDT above, does not provide the necessary clarity on this topic. Perhaps a guideline document specific to the concept/term programmable would be beneficial.	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4, Group Name FirstEnergy Corporation	
Answer	
Document Name	
Comment	
Recommend that a clear definition be established similar to the following: Programmable Electronic Device (PED) – A device that has a microprocessor and firmware or updateable software, which can be altered via a management port, web interface or any other external interface. A device that does not allow its internal programing to be changed, but allows a user to change between pre-defined operational parameters is considered a configurable device and not a Programmable Electronic Device.	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	
Document Name	
Comment	
The SPP Standards Review Group has a concern that the term “programmable” has not been clearly defined. From our perspective, it is unclear since there is no defined term in the NERC Glossary officially referencing “programmable”. At this point, we’re not sure if the intent is to leave the term open	

and let all entities define the term in their internal programs or there is another direction the drafting team would like to go. Either way, we would like the drafting team to provide some clarity on the intent for the term.	
Likes 0	
Dislikes 0	
Response	
David Francis - Midcontinent ISO, Inc. - 2,3 - MRO,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG	
Answer	
Document Name	
Comment	
The context included in the reference compliance guidance would be a good starting place. Consider scoping to those devices that; (1) have a microprocessor, (2) can accept firmware, software or logic, and (3) have a physical or wireless port or a web interface that can be used to “flash” firmware	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Please see Texas RE’s answer to #2.	
Likes 0	
Dislikes 0	
Response	
Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	
Document Name	
Comment	

The definition should be inclusive of programmable and non-programmable in order to capture all cyber assets that can impact the BES CS's.	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	
Document Name	
Comment	
Comments: A document addressing the proper use of criteria mentioned. Specifically, "factors as whether a device is merely configurable, its executable code is not field upgradable, or if its functionality can only be changed via physical DIP switches, swapping internal chips, etc."	
Likes 0	
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	
Document Name	
Comment	
As noted in question 1, ERCOT does not support modifying the definition of Cyber Asset. However, if the SDT does determine that a modification is needed, the context included in the reference compliance guidance would be a good starting place. Consider scoping to those devices that; (1) have a microprocessor, (2) can accept firmware, software or logic, and (3) have a physical or wireless port or a web interface that can be used to "flash" firmware.	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 1,5	
Answer	
Document Name	
Comment	

Reclamation recommends that any clarification of the term programmable be contained within the definition of Cyber Asset. Refer to the recommended definition of Cyber Asset in the response to Question 1.	
Likes 0	
Dislikes 0	
Response	
Lauren Price - ATCO Electric - 1 - MRO,RF	
Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 3,5	
Answer	
Document Name	
Comment	
AEP believes no further clarification of “programmable” is needed.	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8,9 - WECC	
Answer	
Document Name	
Comment	
No comments from SDG&E at this time.	

Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE	
Answer	
Document Name	
Comment	
Not Applicable.	
Likes 0	
Dislikes 0	
Response	
Ronald Donahey - TECO - Tampa Electric Co. - 1,3,5,6	
Answer	
Document Name	
Comment	
TEC would suggest that a separate definition is created to address infrastructure, with Infrastructure identifying configuration as opposed to programmability as criteria. If infrastructure is associated with BES Cyber Assets and could impact the BES Cyber Asset 15 minute test then it must be identified and protected.	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	
Document Name	
Comment	
No comment at this time	
Likes 0	

Dislikes 0	
Response	
Paul Haase - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light	
Answer	
Document Name	
Comment	
see response to question 2, above	
Likes 0	
Dislikes 0	
Response	
Daniel Grinkevich - Con Ed - Consolidated Edison Co. of New York - 1,3,5,6	
Answer	
Document Name	
Comment	
No comment.	
Likes 0	
Dislikes 0	
Response	

4. Do you agree with the proposed definition of Centralized Management Systems (CMS)? If not, please provide rationale to support your position.

Paul Haase - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light

Answer	No
Document Name	

Comment

City Light supports the concept of identifying and defining CMS, but is concerned about the details and possible unintended consequences of the proposed definition. City Light supports APPA's comments to this question. Alternatively, if the proposed definition is prefered by the SDT, City Light recommends that it be modified to apply to virtualized systems, as follows:

CMS: A system used for administration or configuration of VIRTUALIZED BES Cyber System(s) through which the configuration of the VIRTUAL BES Cyber System(s) can be altered. (new words in CAPS; deleted 2nd word "centralized" as unnecessary)

Likes 0	
Dislikes 0	

Response

Ronald Donahey - TECO - Tampa Electric Co. - 1,3,5,6

Answer	No
Document Name	

Comment

The current proposed definition is too ambiguous and will pull in unintended systems and potential classification of a device as both an EACM and a CMS.

The definition as proposed should be revised to only include the administration of the BES Cyber System. The current definition may expand the scope to other tools with unintended consequences. TEC suggests that the definition of CMS needs to follow the format of other Glossary Terms by referring to the configuration of BES Cyber Assets instead of BES Cyber Systems

We envision that there will either be new requirements around CMS or adding them to other requirements/parts. Our efforts here must be to protect the right devices/systems and improve the reliable/secure operation of the BES. As indicated in question 1 above, we suggest that the shared components and shared infrastructure may need different defined terms than BES Cyber System.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE

Answer	No
Document Name	

Comment

KCP&L does not support the proposed Centralized Management Systems (CMS) definition for the following reasons:

Definition is Unnecessary. Introducing a new designation for this class of devices is unnecessary.

Overly Burdensome Implementation. The company’s analysis estimates it will take thousands of hours to review, update documentation with references to CMS assets, and to develop the related processes and procedures.

Alternative. If the SDT concludes the proposed definition is required to address the identified issues, an alternative approach is to modify the existing definition of EACMS to include management systems like those considered in the proposed CMS definition. The approach provides a simpler compliance view by not creating a new class of devices.

Likes 0	
Dislikes 0	

Response

Aaron Austin - AEP - 3,5

Answer	No
Document Name	

Comment

AEP suggests that, at most, the existing definition for EACMS be modified to incorporate “CMS” functions. The CMS definition allows the benefits of (1) the CMS to be within the ESP (Transmission’s current implementation) and (2) applying the CMS definition to other appropriate devices (e.g. Domain Controllers or McAfee EPO).

Likes 0	
Dislikes 0	

Response

Lauren Price - ATCO Electric - 1 - MRO,RF

Answer	No
Document Name	

Comment

ATC requests further consideration of the use and applicability of this term as it relates to other existing categories of Cyber Assets under purview of the Standards today, as well as those extrapolated categories of EACMS proposed later in this concept/comment form. For the below reasons, ATC does not agree with the proposed definition:

1. It is unclear if the proposed CMS definition is intentionally silent to systems used for administration or configuration of Electronic Access Control and Monitoring Systems (EACMS) or Physical Access Control Systems (PACS)? Does this infer that EACMS and PACS cannot be virtualized? Where EACMS and PACS are virtualized, is an associated CMS to be identified and protected?
2. In addition, the creation of a newly defined term increases the number of Cyber Asset classification categories, thereby creating the potential for a given Cyber Asset to have yet another categorization. Careful consideration must be given to the controls applicable to each category so as to assure they are not at odds with each other. Where a Cyber Asset's functionality results in categorization under multiple categories, an unintended consequence cannot be the impossibility of compliance due to conflicting applicable controls.

Likes 0	
Dislikes 0	

Response

Wendy Center - U.S. Bureau of Reclamation - 1,5

Answer	No
Document Name	

Comment

Reclamation does not support the proposed definition of CMS. Reclamation recommends the term CMS be changed to Virtual Centralized Management System (VCMS) and the proposed definition be changed:

from: A centralized system used for administration or configuration of BES Cyber System(s) through which the configuration of the BES Cyber System can be altered.

to: A centralized system used to administer or configure virtual BES Cyber System(s) or virtual BES Cyber Asset(s).

Likes 0	
Dislikes 0	

Response

Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2

Answer	No
Document Name	

Comment

ERCOT notes that the definition is not limited to virtualization. This also introduces questions to some fundamental understanding of physical systems that have been in place since CIP Version 1. ERCOT does not see the value defining Centralized Management System (CMS) as noted in the comment form. It should be left to the determination of the entity on the classification of the systems. The ***Security Guideline for the Electricity Sector: Identifying Critical Cyber Assets*** published in 2010 addressed the concept of management systems. When identifying CCAs, entities were encouraged to consider Cyber Assets in a secondary or supporting role. Based on this guidance, an entity may choose to high watermark the management systems to be equivalent to what they manage due to risk. This means that a management system for a BCA could be classified as a BCA. This approach could also have been applied to EACMS devices.

However, if the SDT is determined to treat management systems as a distinct class of devices, the management systems should be added to the definition of EACMS. Splitting these out will lead to inconsistency in the application of security controls across asset types and increase risk to security programs. Adding management systems to the EACMS definition will present minimal disruption for entities based on the proposal to remove monitoring from the definition.

With regards to the CMS definition proposed, the SDT should clarify the use of “centralized” in the term. The context of “centralized” should be defined. Would this apply to distributed management tools in a virtual environment?

Likes 0	
Dislikes 0	

Response

Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - FRCC,MRO,WECC,Texas RE,SERC,SPP RE, Group Name Southern Company

Answer	No
Document Name	

Comment

Southern Company has concerns that the proposed definition too broadly scopes in system-to-system management consoles used for things like patch management, malicious code prevention signature updates, and other systems that may currently not meet any applicable system definitions that would bring them into scope of the CIP requirements. For example, SCOM/SCCM and Symantec Endpoint protection used to push security patches and AV signatures to enterprise systems, and currently classified as BCSI repositories, would be scoped in and subject to additional compliance requirements as a CMS. Additional clarification is needed to understand the full scope of systems that this proposed definition would apply to. Also, the above notes state “adequately address the risk of systems used to manage virtual environments” and initially speaks specifically to “management systems in a virtual environment”, yet, the proposed definition would be applicable to all environments, physical or virtual. The currently proposed definition could have further reaching impacts to management systems that are not used in virtual environments, and is overly broad and does not properly scope to virtualized environments.

Likes 0	
Dislikes 0	

Response

sean erickson - Western Area Power Administration - 1,6

Answer	No
Document Name	

Comment

Comments: So many systems if used incorrectly or maliciously can gravely affect multiple cyber assets in a BES Cyber System. These include centralized antivirus systems where a defective signature file (e.g. McAfee) could shutdown systems, centralized patching systems, baselining systems (e.g. Tripwire), vulnerability detection systems (e.g. Nessus), software defined networking systems and others. To single out virtualization control consoles seems short-sighted as it does not relate directly to the virtualized devices once they are provisions. There are also the issues around whether a client computer with a fat-client application for VM provisioning is particularly more of a risk, than a system that has a web-interface to the hypervisor that can also effect provision. In summary, centralized control systems are their own security domain, and should either be addressed separately, or under the auspices of protections afforded to all physical and virtual cyber assets.

Likes 0	
Dislikes 0	

Response

Shelby Wade - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company

Answer	No
Document Name	

Comment

While we agree that the appropriate option is to create a new definition, we are concerned that the proposed definition will cause confusion on the scope of the intended systems. The definition should clearly state that it applies only to mixed-mode virtual environments.

Likes 0	
Dislikes 0	

Response

David Francis - Midcontinent ISO, Inc. - 2,3 - MRO,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG

Answer	No
Document Name	

Comment

- It should be left to the determination of the entity on the classification of the systems. The ***Security Guideline for the Electricity Sector: Identifying Critical Cyber Assets*** published in 2010 addressed the concept of management systems. When identifying CCAs, entities were encouraged to consider Cyber Assets in a secondary or supporting role. Based on this guidance, an entity may choose to high watermark the management systems to be equivalent to what they manage due to risk. This means that a management system for a BCA could be classified as a BCA. This approach could also have been applied to EACMS devices.

- If the SDT is determined to treat management systems as a distinct class of devices, the management systems should be added to the definition of EACMS. Splitting these out will lead to inconsistency in the application of security controls across asset types and increase risk to security programs.

- The definition is not limited to virtualization. This also introduces questions to some fundamental understanding of physical systems.
- The SDT should clarify the use of “centralized” in the term. Centralized in what manner? What about distributed management tools in a virtual environment?
- Management systems could be added to the EACMS definition. This will work with minimal disruption for entities based on the proposal to remove monitoring from the definition.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Xcel Energy believes that further clarification of what the CMS definition refers to and the differences between EACMS vs CMS systems should be included. For example, would the term CMS be limited to virtual environments or could a malware management console also be considered a CMS?

Likes 0	
Dislikes 0	

Response

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group

Answer	No
Document Name	

Comment

The SPP Standards Review Group has a concern that the proposed definition may have more impact on other processes besides Virtualization. We feel that if the drafting team has an intent to include other processes that they clearly state that in the proposed definition and supporting language or develop some form of rationale to explain their position on the topic.

Likes 0	
Dislikes 0	

Response

Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4, Group Name FirstEnergy Corporation

Answer	No

Document Name	
Comment	
CMS communication is usually classified as system to system communication and not interactive remote access. The intent is to clarify how entities should implement virtual infrastructure. This definition should be limited to CMS systems that support virtual systems as that is the risk being addressed. This broad of an addition would require a re-write of interactive remote access vs. system to system communication requirements.	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
The proposed definition appears to apply in a much broader sense than just Virtualization management. As currently proposed, this definition of CMS could apply to non-Virtualization tools such as Patching, or Password management. This definition would broaden the scope much farther than just applying to Virtualization.	
Likes 0	
Dislikes 0	
Response	
John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	No
Document Name	
Comment	
Tacoma Power supports comments submitted by APPA.	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	No

Document Name	
Comment	
The proposed definition of Centralized Management Systems is vague as to what is considered a “centralized system,” which could lead to ambiguity and confusion. As currently proposed, AZPS is unsure if the term is referencing hardware, software, firmware, a combination of these, or something else. AZPS respectfully submits for the SDT’s consideration a revised definition of Centralized Management System (CMS). **Centralized Management System (CMS):** *Cyber Asset(s) through which the virtualization of BES Cyber Systems and their associated EACMS, PCAs, and PACs are administered.*	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	No
Document Name	
Comment	
Public power agrees with the concept of separating the management plane from the data plane. However, the current definition includes Active Directory servers and makes it difficult to maintain systems that are inside the ESP.	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	
N&ST believes the proposed definition falls well short of SDT’s intent and, if adopted, would result in endless arguments over its applicability. What does “centralized” mean? Would it apply to the administration and configuration of ALL BES Cyber Systems? Would it apply to ANY device through which an IT or OT administrator could make ANY type of configuration change? Would it apply to systems used to push software patches and/or anti-virus signature files to BES Cyber Systems (N&ST believes some Regional Entity auditors would probably assert that it does)? If it is the SDT’s intent to address systems used to create, configure, modify, and delete virtual machines, then this definition should say so explicitly. In fact, N&ST believes the SDT should consider using the well-understood term, “hypervisor” in any proposed definition.	

Likes 0	
Dislikes 0	
Response	
Don Schmit - Nebraska Public Power District - 1,3,5	
Answer	No
Document Name	
Comment	
Refer to question #23 comments.	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
CenterPoint Energy disagrees with the proposed definition of Centralized Management Systems (CMS) due to the potential for mis-interpretation of the word “centralized.” Entities may avoid classifying management systems as CMS because they are not centralized or, in the case of a PC running a management tool, because they are not “systems”. Vendors provide centralized management systems that automate management of many systems, but the proposed definition could apply to any system that manages another, even if there is only a one-to-one relationship and even if the management is performed by an administrator running commands or simple scripts from a terminal. CenterPoint Energy believes both scenarios do not meet the intended definition of “Centralized Management System,” but the proposed definition may create uncertainty as to the applicability. Further, many management consoles are embedded systems incapable of the security controls required by the standards. Finally, it seems the intent of the SDT is to classify hypervisors as a CMS, but the hypervisor is local, not centralized, and can only impact guests running on that machine. The CMS concept is better left to the entity to categorize, based on impact of unavailability, degradation, or misuse of the management systems on BES reliability.	
Likes 0	
Dislikes 0	
Response	
Brandon McCormick - Florida Municipal Power Agency - 3,4,5,6 - FRCC, Group Name FMPA	
Answer	No
Document Name	2016-02_Virtualization_Unofficial Comment Form_FMPA_comments.docx

Comment

Please see attached comments

Likes 0

Dislikes 0

Response

Janis Weddle - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Chelan PUD

Answer No

Document Name

Comment

The definition as presented is overly broad and would pull in many other types of systems in place for other functions. Systems such as centralized backup, patching platforms, or anti-malware policy servers are certainly capable of modifying the configuration of an Applicable System, but are not currently in scope. They would be unnecessarily brought into scope by this definition. It should be made clear in the definition that CMS would only apply to virtual/multi-instance configurations.

Likes 0

Dislikes 0

Response

Mike Smith - Manitoba Hydro - 1,3,5,6

Answer No

Document Name

Comment

Any management system that can alter the configuration of BCS should be included rather than only the centralized management system, whereas the CMS definition excludes the decentralized management system. Moreover, it can cause dual classification issue as some CMS devices could be the EACMS. We disagree to creating unnecessary new terms that are used to cover the management system and differentiate the electronic access control from the electronic access monitoring devices. These new terms can cause more confusing and more work for the entities to reclassify EACMS and identify the CMS while EACMS have complied with CIP standards. Furthermore, this would require SDT to update all applicable Systems in the CIP standards and create additional requirements for the newly reclassified and identified Cyber Assets such as CMS, EACS and EAG. To meet the same goal and reduce the complexity, we suggest modifying the EACMS definition to include all Cyber Assets that can alter the configuration of BCS into EACMS definition as follows:

“Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems and the cyber systems that can alter the configuration of BES Cyber System.”

Likes 0

Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	
Definitions should not rely on words from the term being defined. In this case, the use of “centralized” in the definition is unnecessary. Also, the definition contains redundant wording. Suggested wording: “One or more Cyber Assets used for administration or configuration of one or more BES Cyber Systems.” The capability for administration or configuration includes the ability to alter a configuration. Also, this appears to be a new class of system that should be protected by the CIP Standards. Which Standards, Requirements, and Parts will need to have “CMS” added to their Applicable Systems designations?	
Likes 0	
Dislikes 0	
Response	
Richard Kinas - Orlando Utilities Commission - 3,5	
Answer	No
Document Name	
Comment	
The definition as proposed should be revised to only include the administration of the BES Cyber System. The current definition may expand the scope to other tools with unintended consequences. Does the definition of CMS need to follow the format of other Glossary Terms by referring to the configuration of BES Cyber Assets instead of BES Cyber Systems? Or is it sufficient as it stands? Does it apply to the administration only of the BCS? We envision that there will either be new requirements around CMS or adding them to other requirements/parts. Our efforts here must be to protect the right devices/systems and improve the reliable/secure operation of the BES. Based on group discussions, we have concerns over what is meant by administration or configuration. There were different interpretations based on individual understanding. This should be resolved with a defined term that can be plugged in to the requirements and be implemented by industry. As indicated in question 1 above, we suggest that the shared components and shared infrastructure may need different defined terms than BES Cyber System It is becoming probablamatic when we have devices that meet multiple definitions, and potentiall when these definitions are used for determinint applicability. I can envision a device being part of a PACs and being a CMS at the same time. Is the CMS intended to be limited to just BCA's and not control devices that are implemented to meet a requirement? **Current definition is too ambiguous and will pull in unintended systems (possibly something that would be both an EACM and a CMS)**	

Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	No
Document Name	
Comment	
This is nearly complete, but still has issues. It is suggested to change this to read “A centralized system used for administration or configuration of BES Cyber System(s) through which the configuration of the managed BES Cyber System(s) can be altered or deleted when no longer needed.”	
Likes 0	
Dislikes 0	
Response	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Is CMS intended to extend to BCSs that have no virtual components? If so, this might be outside the scope of the virtualization mandate. To further the earlier question about if AD is intended to be included in a CMS definition, would the user, group, and permissions management functionality fall under CMS definition or would that continue to be EACMS functionality (or the new EACS category)? Suggest that a CMS be defined as permanent to distinguish from Transient Cyber Assets used for administration/configuration. The risk associated with a CMS would be greater because it could be used inappropriately at any time and potentially remotely. Even if the CMS used the proposed CIP-005 R3 method of communication that might be intermittent, presumably that communication channel would be “on demand” and so would be present the same risk as a permanently connected system.	
Likes 0	
Dislikes 0	

Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Without context of virtualization the definition is too broad and may include systems/assets which are not in scope; the other comment is the definition "Centralized Management System" uses the word centralized to define it, not the function.	
Likes 0	
Dislikes 0	
Response	
John Tolo - Unisource - Tucson Electric Power Co. - 1	
Answer	Yes
Document Name	
Comment	
Does this apply to individual assets as part of a BES Cyber System, or only the BES Cyber System in aggregate? A BES Cyber System would typically have a mixture of assets under disparate CMS control.	
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 ISO-NE NYISO NextERA Con-Ed and HQ	
Answer	Yes
Document Name	
Comment	
We agree that with the model proposed by the SDT, that the term Centralized Management System needs to be defined but are feel that the existing definition provides the clarity needed.	

By just applying the CMS definition and not including any previous conception of a CMS I have the following concerns.

1) Could a Transient Cyber Asset used to configure BCS (protection relays) be considered a CMS? It is probably not a “Centralized system” but I don’t know what that is.

2) Could the cyber systems, owned by the entity or a SCADA vendor, uses to remotely administer or configure multiple SCADA systems (possible at multiple entities) be considered a CMS? Using a intermediate system may eliminate the “centralized system” applicability but would still allow the remote computer to be a CMS in a low impact configuration that does not require an intermediate system.

3) The current definition would identify an Active Directory Server as a CMS. Is this what is intended?

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

It is BPA’s opinion that the proposed definition of CMS captures most types of systems that support automation with a large span of control and privileged access.

BPA recommends that the SDT moves away from the old model of devices and prescriptive requirements to a model of systems and security objectives. Under the current approach, Applicable Systems definitions are necessary to target requirements. However, under a security objectives-based approach, definitions of Applicable Systems would be less critical.

Likes 0	
Dislikes 0	

Response

Chantal Mazza - Hydro-Qu?bec TransEnergie - 2 - NPCC

Answer	Yes
Document Name	

Comment

We agree that with the model proposed by the SDT, that the term Centralized Management System needs to be defined but are feel that the existing definition provides the clarity needed.

By just applying the CMS definition and not including any previous conception of a CMS I have the following
oncerns.

1) Could a Transient Cyber Asset used to configure BCS (protection relays) be considered a CMS? It is probably not a “Centralized system” but I don’t know what that is.

2) Could the cyber systems, owned by the entity or a SCADA vendor, uses to remotely administer or configure multiple SCADA systems (possible at multiple entities) be considered a CMS? Using a intermediate system may eliminate the “centralized system” applicability but would still allow the remote computer to be a CMS in a low impact configuration that does not require an intermediate system.

3) The current definition would identify an Active Directory Server as a CMS. Is this what is intended?

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

TVA supports the definition of CMS. Suggest consider clarifying that the CMS definition isn’t meant to be specific to physical or virtual CMS systems.

Likes 0	
Dislikes 0	

Response

Russell Noble - Cowlitz County PUD - 3,5

Answer	Yes
Document Name	

Comment

Cowlitz PUD supports BPA's comment.

Likes 0	
Dislikes 0	

Response

Joel Charlebois - AESI - Acumen Engineered Solutions International Inc. - 5

Answer	Yes
Document Name	
Comment	
We agree with the definition, but it potentially includes systems outside the scope of virtualization – e.g., a network configuration management system can be used to push out configurations to various networking components, configuration management software (e.g., Puppet, Salt, Chef, etc.) can do the same for virtually any class of cyber asset. Similar systems exist for IEDs (e.g. Subnet Solutions PowerSYSTEM Center, EATON IMS, etc.) A domain controller can push out group policy, altering the configuration of a BCS. Is the intent for these systems to be covered by this definition? - If yes, that is the intent, then the definition is fine. - If no, it is meant to only encompass virtualization management systems, then the definition is too broad and covers more than just virtualizion management systems as written. Regardless, we believe that all configuration management systems that could affect BCS should be covered because they all have the potential to have impactful effects on the BCS whose configurations they manage.	
Likes 0	
Dislikes 0	
Response	
Daniel Grinkevich - Con Ed - Consolidated Edison Co. of New York - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8,9 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Robert Ganley - Long Island Power Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bob Case - Black Hills Corporation - 1 - WECC	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
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	
Scott Downey - Peak Reliability - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Rather than introduce a new term, Texas RE recommends the SDT consider adjusting the existing EACMS definition, which has been applied (applicable systems) to the CIP Requirements already. Texas RE inquires which parts of the requirements would include the new definition of CMS?	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	

5. Do you agree that the proposed definition of ESZ more adequately applies to proper isolation of multi-instance environments, regardless of OSI layer? If not, please provide a rationale to support your position.

Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric

Answer	No
Document Name	

Comment

Creating a new definition for the same concept of an ESP is counter-productive and does not add additional clarity. Additionally, even if we reused ESP, the definition above is not clear. Keep using ESP, but change the definition to be explicitly clear that either physical or virtual (logical is implied with the use of virtual) networks are allowed for the creation of the required security perimeter to isolate network boundaries. As example, “The logical border network border with one or more defined EAPs implemented using physical network topology or virtual (software defined) network tools to which BES Cyber Systems are connected using a routable protocol.” This at least defines the allowed methods and the expected boundary without adding a new term with a vague definition.

Likes 0	
Dislikes 0	

Response

Richard Kinas - Orlando Utilities Commission - 3,5

Answer	No
Document Name	

Comment

What will be required to have logical separation? Need a logical definition. Do ESP's become mandatory ESZ's?

Baselines for virtual devices—hypervisor, need more data than just the ports & service, OS, SW, patches (resource definitions, other security controls, to do comparison). Configuration must prevent resource starvation—hardening guide for VMware—SSH port/TFE….

What is sufficient here: “proper isolation of multi-instance environments"? Can't create a requirments that relies on entities and auditors to interpret what is proper isolation. Need to define it and or replace the language.

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer	No

Document Name	
Comment	
The meaning of “logical separation” needs to be better defined.	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	No
Document Name	
Comment	
The term **area** in this context needs to be defined or clarified. We suggest rewording the definition: “The area within a networking environment with a defined logical boundary that logically separates one or more Cyber Assets.”	
Likes 0	
Dislikes 0	
Response	
Janis Weddle - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Chelan PUD	
Answer	No
Document Name	
Comment	
The proposed definition is not specific enough to pinpoint multi-instance environments. The definition should be limited to ensure that it only applies to virtual environments. Additionally, it should be made clear that all Cyber Assets within the ESZ should reside within the same logical network.	
Likes 0	
Dislikes 0	
Response	
Bob Case - Black Hills Corporation - 1 - WECC	
Answer	No
Document Name	

Comment	
Yes, in theory. If infrastructure was shared, then ESZ would make sense. Would like to see more technical detail to the definition to know where NERC is going with this, to justify the additional term as compared to sticking with just ESP.	
Likes 0	
Dislikes 0	
Response	
Brandon McCormick - Florida Municipal Power Agency - 3,4,5,6 - FRCC, Group Name FMPA	
Answer	No
Document Name	2016-02_Virtualization_Unofficial Comment Form_FMPA_comments.docx
Comment	
Please see attached comments	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
CenterPoint Energy does not agree with the proposed ESZ definition. The term “area” is ambiguous and open to interpretation. Rather than creating a new concept such as ESZ, the SDT should consider adding language to the requirements that provide logical separation between assets. Additionally, it may be challenging to document evidence that demonstrates an ESZ.	
Likes 0	
Dislikes 0	
Response	
Don Schmit - Nebraska Public Power District - 1,3,5	
Answer	No
Document Name	

Comment	
Refer to question #23 comments.	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	
N&ST considers this proposed definition, as written, to be essentially identical to the existing definition of ESP. It appears to be the SDT’s intent to apply the concept of logical separation to virtual machines running on shared hardware/software infrastructures, in which case the definition should be written so as to make this explicit.	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No
Document Name	
Comment	
TVA supports flexibility within the standard to accommodate a multi-tenant architecture and the benefits provided by adaptation of industry standard architectures such as on premises cloud computing and hyper-converged infrastructures. TVA is concerned the ESZ concept as presented is overly complex and creates potential to hamper entities in constructing appropriate security controls or programmatic boundaries for their compliance programs. Loading definitions and program boundaries with new, undefined terms such as “multi-instance, shared infrastructure, management plane, data plane, and containers,” will only compound confusion and fragmentation of interpretation.	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	No

Document Name	
Comment	
AZPS believes the proposed definition does not adequately address the controls needed to perform the necessary separation. AZPS respectfully proposes a revision to the definition of Electronic Security Zone. **Electronic Security Zone:** *A segment of infrastructure services containing one or more Cyber Assets that is established using a logical border and to which the Responsible Entity has applied specific security controls.*	
Likes 0	
Dislikes 0	
Response	
John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	No
Document Name	
Comment	
Tacoma Power supports comments submitted by APPA. Additionally, Tacoma Power has concerns that the boundaries of logical segmentation can be unclear with shared memory, storage and network interfaces.	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4, Group Name FirstEnergy Corporation	
Answer	No
Document Name	
Comment	
This definition is not limited to just systems using virtual technologies and would reduce clarity and industry understanding for classifying routable vs non-routable logical separations. Include a caveat limiting ESZ to multi-tenant systems.	
Likes 0	
Dislikes 0	
Response	

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group

Answer	No
Document Name	

Comment

The SPP Standards Review Group has a concern that the proposed definition may have more impact on other processes besides Virtualization. We feel that if the drafting team has an intent to include other processes that they clearly state that in the proposed definition and supporting language or develop some form of rationale to explain their position on the topic. Also, we have a concern about how the term “logical separation” will be used or the intent of the term. For example, what defines “logical separation,” and does it have physical or technological control?

Likes 0	
Dislikes 0	

Response

David Francis - Midcontinent ISO, Inc. - 2,3 - MRO,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG

Answer	No
Document Name	

Comment

The ESP and ESZ definitions should be aligned within a single definition. There is no need for two definitions that address basically the same idea. Two definitions will cause confusion. Recommend: The border that provides logical separation to isolate BES Cyber Systems from other Cyber Assets.

Likes 0	
Dislikes 0	

Response

sean erickson - Western Area Power Administration - 1,6

Answer	No
Document Name	

Comment

Comments: How appropriate various forms of logical and physical isolation are will always be dependent on the software and hardware implementations. A definition of the boundary between a VM and its hypervisor, or a VM and another VM may be useful to delineate a boundary where security/isolation controls can be evaluated/applied, but by no means addresses the concept of "proper isolation". The concept of proper isolation is a diffuse one and can broach on a multitude of shared infrastructure concerns, including SANs, power distribution systems, separation of computing instructions from data in hardware, etc. Risk can also be evaluated in the context of the systems design, or can encompass the possibility of privilege elevation bugs which further muddies the water. In summary, the isolation of virtual cyber assets isn't necessarily a greater concern than the isolation of physical cyber assets, with the possible exception of how a hypervisor might be treated. It is even conceivable that a VM platform could securely isolate even systems with different security contexts depending on the implementation.

Likes 0	
Dislikes 0	

Response

Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - FRCC,MRO,WECC,Texas RE,SERC,SPP RE, Group Name Southern Company

Answer	No
Document Name	

Comment

Please add to the end of the definition “of one or more Cyber Asset(s) in a virtual multi-instance environment.” Without this clarification directly in the definition, rather than in the Applicable System section, there could be unintended consequences and confusion between ESZ and ESP for Cyber Assets that are not part of a virtual multi-instance environment.

Likes 0	
Dislikes 0	

Response

Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2

Answer	No
Document Name	

Comment

Comments: ERCOT recommends that the ESP and ESZ definitions should be aligned within a single definition. There is no need for two definitions that address basically the same idea. Creating two definitions will add to confusion and may require Entities that have implemented to CIP Version 5/6 to re-assess and re-design their configurations at substantial cost without much added benefit. The ESZ definition is broad and appears focused on a single or few use cases (based upon vendor technologies), but could have negative impact on other use cases (other vendors) beyond the intended purpose. ERCOT asserts that a single definition could be used to address network boundaries holistically and asked that the SDT consider a modification such as, “The border that provides logical separation to isolate BES Cyber Systems from other Cyber Assets.”

Likes 0	
Dislikes 0	

Response

Wendy Center - U.S. Bureau of Reclamation - 1,5

Answer	No
Document Name	

Comment

Reclamation does not support the proposed definition of ESZ. The term ESZ can impact virtualized and non-virtualized systems.

Reclamation recommends the term Electronic Security Zone be changed to Virtual Electronic Security Zone (VESZ), applying only to virtualized environments, and the proposed definition be changed:

from: The area defined by the logical separation of one or more Cyber Asset(s).

to: A boundary housing one or more Virtual Machines logically separated from other BES Cyber Systems or other non-BES Cyber Systems using partitioned and isolated service set identifiers (SSIDs), virtual local area networks (VLANs), or other technologies.

Likes 0	
Dislikes 0	

Response

Aaron Austin - AEP - 3,5

Answer	No
Document Name	

Comment

While the proposed definition does for today give a more specific method of isolation, AEP believes a more effective solution would be to, at most, modify the definition of ESP to allow for greater latitude in establishing logical segmentation of networks whether physical or virtual. AEP believes implementation of processes to meet CIP-005 R1, Parts 1.6-8 would produce sufficient evidence and meet the intent of the proposed requirements without introducing the new definition of an ESZ.

Likes 0	
Dislikes 0	

Response

Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8,9 - WECC

Answer	No
Document Name	

Comment

SDG&E considers this concept of an ESZ to be vague at best and problematic with compliance. Specifically the physical separation that may or may not be achieved in a virtual environment.

Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE	
Answer	No
Document Name	
Comment	
Scope Expansion Adds Complexity. The incorporation of the term “Cyber Asset” within the proposed Glossary Term can easily broaden the scope beyond isolation of multi-instance environments. Expanding the scope will create unnecessary implementation and compliance complexity. **Compliance Uncertainty.** The term “area” is vague and will create compliance uncertainty. We have not been able to identify additional prescriptive language or how to succinctly define the term to mitigate that uncertainty.	
Likes 0	
Dislikes 0	
Response	
John Tolo - Unisource - Tucson Electric Power Co. - 1	
Answer	No
Document Name	
Comment	
The term “logical” should be more specific, up to and including relevant OSI layers. It should also be specified if the ESZ will require separation of specific assets from each other. In physical servers, the communication between devices in an ESP is not controlled and we believe the analogy should carry to virtual infrastructure. Two VMs of the same BES Cyber System could share an ESP and an ESZ, for instance.	
Likes 0	
Dislikes 0	
Response	
Ronald Donahey - TECO - Tampa Electric Co. - 1,3,5,6	
Answer	No
Document Name	
Comment	

- The proposed definition of an ESZ is insufficient to provide guidance to industry.
- TEC has included some of the questions/discussion around the logical separation and layers for the SDT to better understand where the confusion may lie.
    - More than just OSI layer 3 connectivity; need to provide controls at the other layers, but which layers? Who makes the call?.
    - VMware: Can put virtual firewalls inside the cluster; can separate the traffic with controls in place. Which OSI layers—segment layer 2 or layer 3. Concept for ESZ is for non-layer 3.
    - If it is on the same SAN, if you have the potential to use the other hardware, then you have to protect it. Or could encrypt the device. Definition of Cyber Assets—electronic physical or virtual….would apply to the financial box in the image on p. 8.
    - What will be required to have logical separation? Need a logical definition and Virtual Cyber Asset…should not be physical plane into virtual plane.
    - Baselines for virtual devices—hypervisor, need more data than just the ports & service, OS, SW, patches (resource definitions, other security controls, to do comparison). Configuration must prevent resource starvation—hardening guide for VMware—SSH port/TFE….
    - Implement vendor hardening guide—(but that brings in new requirements related to

    Mixed trust—create vm dedicated to CIP; VM for high BES Cyber Systems… what about the EACMs—in a separate environment but not an ESP? What about PACS—now on corporate; separate VM environment for PACS. Will get to be cost prohibitive to use virtual environments if they all have to be separate. Every device on the virtual environment has to be treated according to the high water mark;

    - May apply to one instance but may not apply to others. What is sufficient here: “proper isolation of multi-instance environments,”

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Alliant Energy believes the ESZ definition does not adequately describe the environment options. We request clarification on the relationship between the ESZ and ESP in a virtual instance and whether the ESZ replaces the ESP or is conained within the ESP. Additionaly, the definition should distinguish between BCS ESZ and non-CIP ESZ.

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	No
Document Name	
Comment	
Clarification of the need for an ESZ has not been established within the definition.	
Likes 0	
Dislikes 0	
Response	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	
Comment	
Fundamentally disagree with the creation of a new ESZ concept. It seems to be an attempt to arrange virtual resources in a way similar to what is currently done with Cyber Assets as network nodes in an ESP. However they are not analogous, do not work that way and should not be managed that way. The ESZ concept is not a good fit and explains why most of remaining question is this section are difficult to interpret. Please see summary answer 21 for suggestion of a simpler approach. Also, use of “multi-instance”, if, as it seems to be, is meant to be analogous with the idea of “multi-tenant”, than this would seem to exclude most virtualized systems. Is this intended?	
Likes 0	
Dislikes 0	
Response	
Daniel Grinkevich - Con Ed - Consolidated Edison Co. of New York - 1,3,5,6	
Answer	No
Document Name	
Comment	

The current definition is unclear.	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5	
Answer	Yes
Document Name	
Comment	
ESZ definition is good, but ESP definition should be removed and ESZ controls should be sufficient.	
Likes 0	
Dislikes 0	
Response	
Joel Charlebois - AESI - Acumen Engineered Solutions International Inc. - 5	
Answer	Yes
Document Name	
Comment	
This definition is sufficiently high level that it could encompass any type of logical isolation.	
Likes 0	
Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3,5	
Answer	Yes
Document Name	
Comment	
We support BPA's comment.	

Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
BPA believes the proposed definition promotes proper isolation of multi-instance environments regardless of OSI layers. However, usefulness of ESZ is not limited to multi-instance environments. ESZ enables separating risk associated with different types of technology, layering of controls, and granular security in contrast to the outdated, simplistic, high-watermarking approach of ESP.	
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 ISO-NE NYISO NextERA Con-Ed and HQ	
Answer	Yes
Document Name	
Comment	
We are concerned that because ESZ uses a different definition of “logic” than is used in the BCS definition, the definition used in ESZ could be applied to the BCS. Please provide clarification on the difference between an ESZ and an ESP.	
Likes 0	
Dislikes 0	
Response	
Paul Haase - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light	
Answer	Yes
Document Name	
Comment	

City Light generally supports the ESZ concept but does not find it to sufficiently detailed or evaluated for integration with structure of the existing CIP Standards. As such City Light supports APPA's comments for this question 9especially as regards the varied meanings of "logical"), while generally agreeing with BPA's position.	
Likes 0	
Dislikes 0	
Response	
Scott Downey - Peak Reliability - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Robert Ganley - Long Island Power Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Chantal Mazza - Hydro-Qu?bec TransEnergie - 2 - NPCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shelby Wade - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lauren Price - ATCO Electric - 1 - MRO,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	
Document Name	
Comment	

APPA is concerned that the ESZ uses a different definition of “logic” than is used in the BCS definition and believes the Standard Drafting Team (SDT) should share that concern.

Public power is concerned that the standard could lead to a misunderstanding that the definition of “logic” is the same for BCS, ESZ and the proposed CIP-005 R1.6.

Consequently, the standard needs clarification on how an ESP is not an ESZ.

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	
Document Name	

Comment

Texas RE suggests the current term, Electronic Security Perimeter, is sufficient for protecting Cyber Assets. The BES Cyber System concept is a logical grouping; by definition a BES Cyber System is “***One or more BES Cyber Assets** logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity*.”

Likes 0	
Dislikes 0	

Response

6. Do you agree that the proposed definition of ESZ would aid the development of future CIP Standards by providing a more relevant level of separation? If not, please provide a rationale to support your position.

Daniel Grinkevich - Con Ed - Consolidated Edison Co. of New York - 1,3,5,6

Answer	No
Document Name	

Comment

The proposed definition is not clear.

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC

Answer	No
Document Name	

Comment

Clarification of the need for an ESZ has not been established within the definition. The current ESP and EAP terms are sufficient to describe the access control objective.

Likes 0	
Dislikes 0	

Response

Ronald Donahey - TECO - Tampa Electric Co. - 1,3,5,6

Answer	No
Document Name	

Comment

NERC has clearly stated that Ethernet VLANs are not considered acceptable logical separation. If NERC will not accept VLANs as acceptable (which have been around for 15 years) there is no chance or at least there should be no chance that the ESZ would be found sufficient.

Likes 0	
Dislikes 0	
Response	
John Tolo - Unisource - Tucson Electric Power Co. - 1	
Answer	No
Document Name	
Comment	
We understand the intent is to ensure that VMs in shared environments have controls to keep their data separate, however as written it is ambiguous and appears to be adding security that doesn't exist for physical machines, e.g. separating individual virtual hosts in one BES Cyber System vs. allowing physical BES Cyber Assets in one BES Cyber System to communicate within an ESP.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE	
Answer	No
Document Name	
Comment	
See our response to proposed ESZ definition, Question 5. Also, we do not see the proposed ESZ definition would apply any differently to future CIP Standards. **Request.** If the SDT concludes the proposed definition is required to address the identified issues, clarity is needed to understand the relationship between the Electronic Security Zones and the existing structure of the Electronic Security Perimeter. For example, are the terms ESZ and ESP complementary, or does implementing an ESZ eliminate the need for an ESP?	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8,9 - WECC	
Answer	No
Document Name	
Comment	

A more thorough examination of the physical separation of the virtual environment must be addressed before a true ESZ can be made to be compliant. How does storage factor into the establishment of a ESZ?	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 3,5	
Answer	No
Document Name	
Comment	
While the proposed definition does for today give a more specific method of isolation, AEP believes a more effective solution would be to, at most, modify the definition of ESP to allow for greater latitude in establishing logical segmentation of networks whether physical or virtual. AEP believes implementation of processes to meet CIP-005 R1, Parts 1.6-8 would produce sufficient evidence and meet the intent of the proposed requirements without introducing the new definition of an ESZ.	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	
Reclamation does not support the proposed definition of ESZ. Reclamation recommends the proposed term Virtual Electronic Security Zone (VESZ) (described in the response to Question 5) will provide a more relevant level of separation. Reclamation also recommends changing the terms “instance” and “multi-instance” to “Virtual Instance” and “Multi-Virtual Instance” and adding them to the NERC Glossary of Terms using the SDT’s intended meanings as the definitions.	
Likes 0	
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	

Answer	No
Document Name	
Comment	
See comments for question 5.	
Likes 0	
Dislikes 0	
Response	
Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - FRCC,MRO,WECC,Texas RE,SERC,SPP RE, Group Name Southern Company	
Answer	No
Document Name	
Comment	
The definition, as proposed, does not properly scope the implementation of the term to virtual multi-instance environments, and could have broader impacts as currently stated.	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	No
Document Name	
Comment	
Comments: The adequacy of separation is dependent upon the hardware and software of a specific implementation, and also to the evaluation of issues with such separation overtime. A definition as a placeholder for future VM isolation requirements seems to presuppose that the need of logical segregation for virtual cyber assets exceeds that of physical cyber assets.	
Likes 0	
Dislikes 0	
Response	
David Francis - Midcontinent ISO, Inc. - 2,3 - MRO,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG	

Answer	No
Document Name	
Comment	
The ESP and ESZ definitions should be aligned within a single definition. There is no need for two definitions that address basically the same idea. Two definitions will cause confusion. A consistent approach to logical boundaries.	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	No
Document Name	
Comment	
The SPP Standards Review Group recommends that the drafting team provides more supporting detail in the definition.	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4, Group Name FirstEnergy Corporation	
Answer	No
Document Name	
Comment	
This definition reduces the clarity for levels of logical separation by adding a level. Increasing the number of logical separations a system may have adds to confusion within the standard and increases compliance complexity which is not desired.	
Likes 0	
Dislikes 0	
Response	
John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	No

Document Name	
Comment	
Tacoma Power supports comments submitted by APPA.	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
The proposed definition of ESZ appears to be overly broad. Does the drafting team intend that the definition of ESZ supersede the ESP? As currently proposed, situations could exist where a Cyber Asset would need to comply with both ESP and ESZ requirements.	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	No
Document Name	
Comment	
AZPS is concerned that the definition and concept as proposed could lead to ambiguity and confusion if it does not address all of the concepts and potential configurations indicated in this document and its associated diagrams. In particular, AZPS recommends that the definition needs to address the separation controls as mentioned in the rationale provided in Questions 5, 7, 8, etc. Additionally, AZPS recommends that the terms instance and multi-instance be revised to refer to tenancy as this is a more accurate representation of virtualized devices and environments. The term instance could be confused relative to whether it is referencing a segment of the virtualized environment or the assets within that environment. To alleviate that confusion, AZPS believes that use of the terms tenant and multi-tenant will more clearly delineate the cyber assets versus the environment. &bull; Tenant: Discrete organizational environment with specific privileges or security levels, consisting of functions that consume resources from the shared infrastructure. Tenants are logically isolated, but physically interconnected. &bull; Multi-Tenant: An environment where a shared infrastructure provides containers for more than one tenant.	

Likes 0	
Dislikes 0	

Response

Jack Cashin - American Public Power Association - 4

Answer	No
Document Name	

Comment

APPA does not believe that the proposed definition for ESZ would provide the relevant level of separation needed. “Logical separation” is based on current technology and may not be applicable to future controls.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

TVA supports flexibility within the standard to accommodate a multi-tenant architecture and the benefits provided by adaptation of industry standard architectures such as on premises cloud computing and hyper-converged infrastructures. The ESZ concept, as presented, is overly complex, and lacks clarity to help entities how to institute separation between tenants, and shared underlying physical compute resources, whether processor (compute), storage, or transport (network).

Likes 0	
Dislikes 0	

Response

Nicholas Lauriat - Network and Security Technologies - 1

Answer	No
Document Name	

Comment

N&ST believes a properly written definition of “ESZ” would aid in the development of future CIP requirements, but has checked “No” to reflect concerns about the inadequacy of the current proposed definition.	
Likes 0	
Dislikes 0	
Response	
Don Schmit - Nebraska Public Power District - 1,3,5	
Answer	No
Document Name	
Comment	
Refer to question #23 comments.	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
The ESZ concept is potentially confusing and will not aid in clarity for future Standards. Standards relevant to logical separation can state requirements for logical separation where appropriate. Further, business needs vary in different environments, and an entity may have valid reasons for not logically separating systems that do not introduce unacceptable security risks. Requiring an ESZ to be defined limits the flexibility an entity has to design and manage systems in their own environments.	
Likes 0	
Dislikes 0	
Response	
Brandon McCormick - Florida Municipal Power Agency - 3,4,5,6 - FRCC, Group Name FMPA	
Answer	No
Document Name	2016-02_Virtualization_Unofficial Comment Form_FMPA_comments.docx
Comment	

Please see attached comments	
Likes 0	
Dislikes 0	
Response	
Bob Case - Black Hills Corporation - 1 - WECC	
Answer	No
Document Name	
Comment	
Do not see the benefit to entities of a separate term at this time. But if shared infrastructure is in place at an entity, then this could make sense.	
Likes 0	
Dislikes 0	
Response	
Janis Weddle - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Chelan PUD	
Answer	No
Document Name	
Comment	
With an appropriately narrow definition (see #5 comments), we would consider the addition of ESZ to be adequate.	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	No
Document Name	
Comment	

The ESZ definition is not clear and doesn’t define what Cyber Asset should reside in the ESZ. If all Cyber Asset inside a ESP, in our opinion, the ESZ is not necessary.

Likes 0

Dislikes 0

Response

Richard Kinas - Orlando Utilities Commission - 3,5

Answer No

Document Name

Comment

NERC has clearly stated that Ethernet VLANs are not considered acceptable logical separation. If NERC will not accept VLANs as acceptable (which have been around for 15 years) there is no chance or at least there should be no chance that the ESZ would be found sufficient. We have concern that NERC will not accept (nor should they based on their current concerns over VLANs) this definition without the underlying acceptance of the vlans use for logical separation.

Likes 0

Dislikes 0

Response

Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric

Answer No

Document Name

Comment

As stated above, adding a new term without any definition of what is expected adds confusion. The proposed definition is similar to how PCI (Payment Card Industry) standards defined the use of virtualization and lead to the delay in properly defining a secure usage for the technology allowing virtual networks and micro-segmentation.

Likes 0

Dislikes 0

Response

David Ramkalawan - Ontario Power Generation Inc. - 5

Answer No

Document Name

Comment	
Likes 0	
Dislikes 0	
Response	
Paul Haase - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light	
Answer	Yes
Document Name	
Comment	
City Light supprots the direction introduced by ESZ but believes additional work is necessary to clarify its implications and ensure its correct functioning with the existing CIP framework. City Light supports both the comments of APPA and BPA.	
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 ISO-NE NYISO NextERA Con-Ed and HQ	
Answer	Yes
Document Name	
Comment	
“Logical separation” is based on current technology and may not be applicable to future controls. Suggest that it would be better to require the separation and that the separation could include logical methods but not limiting it to just logical.	
Likes 0	
Dislikes 0	
Response	
Lauren Price - ATCO Electric - 1 - MRO,RF	
Answer	Yes
Document Name	
Comment	

Having another defined term for a security zone helps provide additional clarity.	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
As virtualization matures in this industry, it will require a more effective construct than the existing ESP. ESZ is the more effective construct for multilayered, modern security strategies as opposed to ESP which is one dimensional and has been applied at one layer of the OSI model.	
Likes 0	
Dislikes 0	
Response	
Chantal Mazza - Hydro-Qu?bec TransEnergie - 2 - NPCC	
Answer	Yes
Document Name	
Comment	
“Logical separation” is based on current technology and may not be applicable to future controls. Suggest that it would be better to require the separation and that the separation could include logical methods but not limiting it to just logical.	
Likes 0	
Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3,5	
Answer	Yes
Document Name	
Comment	

We support BPA's comment, but also caution development to allow for future advances in controls.	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
With a stronger definition of ESZ, this concept may be worth pursuing.	
Likes 0	
Dislikes 0	
Response	
Joel Charlebois - AESI - Acumen Engineered Solutions International Inc. - 5	
Answer	Yes
Document Name	
Comment	
It is difficult to tell from the definition alone. It would need to be shown in context to determine if it is useful. It is sufficiently high level to cover many different types of logical separation, but it may be so abstract that entities will have trouble interpreting what to do. Based on some of the following requirements though, it looks like it will aid in development of future CIP Standards.	
Likes 0	
Dislikes 0	
Response	
Shelby Wade - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Robert Ganley - Long Island Power Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
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	
Scott Downey - Peak Reliability - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	
Document Name	
Comment	

No comment at this time	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Please see Texas RE’s response for #5.	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	

7. Do you agree that the proposed CIP-005 Requirement R1, Part 1.6 provides sufficient security controls for the high and medium impact BES Cyber Systems residing in a multi-instance environment and their associated CMS to reduce the stated risks inherent to virtualization? If not, please provide a rationale to support your position.

Scott Downey - Peak Reliability - 1	
Answer	No
Document Name	
Comment	
In many instances the management plane uses centralized authentication such as radius or Idap. This makes the management plane dependent on the supporting authentication servers. The supporting authentication servers often have a managmeent backplane. For simplicity the managment plane of the authentication servers may be connected to the date plane as the benefit of separating the planes is limited due to the dependency.	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	No
Document Name	
Comment	
This is close, but needs more definition and a requirement to ensure that the CMS still reside within the ESP (again remove the use of an ESZ as this adds more confusion). Suggestion re-write: Logically separate, using Hypervisor controls and an associated CMS, all Applicable Systems into defined groups of one or more Cyber Asset(s) to achieve the objective of mitigating the risks of span-of-control, insider threats, and lateral privilege expansion. At a minimum: 1. The management plane (CMS) and the data plane of the managed BES Cyber system shall be separated on different managed networks while ensuring both must reside in the same ESP. 2. The CMS of the managed BES Cyber Systems shall be separated from the data planes in which the BES Cyber Systems operate.	
Likes 0	
Dislikes 0	
Response	
Richard Kinas - Orlando Utilities Commission - 3,5	
Answer	No
Document Name	

Comment	
Part 1.6.1 potentially mitigates the risk of lateral privilege expansion and possibly insider threats We are concerned that none deal with mitigation of span-of-control In addition, not all vendor solutions may be able to address Part 1.6. If it is added, there should be TFE capability. In addition, the proposed Part 1.6 introduces the requirement for lists to demonstrate compliance. We also suggest that the word “achieves “ is not the appropriate term for the requirement part. We recommend changing it as follows: Logically separate all Applicable Systems (is this a new defined term?) into defined groups of one or more Cyber Asset(s) to **address potential risks** related to span-of-control, insider threats, and lateral privilege expansion.	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	
This concept has great promise, but terms need to be either defined in the Glossary (preferred), or explained thoroughly in a Technical Guidance document that can become Implementation Guidance. Also, consider adding EACMS and PACS to the applicable systems, as EACMS and PACS can benefit from virtualization technologies as well.	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	No
Document Name	
Comment	

We suggest changing the wording from “defined groups of one or more Cyber Assets to “defined ESZs”. Also we suggest changing the wording from “The management plane and the data plane of the applicable BES Cyber System shall be separated” to “The management plane and the data plane of the applicable BES Cyber System shall be separated by ESZ”. As we proposed EACMS definition modification, “CMS” would be changed to “EACMS”. Please clarify whether the management plane and data plane need to be separated by ESZ, provided that both planes reside inside ESP. Given that the modified Cyber Asset definition includes physical and virtual devices, this requirement will apply to physical cyber system as well, where it means the current in-band network architeture is required to be changed. For instance, an EACMS inside ESP would requires a ESZ to separate it from the BES Cyber Systems.

Likes 0	
Dislikes 0	

Response

Janis Weddle - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Chelan PUD

Answer	No
Document Name	

Comment

CIP-005 R1.6 should explicitly require the defined groups to be ESZs rather than implicitly. "Logically separate all Applicable Systems into Electronic Security Zones to achieve the…”.

Additionally, “span-of-control, insider threats, and lateral privilege expansion” should be removed from the proposed requirements and moved to the Guidance and Technical Basis.

Likes 0	
Dislikes 0	

Response

Brandon McCormick - Florida Municipal Power Agency - 3,4,5,6 - FRCC, Group Name FMPA

Answer	No
Document Name	2016-02_Virtualization_Unofficial Comment Form_FMPA_comments.docx

Comment

Please see attached comments

Likes 0	
Dislikes 0	

Response

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
The Requirement language as written will be challenging for entities to demonstrate compliance because it is objective and intent based. Registered entities may have difficulty producing evidence of intent. Also, entities may encounter situations where there is a valid reason for not separating the management and data plane of an asset or system, and the proposed Requirement R1, Part 1.6 would not allow that. Further, many assets do not have a capability of logical separation of management and data plane. For those that do have the capability of such separation, it is not clear what evidence can be provided to prove the separation is achieved and that no management activity has or can occur from the data plane. This requirement seems to be aimed at multi-instance environments but does not state this in the language, and it would be difficult to achieve and demonstrate for many non-virtual environments. If the proposed Requirement R1, Part 1.6 is intended for multi-instance environments, the wording should be revised to make such intent clear.	
Likes 0	
Dislikes 0	
Response	
Don Schmit - Nebraska Public Power District - 1,3,5	
Answer	No
Document Name	
Comment	
Refer to question #23 comments.	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	
N&ST considers the stated objectives to be worthy but they should not be included in a requirement statement. How would an entity actually demonstrate they have effectively mitigated the identified risks? N&ST assumes “applicable systems” are “BES Cyber Systems comprising one or more virtual machines” and “associated CMS” but the SDT should say explicitly what are “applicable systems.” N&ST wonders why the SDT, having defined “ESZ,” doesn’t use it here. Why not say, “The data and management planes of applicable systems shall reside in separate ESZs”? N&ST also	

recommends that, at a minimum, any potential requirement such as this include a brief description of what is meant by “management planes” and “data planes.”	
Likes 0	
Dislikes 0	
Response	
Chantal Mazza - Hydro-Qu?bec TransEnergie - 2 - NPCC	
Answer	No
Document Name	
Comment	
Too prescriptive because some products do not allow separation of management and data planes It is difficult to answer this question because it is not completely clear what the proposed R1.6 requires. The first part of this requirement is almost identical to the definition of ESZ. If this requirement is to implement ESZ(s) than it should use the ESZ term. If not, it should be clarified on how this is not an ESZ. Have the same concern as with the use of “logical” in the ESZ definition. The use of “logically separate” in this requirement could redefine the “logically grouped” in the BCS definition. How is “logically separate … into defined groups” used here different than “logically grouped” used in the BCS definition?	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	No
Document Name	
Comment	
While AZPS agrees with the intent to separate the management and data plane, it suggests that the proposed CIP-005, R1.6 is not as clear and unambiguous as it could be and, therefore, could result in confusion regarding applicability. To ensure that the scope of the requirement is clear, AZPS recommends that the language of R1.6 specifically reference virtual, multi-tenant environments.	
Likes 0	
Dislikes 0	
Response	

Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
Duke Energy requests additional clarity as to what the SDT is referring to when referencing lateral privilege expansion. Also, as written, ambiguity exists as to the actions that an entity will need to take to comply. In some instances, more actions may need to be taken to address the risks mentioned in Part 1.6.	
Likes 0	
Dislikes 0	
Response	
John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	No
Document Name	
Comment	
Tacoma Power supports comments submitted by APPA.	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	No
Document Name	
Comment	
The SPP Standards Review Group recommends that the drafting team needs to better identify or define what the two terms “management plane” and “data plane” mean. Also, we would recommend that there be an illustration provided for Part 1.6 as it is in Part 1.8. Question: Does the drafting team intend for the management plane to always be included in the ESP as illustrated in figure 1.8 shown below?	
Likes 0	
Dislikes 0	

Response	
David Francis - Midcontinent ISO, Inc. - 2,3 - MRO,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG	
Answer	No
Document Name	
Comment	
• The SDT should clarify the meaning of separation. Is this intended to be routable protocol separation or memory separation within the hypervisor itself? Seems to be a judgment call. • Refer to the diagram below. It shows management and data plane in the same ESP. • Consider defining span of control and insider threats? • Lateral relative to what? • The security objective adds confusion. • The requirement could simply state “Logically separate Applicable Systems”. • What does “its” refer to in #2? • Management and data functions should be defined and common access prohibited	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	No
Document Name	
Comment	
Comments: While defining groups of cyber assets (physical or virtual) that need to communicate to perform a function, and isolating/limiting such communication within the group makes sense, bringing management and data planes into the standards when so many products do not even have a cohesive mapping to the concepts seems unwise, not to mention the omission of the control plane.	
Likes 0	
Dislikes 0	
Response	

Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - FRCC,MRO,WECC,Texas RE,SERC,SPP RE, Group Name Southern Company

Answer	No
Document Name	

Comment

Southern Company views the proposed requirement as being too prescriptive, reducing the Responsible Entities flexibility in implementing secure concepts in a virtual environment. The SDT should consider also defining the terms “management plan” and “data place” to provide better understanding and specificity.

Likes 0	
Dislikes 0	

Response

Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2

Answer	No
Document Name	

Comment

ERCOT asserts that the requirement increases complexity while creating confusion for Entities that have already implemented CIP Version 5/6. The standard requires an Entity to configure and implement based upon specific configurations concepts creating risk for other technologies. Result or outcome-based standards should be used and not be as prescriptive as the requirement proposed. This allows Entities to use definitions to illustrate their architecture and implementation.

ERCOT offers that the requirement could simply state “Logically separate Applicable Systems”. The proposed requirement offers a security objective, but also goes into specifics that are prescriptive in nature. The SDT should ensure that a proposed requirement is clear and implementable as defined by industry.

With regards to the proposed requirement, ERCOT offers the following feedback. (1) The SDT should clarify the meaning of separation. Is this intended to be routable protocol separation or memory separation within the hypervisor itself? Seems to be a judgment call, which is not appropriate for a mandatory and enforceable requirement. (2) The SDT should consider defining span of control and insider threats. (3) ERCOT requests clarification of the context of “lateral”. Lateral relative to what? (4) The SDT should clarify what “its” refers to in item 2 of the requirement. (5) Management and data functions should be defined and common access prohibited. ERCOT also notes that in the diagram below, the management and data plane in the same ESP.

Likes 0	
Dislikes 0	

Response

Wendy Center - U.S. Bureau of Reclamation - 1,5

Answer	No
Document Name	

Comment

Reclamation does not support the addition of Part 1.6. Reclamation recommends that revising the definition of BES Cyber System and the Impact Rating Criteria will provide sufficient security controls and reduce the stated risks inherent to virtualization. Refer to the principles, recommended definitions, rationale, and recommended Impact Rating Criteria described in the response to Question 24.

Likes 0	
Dislikes 0	

Response

Lauren Price - ATCO Electric - 1 - MRO,RF

Answer	No
Document Name	

Comment

ATC agrees that the proposed addition of CIP-005 Requirement R1, Part 1.6 addresses span of control and lateral privilege expansion. However, ATC does not feel it sufficiently addresses insider threats. ATC suggests striking “insider threats” from the requirement as logical separation does little to stop an insider with knowledge of the environment.

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 ISO-NE NYISO NextERA Con-Ed and HQ

Answer	No
Document Name	

Comment

Too prescriptive because some products do not allow separation of management and data planes

It is difficult to answer this question because it is not completely clear what the proposed R1.6 requires.

The first part of this requirement is almost identical to the definition of ESZ. If this requirement is to implement ESZ(s) than it should use the ESZ term. If not, it should be clarified on how this is not an ESZ.

Have the same concern as with the use of “logical” in the ESZ definition. The use of “logically separate” in this requirement could redefine the “logically grouped” in the BCS definition. How is “logically separate … into defined groups” used here different than “logically grouped” used in the BCS definition?	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 3,5	
Answer	No
Document Name	
Comment	
AEP believes the existing requirements can be determined to be applicable in a virtual environment by a reasonable person. New requirements are not necessary.	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8,9 - WECC	
Answer	No
Document Name	
Comment	
SDG&E considers this proposed requirement to be far too undeveloped to be considered for advancement. SDG&E would like more detailed explanations of the separation of management plane, storage element and data plane. Seek further clarification of where the CMS can reside and be compliant with this requirement. How does a multi-impact criteria CMS meet this requirement?	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE	
Answer	No
Document Name	

Comment

The proposed CIP-005 R1, Part 1.6. creates:

Compliance Uncertainty. The terms “applicable systems,” “span-of-control,” “insider threats,” and “lateral privilege expansion” used in proposed Part 1.6 can easily be construed and interpreted broadly, creating significant compliance uncertainty.

Recognizing that some of the terms occasionally popup within the context of cybersecurity, we have not been able to identify additional prescriptive language or determine how to define the terms to mitigate that uncertainty. Without additional clarity, the terms create compliance uncertainty.

Burdensome Costs. The cost to implement and maintain Part 1.6 compliance is burdensome. The compliance uncertainty associated with the subpart further muddies determination of the eventual security benefit, if any.

System Performance Impacts. It is expected that implementing Part 1.6 will require new or modification to current systems, processes, and procedures. The added complexity will unfavorably affect system performance.

Unintended Consequence. It is generally accepted that added complexity weakens security by increasing potential cyber vulnerability paths.

Likes 0	
Dislikes 0	

Response

John Tolo - Unisource - Tucson Electric Power Co. - 1

Answer	No
Document Name	

Comment

These terms appear to specifically reference VMWare NSX. The webinar showed that it would be acceptable to address management interfaces on one LAN and the public VM on another. That makes sense to us and is a best-practice in general. That said, the definitions should reflect that concept better and be specific about how “deep” that separation needs to be, e.g. does it require two ESPs? Can they be VLAN-separated? (See later comments on VLANs.)

Likes 0	
Dislikes 0	

Response

Ronald Donahey - TECO - Tampa Electric Co. - 1,3,5,6

Answer	No
Document Name	

Comment

We suggest that the proposed requirement Part 1.6 could this be a policy with entity documentation of risk mitigation.

1. Part 1.6.1 potentially mitigates the risk of lateral privilege expansion and possibly insider threats
2. We are concerned that neither minimum inclusions deal with mitigation of span-of-control

In addition, not all vendor solutions may be able to address Part 1.6. If it is added, there should be TFE capability. In addition, the proposed Part 1.6 introduces the requirement for lists to demonstrate compliance. We also suggest that the word “achieves“ is not the appropriate term for the requirement part. We recommend changing it as follows:

Logically separate all Applicable Systems (is this a new defined term?) into defined groups of one or more Cyber Asset(s) to address potential risks related to span-of-control, insider threats, and lateral privilege expansion.

Likes 0	
Dislikes 0	

Response

Paul Haase - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light

Answer	No
Document Name	

Comment

City Light supports the concept of the new requirement but cannot support the wording. Management plane and data plane must be clarified or defined, if used within a legal requirement, and the term "Cyber Asset" must be modified to ensure only 'applicable' or 'virtualized' Cyber Assets are in scope, not all possible Cyber Assets (because the CIP Standards only apply to BES Cyber Assets and applicable Cyber Assets as identified by CIP-002, and not all possible Cyber Assets). Considerable conflict remains between the logical-based concepts on ESZ and the physical-based concepts of devices and Cyber Assets.

City Light further supports APPA's additional comments.

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC

Answer	No
Document Name	

Comment

The new requirement may be adding complexity without addressing the security objective.

Likes 0

Dislikes 0

Response

David Ramkalawan - Ontario Power Generation Inc. - 5

Answer	No
Document Name	

Comment

Agree this is a good idea. However, in practice what it means is most control, at least in terms of interaction by a user through a CMS cyber asset, is via network connection. The simple approach is to require all such CMS cyber assets (virtual or real) to be in a distinct ESP from the hosted cyber assets. Possibly a requirement could be made that any non-IP interaction (a proprietary management plane or direct hooks into the host OS) b/w the CMS cyber asset and the host have some security provisions, but this is usually proprietary and vendor specific and difficult to define in a universal way.

Likes 0

Dislikes 0

Response

Joel Charlebois - AESI - Acumen Engineered Solutions International Inc. - 5

Answer	Yes
Document Name	

Comment

Yes but there needs to be some provision for separating the management planes for BCA and non-BCA. Separation of the management plane is necessary to ensure Cyber Assets are appropriately categorized and that unnecessary cyber assets are not brought into scope when not needed to be.

For instance some entities will use one CMS for all virtualized Cyber Assets. Some of these may be BCA, some may not. Entities will often separate the data planes of these virtual Cyber Assets, but may forget to separate the management plane, thus inadvertently making all of the non-BCAs PCAs even though the data planes are separated. There should be some guidance on this topic to make sure entities are separating virtualized Cyber Assets appropriately.

Likes 0

Dislikes 0

Response

Bob Case - Black Hills Corporation - 1 - WECC	
Answer	Yes
Document Name	
Comment	
: **But should only apply to CMS for BCS.**	
Likes 0	
Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3,5	
Answer	Yes
Document Name	
Comment	
We support BPA's 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	
TVA supports flexibility within the standard to accommodate a multi-tenant architecture and the benefits provided by adaptation of industry standard architectures such as on premises cloud computing and hyper-converged infrastructures. The ESZ concept, as presented, is overly complex, and lacks clarity to help entities how to institute separation between tenants, and shared underlying physical compute resources, whether processor (compute), storage, or transport (network). In the language provided, it is unclear as to the target of the separation (e.g., specific groups of Cyber Assets).	
Likes 0	
Dislikes 0	
Response	

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
BPA recommends clarifying that remote access clients or terminal emulators that are used to connect to a CMS are not a CMS in themselves.	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4, Group Name FirstEnergy Corporation	
Answer	Yes
Document Name	
Comment	
Consider additional clarity on the meaning of management plane and data plane.	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	Yes
Document Name	
Comment	
Please ensure the terms management plane and data plane are defined terms added to the NERC Glossary.	
Likes 0	
Dislikes 0	
Response	
Shelby Wade - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company	
Answer	Yes

Document Name	
Comment	
While we support this concept, please see comment under question 24.	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Alliant Energy agrees that these security controls are needed, but the requirement should be clearer on how the defined groups relate to an ESZ. If ESZ is a new term created for this type of scenario, then the requirement should refer to that term.	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Robert Ganley - Long Island Power Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	

Response

Jack Cashin - American Public Power Association - 4

Answer

Document Name

Comment

By not requiring an ESZ, public power believes that this Requirement construct simplifies the requirement and provides the appropriate control objectives.

The use of the word “achieve” in the draft standard sets a requirement that could be impossible to maintain as new risks emerge. Therefore, APPA proposes replacing “achieve the objective of mitigating the risks” with “address the known risks associated with,” in the standard.

Additionally, public power proposes that this Requirement have the “per device capability” clause.

Public power is concerned that the use of “logically separate” in this proposed requirement could redefine “logically grouped” in the BCS definition. Consequently, members would need to understand how “logically separate … into defined groups” is specifically different than “logically group.” APPA recommends that this aspect of the standard language be clarified.

Likes 0

Dislikes 0

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer

Document Name

Comment

Texas RE does not have comments on this question.

Likes 0

Dislikes 0

Response

8. Do you agree that the proposed CIP-005 Requirement R1, Part 1.7 provides a necessary security control to the high and medium impact BES Cyber Systems residing in a multi-instance environment and their associated CMS(s) to reduce risks inherent to virtualization? If not, please provide a rationale to support your position.	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	
Comment	
Again, since it not understood what an ESZ actually is, the communication in question (if it's not network communication) is not clear, nor are what the mechanisms to control it would be.	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	No
Document Name	
Comment	
A case study demonstrating the use and limitations of achieving the security objectives in a virtualized environment with existing standards should be considered before developing new standards.	
Likes 0	
Dislikes 0	
Response	
Paul Haase - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light	
Answer	No
Document Name	
Comment	

City Light, as above, supports the concept but not the specific wording or detail. Again, Cyber Assets must be modified as "applicable" or "virtual" Cyber Assets. City Light supports APPA's simplification of this proposed requirement.	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	No
Document Name	
Comment	
Whether Alliant Energy agrees with this requirement is dependent on clarification of the ESZ definition. Alliant Energy does agree that technical controls to enforce separation should be required.	
Likes 0	
Dislikes 0	
Response	
Ronald Donahey - TECO - Tampa Electric Co. - 1,3,5,6	
Answer	No
Document Name	
Comment	
We recommend that the SDT consider the scoping on this requirement part. Would this be identified in the applicability table since it only applies to multi-instance? At the top of the standard/requirement? Or as shown within the requirement? We recommend the SDT provide additional clarity on the ability to have technical controls for other layers (aside from the communication layer) and with shared memory space. We would also like the SDT to consider the ramifications on the use of a cloud based SIEM vendor who is most likely using a virtualized environment. In the cloud environment, an entity would be transferring risk as well as trust	
Likes 0	
Dislikes 0	
Response	
John Tolo - Unisource - Tucson Electric Power Co. - 1	

Answer	No
Document Name	
Comment	
As above, the type of communication should be enumerated. Network and Systems engineers are aware of constructs like OSI layers and so avoiding terms like “layer 2” and “layer 3” are counterproductive in our opinion. We support the idea. We had significant internal discussion about whether you are describing a typical VMWare environment, which we consider multi-instance, or if you meant one layer removed such as Containers. The fact that we had significant internal disagreement indicates that this is unclear.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE	
Answer	No
Document Name	
Comment	
Proposed Part 1.7 incorporated the term ESZ. See our response to the proposed ESZ definition, Question 5. Also, we do not see that the concerns regarding the proposed ESZ definition would apply any differently in proposed CIP-005 R1, Part 1.7.	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8,9 - WECC	
Answer	No
Document Name	
Comment	
SDG&E disagrees that the proposed control will provide necessary security controls between high and medium impact BES Cyber Systems residing in a mult-instance environment because “communications” in context of necessary inbound and outbound can mean a multitude of different types and needs of device to device or other communications. Define communications down to a much more granular level. (TCP/IP, I/O, Vsphere config, SCSI?)	
Likes 0	
Dislikes 0	
Response	

Aaron Austin - AEP - 3,5	
Answer	No
Document Name	
Comment	
AEP believes the existing requirements can be determined to be applicable in a virtual environment by a reasonable person. New requirements are not necessary. However, the definition ESZ should be replaced with a more general term (e.g. “Virtual Networks”).	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	
Reclamation does not support the addition of Part 1.7. Reclamation recommends that revising the definition of BES Cyber System and the Impact Rating Criteria will provide sufficient security controls and reduce risks inherent to virtualization. Refer to the principles, recommended definitions, rationale, and recommended Impact Rating Criteria described in the response to Question 24.	
Likes 0	
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
ERCOT asserts that the intent of this requirement is unclear. The proposed ESZ appears to be focused on specific vendor technologies. Virtualization of networks verses host or integrated systems all have very different implementation based upon vendors. Adding a CMS outside of the ESP further complicates security controls.	

ERCOT requests examples of systems that can basically “firewall” non-routable protocols. Additionally, ERCOT requests clarification of an EAP equivalent for the ESZ boundary where inbound and outbound permissions can be applied. If the intention is to only refer to a routable protocol, this requirement part is redundant to the existing firewall requirement in CIP-005 Requirement R1, Part 1.3.

Likes 0	
Dislikes 0	

Response

Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - FRCC,MRO,WECC,Texas RE,SERC,SPP RE, Group Name Southern Company

Answer	No
Document Name	

Comment

Southern Company respectfully requests additional clarity around the use of the term “communications” as it is used in the proposed requirement to achieve micro-segmentation. Does “communications” include resource usage between instances, and does it include LANs, VLANs, virtual switches, port groups, and backplane communications? Consider that for some entities, meeting strict compliance with this requirement as proposed may demand additional procurement of network virtualization solutions from vendors, such as VMWare NSX.

Likes 0	
Dislikes 0	

Response

sean erickson - Western Area Power Administration - 1,6

Answer	No
Document Name	

Comment

Comments: CIP-005 R1, Part 1.7 may be a good requirement for multi-instance environments, but limiting it to virtualized systems rather than considering the proper isolation regarding communications between all virtual and physical systems may not be ideal.

Likes 0	
Dislikes 0	

Response

David Francis - Midcontinent ISO, Inc. - 2,3 - MRO,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG

Answer	No
Document Name	

Comment	
• The intent of this requirement is unclear. Examples of systems that can basically “firewall” non-routable protocols would be helpful. If this only refers to a routable protocol, this is redundant to the existing firewall requirement in CIP-005 Requirement R1, Part 1.3. • What is the EAP equivalent for the ESZ boundary where inbound and outbound permissions can be applied?	
Likes 0	
Dislikes 0	
Response	
John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	No
Document Name	
Comment	
Tacoma Power supports comments submitted by APPA.	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
Does an ESZ have to contain an ESP? Additional clarity on this aspect would be helpful.	
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	

Not all systems can be separated this way without introducing additional hardware such as firewalls between ESZ’s. Some of the systems can be separated into ESZ’s through access controls such as separating administrator roles or other methods. TVA supports flexibility within the standard to accommodate a multi-tenant architecture and the benefits provided by adaptation of industry standard architectures such as on premises cloud computing and hyper-converged infrastructures. The ESZ concept, as presented, is overly complex, and lacks clarity to help entities how to institute separation between tenants, and shared underlying physical compute resources, whether processor (compute), storage, or transport (network). In the language provided, it is unclear as to how access control is to be executed.	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	
N&ST recommends simplifying this requirement to, “Implement technical controls that limit communication between separate ESZs to only that which is necessary, as determined by the Responsible Entity.”	
Likes 0	
Dislikes 0	
Response	
Don Schmit - Nebraska Public Power District - 1,3,5	
Answer	No
Document Name	
Comment	
Refer to question #23 comments.	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No

Document Name	
Comment	
This requirement implies a firewall working on routable communications. If there is a non-routable separation, the requirement is difficult to comply with. This requirement makes the demonstration of logical separation even more difficult than the logical separation in proposed CIP-005 Requirement R1, Part 1.6.	
Likes 0	
Dislikes 0	
Response	
Brandon McCormick - Florida Municipal Power Agency - 3,4,5,6 - FRCC, Group Name FMPA	
Answer	No
Document Name	2016-02_Virtualization_Unofficial Comment Form_FMPA_comments.docx
Comment	
Please see attached comments	
Likes 0	
Dislikes 0	
Response	
Janis Weddle - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Chelan PUD	
Answer	No
Document Name	
Comment	
Electronic Security Zones should already reside in separate ESPs, so the addition of this requirement should be unnecessary, unless the requirement is referring to communications such as access to the virtual console from the hypervisor and other similar communications. If it is intended to refer to those forms of communications, it needs to be clarified.	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	No

Document Name	
Comment	
Given that the modified Cyber Asset definition includes physical and virtual devices, this requirement will apply to physical cyber system as well, where this requirement means the current in-band network architeture is required to be redesinged. For instance, an EACMS inside ESP may require a ESZ to separate it from the BES Cyber Systems. Please clarify if SDT's intention is to apply this requirement to the virtual devices only.	
Likes 0	
Dislikes 0	
Response	
Richard Kinas - Orlando Utilities Commission - 3,5	
Answer	No
Document Name	
Comment	
We recommend that the SDT consider the scoping on this requirement part. Would this be identified in the applicability table since it only applies to multi-instance? At the top of the standard/requirement? Or as shown within the requirement? We recommend the SDT provide additional clarity on the ability to have technical controls for other layers (aside from the communication layer) and with shared memory space. We would also like the SDT to consider the ramifications on the use of a cloud based SIEM vendor who is most likely using a virtualized environment. In the cloud environment, an entity would be transferring risk as well as trust. Baseline configuration information must be gathered and maintained for VM environment including multi-instance implementations.	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	No
Document Name	
Comment	
The use of an ESZ is still confusing. Rather than introduce a new concept, simply state that multiple networks (either virtual or physical) may be used in the same Shared Multi-Instance Environment (the diagram for Part 1.8 perfectly illustrates this). What then is required is that traffic between any ESP or outside of an ESP defined in the same Shared environment must implement the required security controls to enforce secured traffic between the boundaries. This then ensures that all the same controls already required for ESPs must be enforced regardless of whether it is a physical network or virtual network with physical hardware or virtualized 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 ISO-NE NYISO NextERA Con-Ed and HQ	
Answer	Yes
Document Name	
Comment	
It is difficult to answer this question because it is not completely clear what the proposed R1.7 requires. Shouldn’t this be “only necessary inbound and outbound communication outside the ESZ”? It seems that using “Cyber Asset(s)” could require inbound and outbound controls between two VM’s in the same ESZ. The applicability for this is for BCS in a multi-instance environment. It is seems that both a single VM and an ESZ could meet the definition of “instance”.	
Likes 0	
Dislikes 0	
Response	
Shelby Wade - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company	
Answer	Yes
Document Name	
Comment	
While we support this concept, please see comment under question 24.	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	

Comment	
AZPS reiterates its comments regarding the revision of multi-instance to multi-tenant.	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
BPA appreciates that this is objectives-based language. Measures should be descriptions of controls used to provide the separation, not lists of inbound and outbound access ports. These are not ESPs with EAPs.	
Likes 0	
Dislikes 0	
Response	
Chantal Mazza - Hydro-Qu?bec TransEnergie - 2 - NPCC	
Answer	Yes
Document Name	
Comment	
It is difficult to answer this question because it is not completely clear what the proposed R1.7 requires. Shouldn't this be "only necessary inbound and outbound communication outside the ESZ"? It seems that using "Cyber Asset(s)" could require inbound and outbound controls between two VM's in the same ESZ. The applicability for this is for BCS in a multi-instance environment. It is seems that both a single VM and an ESZ could meet the definition of "instance".	
Likes 0	
Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3,5	

Answer	Yes
Document Name	
Comment	
We support BPA's comment.	
Likes 0	
Dislikes 0	
Response	
Bob Case - Black Hills Corporation - 1 - WECC	
Answer	Yes
Document Name	
Comment	
We agree with the direction of 1.7 but would request more details on implementation and requirements. Technical control definition could have unintended impacts and not provide any greater security controls.	
Likes 0	
Dislikes 0	
Response	
Lauren Price - ATCO Electric - 1 - MRO,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4, Group Name FirstEnergy Corporation	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Robert Ganley - Long Island Power Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joel Charlebois - AESI - Acumen Engineered Solutions International Inc. - 5	
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	
Scott Downey - Peak Reliability - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE does not have comments on this question.	
Likes 0	
Dislikes 0	
Response	

Jack Cashin - American Public Power Association - 4	
Answer	
Document Name	
Comment	
APPA suggests removing the ESZ and replacing it with “Implement technical controls that enforce only necessary inbound and outbound communication between the separated management and data planes of Cyber Asset(s) residing in a multi-instance environment.”	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	

9. Do you agree that the proposed CIP-005 Requirement R1, Part 1.8 provides sufficient security control to reduce the risks associated with shared multi-instance environments? If not, please provide a rationale to support your position.

Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric

Answer	No
Document Name	

Comment

This is still not clear and does not even match the diagram given. The problem with the current definition is that it does not account for the fact that I may have multiple virtual servers on the same VLAN defined within the Hypervisor that are still in the same ESP, but not part of the BES Cyber System (e.g. a PCA that is taking advantage of the Virtual Environment). Instead, this should be used:

1. The BES Cyber System, the management plane of the shared infrastructure, and any hosted Cyber Assets not part of a BES Cyber Systems shall all be separated using an ESP defined virtually within the Virtual environment or using physical equipment linked to the virtual environment; and
2. Communications between the BES Cyber System and any hosted Cyber Assets not part of the same ESP shall all be denied by default.

Likes 0	
Dislikes 0	

Response

Richard Kinas - Orlando Utilities Commission - 3,5

Answer	No
Document Name	

Comment

There are discrepancies between the language in the Part 1.8 and in the question. Question identifies “shared multi-instance environments “ where the requirement does not. We recommend that the SDT provide guidance on what is infrastructure (possibly using language such as BES related infrastructure) and suggest that the SDT define “Multi-instance”.

If a Jump-host (a required security control for IRA for High BESCS) which is outside of the ESP, then requirement would not be applicable. (remember that EACMs will be split—EAC and EAM). If the Jump-host was on the VM infrastructure is this a multi-instance environment?

Question—how much security do you have to implement (how many firewalls? Reside in same physical location? Trade ease of administration for security…trying to balance it; how far do you have to go to prove that it is “secured”; each environment is different.

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer	No
Document Name	

Comment

Logical separation and “deny by default” communications are insufficient to ensure complete separation of two environments. Suggested rewording:

When an infrastructure is shared between BES Cyber Systems and other Cyber Assets not part of a BES Cyber System:

1. The BES Cyber System, the management plane of the shared infrastructure, and any hosted Cyber Assets not part of a BES Cyber Systems shall all be separated. Such separation shall achieve the objective of preventing data leakage across the separation. Such separation shall also achieve the objective of preventing code, malicious or otherwise, from migrating across the separation; and

2. Communications, if any, between the BES Cyber System and any hosted Cyber Assets not part of a BES Cyber System shall be through a defined Electronic Access Point.

Likes 0	
Dislikes 0	

Response

Mike Smith - Manitoba Hydro - 1,3,5,6

Answer	No
Document Name	

Comment

Given that the modified Cyber Asset definition includes physical and virtual devices, this requirement will apply to physical cyber system as well. For the existing EACMS, PACS and PCA that are sharing the same network infrastructure, please clarify if now they need to be separated from the BES Cyber Systems. Please define what constitutes a separation and whether the separation means the authentication, inbound and outbound access control or both. Please clarify how a BES Cyber System achieves denied by default and whether it means no listening ports are allowed.

Likes 0	
Dislikes 0	

Response

Janis Weddle - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Chelan PUD

Answer	No
Document Name	

Comment

As with the comments provided for #8 above, the term Electronic Security Zone should be explicitly used, i.e. “The BES Cyber System, the management plane of the shared infrastructure, and any hosted Cyber Assets not part of a BES Cyber System shall reside in separate ESZs”.

Additionally, this requirement does not account for Protected Cyber Assets which may need to reside within the Electronic Security Perimeter and Electronic Security Zone with the BES Cyber Assets they are associated with but do not meet the criteria for classification, or BES Cyber Assets that are treated as such because of high-water marking.

This requirement would be unecessary if the ESZ definition were amended as listed in #8 above.

Likes 0	
Dislikes 0	

Response

Bob Case - Black Hills Corporation - 1 - WECC

Answer	No
Document Name	

Comment

Although this would be acceptable for EACMS and PACS (multi-instance virtual), hardware separation should be required for BCS.

Likes 0	
Dislikes 0	

Response

Brandon McCormick - Florida Municipal Power Agency - 3,4,5,6 - FRCC, Group Name FMPA

Answer	No
Document Name	2016-02_Virtualization_Unofficial Comment Form_FMPA_comments.docx

Comment

Please see attached comments

Likes 0	
Dislikes 0	

Response

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

Answer	No

Document Name	
Comment	
CenterPoint Energy does not believe this requirement is necessary because part 2 of proposed CIP-005 R1.8 is redundant to the existing deny by default requirement in CIP-005 Requirement R1.3.	
Likes 0	
Dislikes 0	
Response	
Don Schmit - Nebraska Public Power District - 1,3,5	
Answer	No
Document Name	
Comment	
Refer to question #23 comments.	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	
N&ST believe the proposed wording does not address the scenario depicted in the diagram that accompanies the narrative preceding proposed Part 1.8. Suggested rewording: “When a virtual computing infrastructure is shared between BES Cyber Systems within an ESP and other Cyber Assets outside of that ESP, the hosting virtual infrastructure shall be configured so that: (1) the infrastructure’s management plane is entirely within the ESP, (2) the infrastructure’s management plane is in a separate ESZ from both the BES Cyber Systems and other Cyber Assets that share the infrastructure, (3) communications between BES Cyber Systems and other hosted Cyber Assets that are outside of the ESP are denied by default, and (4) any and all allowed communications between BES Cyber Systems and other hosted Cyber Assets that are outside of the ESP must take place through a defined EAP."	

Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No
Document Name	
Comment	
TVA supports flexibility within the standard to accommodate a multi-tenant architecture and the benefits provided by adaptation of industry standard architectures, such as on premises cloud computing and hyper-converged infrastructures. The ESZ concept, as presented, is overly complex, and lacks clarity to help entities how to institute separation between tenants, and shared underlying physical compute resources, whether processor (compute), storage, or transport (network). In the language provided, it is unclear as to the target of the separation (e.g., specific groups of Cyber Assets). Policies and procedures to restrict storage of VM images and snapshots do not exist. Formal change management processes that govern image creation, security, distribution, storage, use, retirement, and destruction must be created or incorporated into the existing NERC CIP controlled change management process. Additional security monitoring and control of stored images and snapshots should be implemented. This requirement does not cover striping of BES data, where system information may cross multiple volumes and assets.	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
What does the SDT mean when referencing Multi-Instance in the diagram above? Is this supposed to be referencing a cluster?	
Likes 0	
Dislikes 0	
Response	
John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	No
Document Name	

Comment	
Tacoma Power supports comments submitted by APPA.	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	No
Document Name	
Comment	
The SPP Standards Review Group has the concern with the proposed language that the drafting team is presenting at this point. From our perspective, the language is suggesting coverage of other infrastructure besides Virtualization. If that’s the drafting team’s intent, we recommend that the drafting team provides support details to help inform the industry on their direction for this process.	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	No
Document Name	
Comment	
The term "management plane" needs to be further defined in this section before being able to state agreement. The word "separated" is important and is not fully understood. Xcel Energy suggests adding the term "logically" before the term separated in #1 of Part 1.8.	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	No
Document Name	

Comment	
Comments: Frankly, it would almost be preferable that shared infrastructure not be allowed in the sense indicated, than to impose such controls on virtualized systems.	
Likes 0	
Dislikes 0	
Response	
Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - FRCC,MRO,WECC,Texas RE,SERC,SPP RE, Group Name Southern Company	
Answer	No
Document Name	
Comment	
Southern Company requests additional clarification on why the management plane must reside fully within the ESP? Additionally, a description of the ESZ applicable to the example diagram would help clarify the concepts behind the proposed requirement. Southern has concerns that, if the management plane must reside fully within the ESP, the gains proposed for an Entity “to leverage the investments and protection of infrastructure shared between applicable Cyber Assets and other programmable devices” might not be realized due to the compliance burden of doing so. As stated in question 8, Part 2 of the proposed requirement needs additional clarification with regard to the use of the term “communications”. Is Part 2 of the requirement analogous to firewall rule base language, is it also applicable to shared SAN, fiber, etc. resources, and how is that expected to be implemented with regard to all forms of “communication”?	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	
Reclamation does not support the addition of Part 1.8. Reclamation recommends that revising the definition of BES Cyber System and the Impact Rating Criteria will provide sufficient security controls and reduce the risks associated with shared multi-instance environments. Refer to the principles, recommended definitions, rationale, and recommended Impact Rating Criteria described in the response to Question 24.	
Likes 0	
Dislikes 0	
Response	

Lauren Price - ATCO Electric - 1 - MRO,RF	
Answer	No
Document Name	
Comment	
ATC proposes changing the language for CIP-005 Requirement R1, Part 1.8 #2 to say - “Communications between the BES Cyber System and any hosted Cyber Assets not part of the BES Cyber System shall be denied by default unless explicitly allowed through an EAP.” This would allow required communications for devices inside and outside of the ESP to talk to each other.	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 3,5	
Answer	No
Document Name	
Comment	
AEP agrees with R1, Part 1.8 as written. (Note that Transmission’s current VM environment does not have BES Cyber Systems and NON-BES Cyber Assets shared on the same Host/Hypervisor. The BES Cyber Systems are hosted on separate hypervisors (physical servers). AEP believes the existing requirements can be determined to be applicable in a virtual environment by a reasonable person. New requirements are not necessary.	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8,9 - WECC	
Answer	No
Document Name	
Comment	
SDG&E does not agree that the proposed requirement provides sufficient security. Communications is too vague of a term, Storage is not sufficiently addressed in this control and the administrative overhead to deny by default is considerable in a shared multi-instance infrastructure.	
Likes 0	
Dislikes 0	

Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE	
Answer	No
Document Name	
Comment	
Current Standards Already Address Risk. Proposed Part 1.8 is seeking to address the risk described and illustrated in the diagram. The risk is already addressed, or can be addressed by, using current CIP Standards.	
Likes 0	
Dislikes 0	
Response	
John Tolo - Unisource - Tucson Electric Power Co. - 1	
Answer	No
Document Name	
Comment	
We understand the intent here builds upon previous concepts, however as stated before, “separation” is too vague. Your diagram illustrates a “high watermark” approach to where you place the management system and the diagram illustrates your intent better than the words.	
Likes 0	
Dislikes 0	
Response	
Ronald Donahey - TECO - Tampa Electric Co. - 1,3,5,6	
Answer	No
Document Name	
Comment	
There are discrepancies between the language in the Part 1.8 and in the question. The Question identifies “shared multi-instance environments“ where the requirement does not. We recommend that the SDT provide guidance on what is infrastructure (possibly using language such as BES related infrastructure) and suggest that the SDT define “Multi-instance”.	

If a Jump-host (a required security control for IRA for High BESCS) which is outside of the ESP, then requirement would not be applicable. (remember that EACMs will be split—EAC and EAM). If the Jump-host was on the VM infrastructure is this a multi-instance environment? Question—how much security do you have to implement (how many firewalls? Reside in same physical location? Trade ease of administration for security…trying to balance it; how far do you have to go to prove that it is "secured"; each environment is different.	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	No
Document Name	
Comment	
The separation methodology is not described in sufficient detail to determine if the security control objective is achieved.	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5	
Answer	Yes
Document Name	
Comment	
Provide clarification around the use of Virtual EAPs in the same multi-instance environment separating BCAs and non-CIP devices.	
Likes 0	
Dislikes 0	
Response	
Joel Charlebois - AESI - Acumen Engineered Solutions International Inc. - 5	
Answer	Yes
Document Name	
Comment	

Yes, but it is unclear where the CMS should/must reside. The management plane is inside the ESP, but is the implication that the CMS is also inside the ESP or some equivalent ESZ meant for CMS? Putting the CMS outside a protected area such as an ESP/ESZ increases the risk to the BCS and an EAP between the CMS and the management plane reduces some of the risk, but not all.	
Likes 0	
Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3,5	
Answer	Yes
Document Name	
Comment	
We support BPA comment.	
Likes 0	
Dislikes 0	
Response	
Chantal Mazza - Hydro-Qu?bec TransEnergie - 2 - NPCC	
Answer	Yes
Document Name	
Comment	
Request clarification of “infrastructure.” Does infrastructure refer to only the virtual environment? Is this the “infrastructure” in the Virtualization Terms and Requirements section of the comment form which only listed virtual components? Could “infrastructure” mean the UPS systems, equipment racks, HVAC systems, floors, lighting…. The “management plane of the shared infrastructure” seems to limit and define “infrastructure” to be components of the virtual environment. Should 1 be “logically separated” and not just “separated”? Consider striking “by default.” This Part is the foundation for virtualization requirements.	
Likes 0	
Dislikes 0	

Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
BPA appreciates the SDT's effort in drafting objectives-based standards language. BPA agrees that Part 1.8 provides necessary additional security controls for shared infrastructure by separating hosted cyber assets that are not part of BES Cyber Systems as part of a comprehensive security strategy.	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
AZPS agrees with CIP-005 R1.8, section 1 that there should be separation between the BES Cyber System, the management plane and any other Cyber Assets not part of the BES Cyber System. AZPS encourages the SDT to consider revising CIP-005-5 R1.1 to state that a defined ESP can exist within a multi-instance environment. In the event that the SDT retains section 2 of CIP-005 R1.8, AZPS respectfully recommends having this requirement applicable to only EACMS, CMS, and PACS, and keep CIP-005 R1.1-1.3 applicable to only high and medium impact BES Cyber Assets.	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4, Group Name FirstEnergy Corporation	
Answer	Yes
Document Name	
Comment	
Recommend inserting the word "logically" before separated in the Requirement.	

Likes 0	
Dislikes 0	
Response	
David Francis - Midcontinent ISO, Inc. - 2,3 - MRO,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG	
Answer	Yes
Document Name	
Comment	
• Where does an ESZ apply to the diagram? • Without this requirement, there really is no value in writing requirements for virtualization. This will help entities better utilize converged infrastructure	
Likes 0	
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
ERCOT notes that without this requirement, there really is no value in writing requirements for virtualization. This will help entities better utilize converged infrastructure. However, ERCOT seek clarification on how an ESZ applies to the diagram above.	
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 ISO-NE NYISO NextERA Con-Ed and HQ	
Answer	Yes
Document Name	
Comment	
Request clarification of “infrastructure.” Does infrastructure refer to only the virtual environment?	

Is this the “infrastructure” in the Virtualization Terms and Requirements section of the comment form which only listed virtual components? Could “infrastructure” mean the UPS systems, equipment racks, HVAC systems, floors, lighting…. The “management plane of the shared infrastructure” seems to limit and define “infrastructure” to be components of the virtual environment.

Should 1 be “logically separated” and not just “separated”?

Consider striking “by default.”

This Part is the foundation for virtualization requirements.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

Alliant Energy agrees there should be separation between the BCS, the management plane, and any hosted Cyber Assets not part of a BCS. It should be more clear in the requirement whether separation between all 3 categories are required.

Communications between BCS and non-BCS is already required go through an EAP and to be denied by default per CIP-005-5 R1.3.

Likes 0	
Dislikes 0	

Response

David Ramkalawan - Ontario Power Generation Inc. - 5

Answer	Yes
Document Name	

Comment

It is not certain what is meant by “separated”. Is this meant in the networking sense? Or in an ESZ sense?

Likes 0	
Dislikes 0	

Response	
Scott Downey - Peak Reliability - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Robert Ganley - Long Island Power Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Shelby Wade - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	
Document Name	
Comment	
The guidance provided above in the question, states: “In order to manage Partition 2, or any Cyber Asset hosted by the multi-instance environment and outside the ESP, IP communication to the management plane from outside the ESP has to go through the EAP since the management plan of shared	

multi-instance environment has to reside inside the ESP.” APPA believes that the Requirement does not address the management plane inside the ESP. Consequently, APPA believes both aspects should be included in this Requirement. The proposed language in Question 8 would eliminate the need for the “denied by default” in R1.8.2. The word “infrastructure” is not defined in the proposed Standard. Consequently, the “infrastructure” on page 4 appears to only include virtual components. APPA questions if this would also include the UPS systems, equipment racks, HVAC systems, floors, lighting, etc.? The “management plane of the shared infrastructure” seems to limit and define “infrastructure” to be components only of the virtual environment.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE does not have comments on this question.	
Likes 0	
Dislikes 0	
Response	
Paul Haase - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light	
Answer	
Document Name	
Comment	
City Light, as above, supports the concept but not the specific wording or detail. Again, Cyber Assets must be modified as "applicable" or "virtual" Cyber Assets. City Light supports APPA's comments about this requirement, which also acknowledging the value of BPA's comments.	
Likes 0	
Dislikes 0	
Response	

10. The SDT asserts that the proposed CIP-005 Requirement 1, Part 3.1 provides additional security controls for remote access when performing CMS functions. These are necessary to reduce the risk associated with remote access to multi-instance environments. Do you agree with this assertion? If not, please provide a rationale to support your position.

Paul Haase - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light

Answer	No
Document Name	

Comment

City Light generally supports the security enhancements proposed in this requirement for virtual systems, but is concerned about expanding scope for non-virtual systems (which is not the mandate of this SDT). Such changes should be handled in a more transparent manner and not included as a minor change within a major new concept.

City Light additionally supports the comments of both APPA and BPA, except as noted above.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Alliant Energy disagrees with the phrase "initiated outside of the ESZ." Access to perform CMS functions should be controlled regardless of source.

Likes 0	
Dislikes 0	

Response

Ronald Donahey - TECO - Tampa Electric Co. - 1,3,5,6

Answer	No
Document Name	

Comment

As CIP-005 Requirement 1, Part applies to remote access, we considered that authentication takes place to the application or the management interface not to the communication. Authentication may be considered to be digital certificates for layer 2 tunnel. The requirement as written states for all sessions. Meaning each session established must perform the requirement, which may prevent an entity from using a layer 2 tunnel to perform this activity depending on particular vendor implementation.

The SDT should add Implementation Guidance that digital certificates meet the “authentication, integrity and non-repudiation controls”. The requirement does not prescribe where they have to terminate. Could be to the jump host—then connect to CMS to perform CMS functions.   If the communication is scheduled via scripts – first attempt to define either user initiated or system-to-systems communications? As it is currently written, any communication between device and CMS might have to meet the requirement. CMS should include administration….not with configuration, otherwise unintended systems are brought in (ivanti, Solar Winds)

Should include the virtual concept in that definition/term. The following is a potential definition for consideration by the SDT:

“Hypervisor or products with other similar functionality”

As CIP-005 Requirement 1, Part applies to remote access, we considered that authentication takes place to the application or the management interface not to the communication. Authentication may be considered to be digital certificates for layer 2 tunnel. The requirement as written states for all sessions. Meaning each session established must perform the requirement, which may prevent an entity from using a layer 2 tunnel to perform this activity depending on particular vendor implementation.

The SDT should add Implementation Guidance that digital certificates meet the “authentication, integrity and non-repudiation controls”. The requirement does not prescribe where they have to terminate. Could be to the jump host—then connect to CMS to perform CMS functions.   If the communication is scheduled via scripts – first attempt to define either user initiated or system-to-systems communications? As it is currently written, any communication between device and CMS might have to meet the requirement. CMS should include administration….not with configuration, otherwise unintended systems are brought in (ivanti, Solar Winds)

Should include the virtual concept in that definition/term. The following is a potential definition for consideration by the SDT:

“Hypervisor or products with other similar functionality”

A hypervisor or virtual machine monitor (VMM) is a piece of **computer software**, firmware or hardware that creates and runs virtual machines. A computer on which a hypervisor is running one or more virtual machines is defined as a host machine.

Likes 0	
Dislikes 0	

Response

John Tolo - Unisource - Tucson Electric Power Co. - 1

Answer	No
Document Name	

Comment

This would be difficult to implement in practice for many types of assets and their integrations and management systems. Non-repudiation generally requires some type of cryptographic signature and a majority of system-to-system communications inherently do not support that mechanism. Requiring it for Interactive Remote Access for a CMS makes sense, but we imagine that will be enumerated in existing standards as in-scope for CMS the way it would be in-scope for PACS, as an example.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE

Answer	No
Document Name	

Comment

Proposed Part 1.7 incorporates the proposed terms CMS and ESZ. See our responses to the proposed CMS definition, Question 4, and the proposed ESZ, Question 5. Also, we do not see that the concerns regarding the proposed CMS and ESZ definitions would apply any differently in proposed CIP-005 R1, Part 3.1.

Alternative. If the SDT concludes proposed Part 1.7 is required to address the identified issues, an alternative approach is to maintain the Interactive Remote Access requirements and incorporate relevant concepts contemplated by the CMS requirements.

Likes 0	
Dislikes 0	

Response

Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8,9 - WECC

Answer	No
Document Name	

Comment

See earlier requirement of clarification of where the CMS resides in this control as well as stronger definition of non-repudiation of system-to-system communication.

Likes 0	
Dislikes 0	

Response

Aaron Austin - AEP - 3,5

Answer	No
Document Name	

Comment

AEP believes the existing requirements can be determined to be applicable in a virtual environment by a reasonable person. New requirements are not necessary. However, further clarification is needed for the terms “Authentication, Integrity, and Non-Repudiation” in the compliance guidance.

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 ISO-NE NYISO NextERA Con-Ed and HQ

Answer	No
Document Name	

Comment

Is this redundant with CIP-005, Requirement 1, Part 1.3?

Request specifics on “authentication, integrity and non-repudiation controls.”

Please clarify if non-repudiation controls is a technical control. If YES, are we moving too far away from outcome based controls?

This requirement may need to include the “per device capability” phrase.

Likes 0

Dislikes 0

Response

Wendy Center - U.S. Bureau of Reclamation - 1,5

Answer	No
Document Name	

Comment

Reclamation does not support the addition of Part 3.1. Reclamation recommends that revising the definition of BES Cyber System and the Impact Rating Criteria will provide sufficient security controls to reduce the risk associated with remote access to multi-instance environments. Refer to the principles, recommended definitions, rationale, and recommended Impact Rating Criteria described in the response to Question 24.

Likes 0

Dislikes 0

Response

Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
ERCOT asserts that this requirement is redundant to the existing firewall requirement in CIP-005 Requirement R1, Part 1.3. As written, ERCOT offers the following comments. (1) The requirement lacks complete and appropriate details necessary for evaluation and implementation. (2) The requirement may create conflict with existing CIP Version 5/6 implementations. (3) While the security controls may be appropriate, the technologies may not support all or some of the requirement. Clarification for network verses host technologies is required. (4) The requirement does not specify it is for multi-instance. (5) The SDT should be specific about the meaning of “authentication, integrity and non-repudiation controls”. Are these existing controls in the CIP standards for non-virtual systems? (6) With non-repudiation, the SDT appears to be adding an additional requirement for key management that is not clearly stated. (7) As noted in question 8, ERCOT requests examples of systems that can basically “firewall” non-routable protocols. ERCOT recommends the creation of ERO-endorsed guidance before standards to aid in evaluating options. The guidance can document the implementation under various vendor and technology types.	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	No
Document Name	
Comment	
Comments: Singling out virtualized environments for special controls seems unnecessary. Surely remote access rights and rules could be based on the nature and quantity of what cyber assets could be affected regardless of their physical or virtual nature.	
Likes 0	
Dislikes 0	
Response	
David Francis - Midcontinent ISO, Inc. - 2,3 - MRO,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG	
Answer	No
Document Name	
Comment	

- This is redundant to the existing firewall requirement in CIP-005 Requirement R1, Part 1.3.
- Examples of systems that can basically “firewall” non-routable protocols would be helpful.
- The requirement does not specify it is for multi-instance.
- Be specific about what is meant by “authentication, integrity and non-repudiation controls”. Are these existing controls in the CIP standards?
- With non-repudiation, are you requiring key management, etc. in a backdoor manner?

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Not sure how "non-repudiation controls" applies in this part 3.1. Xcel Energy suggests that the term "integrity" be further defined. For example, does it mean traffic must be encrypted or does it have other mechanisms to validate and authenticate the communication? Additional technical guidance will be needed to understand the differences between this and Interactive Remote Access.

Likes 0	
Dislikes 0	

Response

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group

Answer	No
Document Name	

Comment

The SPP Standards Review Group has a concern on how the terms “ESP” and “ESZ” are used in this section of the documentation while discussing the risks associated with communication. At this point, we feel that there is no consistency in reference to the use of the terms. For example, the supporting details for the section mentions “ESP” while language in Part 3.1 mentions “ESZ”.

Question:

What are the drafting team’s expectation in reference to meeting the compliance need of the terms “integrity” and “non-repudiation” controls?

Will the drafting team have the expectation of all system to system communication outside of the ESZ to communicate with system inside of the ESZ to be encrypted?

Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4, Group Name FirstEnergy Corporation	
Answer	No
Document Name	
Comment	
Consider defining “integrity” and “non-repudiation controls” in the context of this Requirement.	
Likes 0	
Dislikes 0	
Response	
Chantal Mazza - Hydro-Qu?bec TransEnergie - 2 - NPCC	
Answer	No
Document Name	
Comment	
Is this redundant with CIP-005, Requirement 1, Part 1.3? Request specifics on “authentication, integrity and non-repudiation controls.” Please clarify if non-repudiation controls is a technical control. If YES, are we moving too far away from outcome based controls? This requirement may need to include the “per device capability” phrase.	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No
Document Name	
Comment	

TVA requests additional context for understanding the proposed requirement. If an entity has multiple ESZs and/or ESPs, it is unclear how an entity would satisfy the proposed language. Network traffic traversing does not identify itself on a technical level as being interactive or machine-to-machine. Unless an entity has implemented software defined networking, which can associate traffic flows to and process identity end-to-end, it is difficult to envision a technical solution that satisfies the draft language.

Likes 0	
Dislikes 0	

Response

Nicholas Lauriat - Network and Security Technologies - 1

Answer	No
Document Name	

Comment

While N&ST agrees there should be strong technical and procedural protections around hypervisors, N&ST does not believe this goal is well-served by the proposed requirement and is not convinced there are “gaps” in the current requirements for Interactive Remote Access. In addition, N&ST notes:

(1) The narrative section preceding the proposed requirement discusses CMS access from outside an ESP, whereas the proposed requirement language says, “ESZ.”

(2) Authentication is already required for access by human operators.

(3) System-to-system communications from outside an ESP are already subject to controls implemented by EAPs.

(4) It is unclear what type of “integrity” control(s) the SDT envisions in this context.

(5) It is unclear what goal(s) would be served by “non-repudiation,” nor is it clear how it might be achieved in this context. Perhaps all CMS transactions should be logged, with an accompanying requirement that the entity be capable of determining what individual or system initiated any given recorded transaction.

Likes 0	
Dislikes 0	

Response

Don Schmit - Nebraska Public Power District - 1,3,5

Answer	No
Document Name	

Comment

Refer to question #23 comments.

Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
CenterPoint Energy does not agree with the proposed requirement because of the difficulty in implementation and demonstration of compliance. It is not clear how an entity can distinguish between sessions used for CMS functions and those that are not. Further, it may be challenging to distinguish between user initiated and system-to-system sessions, when such communications are allowed between the hosts, ports, and applications involved. Further, it does not account for system capability. The requirement can be even more challenging to comply with if the logical separation in the ESZ is not through a firewall.	
Likes 0	
Dislikes 0	
Response	
Brandon McCormick - Florida Municipal Power Agency - 3,4,5,6 - FRCC, Group Name FMPA	
Answer	No
Document Name	2016-02_Virtualization_Unofficial Comment Form_FMPA_comments.docx
Comment	
Please see attached comments	
Likes 0	
Dislikes 0	
Response	
Bob Case - Black Hills Corporation - 1 - WECC	
Answer	No
Document Name	
Comment	

There has not been enough definition around ESZ’s and if they exist inside or outside of a ESP. The required controls are vague and poorly defined. We do not recognize a gap in the intermediate system. The CMS should always reside inside the ESP on separated hardware. This alleviates the remote access to perform CMS function gap.	
Likes 0	
Dislikes 0	
Response	
Janis Weddle - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Chelan PUD	
Answer	No
Document Name	
Comment	
The language of the proposed requirement is unclear as to what communications this applies to. Does it apply to the client connection to the CMS, or to the CMS connection to the BES Cyber Asset? The language of this requirement is also not consistent with the rationale given, as the rationale describes issues with communications from outside the ESP, but the requirement addresses the ESZ.	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	No
Document Name	
Comment	
The gap identifed by the STD is not defined and needs further clarification. As we proposed EACMS modification that includes CMS in question 4, this requirement is not necessary since the current EACMS requirements can meet this.	
Likes 0	
Dislikes 0	
Response	
Richard Kinas - Orlando Utilities Commission - 3,5	
Answer	No
Document Name	

Comment	
As CIP-005 Requirement 1, Part 3. Applies to remote access, we considered that Authentication takes place to the application or the management interface not to the communication. Authentication may be considered to be digital certificates for layer 2 tunnel. The requirement as written states for all sessions. Meaning each session established must perform the requirement, which may prevent an entity from using a layer 2 tunnel to perform this activity depending on particular vendor implementaions. The SDT should add Implementation Guidance that digital certificates meet the “authentication, integrity and non-repudiation controls”. The requirement does not prescribe where they have to terminate. Could be to the jump host—then connect to CMS to perform CMS functions. If the communication is scheduled via scripts – first attempt to define either user initiated or system-to-systems communications? As it is currently written, any communication between device and CMS might have to meet the requirement. CMS should include administration….not with configuration, otherwise unintended systems are brought in (ivanti, Solar Winds)	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	No
Document Name	
Comment	
It is acceptable if ESZ was replaced with ESP.	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Shelby Wade - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company	
Answer	Yes
Document Name	
Comment	
We do agree that Part 3.1 provides additional security controls for remote access; however, the Applicable Systems should be updated to say “high and medium impact BES Cyber Systems residing in a multi-instance environment and their associated CMS(s)”.	
Likes 0	
Dislikes 0	
Response	
John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
Tacoma Power supports comments submitted by APPA.	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy agrees that controls are necessary, but do not feel that the proposed language clearly explains what controls should be implemented, and where said controls should be implemented as well. As written, it isn’t clear what the SDT intends to be implemented.	
Likes 0	
Dislikes 0	
Response	

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
BPA appreciates efforts to align NERC CIP standards with recognized cyber security principles and objectives.	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Stronger language is needed to bring authentication up to at least the level required for Interactive Remote Access.	
Likes 0	
Dislikes 0	
Response	
Joel Charlebois - AESI - Acumen Engineered Solutions International Inc. - 5	
Answer	Yes
Document Name	
Comment	
Yes but this may not be enough – e.g., the system-to-system communications between an out of ESZ CMS and the management plane may in fact meet all of the items in part 3.1, but if the CMS is already compromised (which is more likely if it is not in the ESZ) then these controls do nothing to prevent the attacker controlling the CMS from causing damage.	
Likes 0	
Dislikes 0	
Response	
Lauren Price - ATCO Electric - 1 - MRO,RF	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - FRCC,MRO,WECC,Texas RE,SERC,SPP RE, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Robert Ganley - Long Island Power Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
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	
Scott Downey - Peak Reliability - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE does not have comments on this question.	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	
Document Name	
Comment	

Public power believes that this Requirement conflicts with the implied requirement identified in comments to question 8 that the management plane of the BCS must be inside the ESZ. APPA recommends replacing the proposed language with: “Require authentication, integrity and non-repudiation controls for all CMS functions, per device capability.” If the suggested modification is not used, in the alternative APPA proposes that this Requirement have the “per device capability” clause. Encryption of network traffic form CMS to device could make compliance with this Requirement impossible to achieve.	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	

11. Should the gap between Interactive Remote Access and system-to-system communication that was exposed by the examination of the risks inherent to virtualization be addressed for systems other than high and medium impact BES Cyber Systems residing in a multi-instance environment and their associated CMS? If not, please provide a rationale to support your position.

Teresa Cantwell - Lower Colorado River Authority - 1,5	
Answer	No
Document Name	
Comment	
This question is unclear – please provide clarification. Is this about Lows? Is it about non-multi-instance Highs and Mediums? Both? Etc.	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	No
Document Name	
Comment	
We proposed EACMS modification including the cyber system that can alter the configuration of BCS regardless of whether it has IRA or system-to-system access to the BCS that resides inside or outside ESZ.	
Likes 0	
Dislikes 0	
Response	
Janis Weddle - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Chelan PUD	
Answer	No
Document Name	
Comment	
System-to-system communications should be addressed the same as CIP-005-5 R2.	
Likes 0	
Dislikes 0	

Response	
Bob Case - Black Hills Corporation - 1 - WECC	
Answer	No
Document Name	
Comment	
SDT’s example of CMS in a virtualized high/medium impact environment should not be permitted.	
Likes 0	
Dislikes 0	
Response	
Brandon McCormick - Florida Municipal Power Agency - 3,4,5,6 - FRCC, Group Name FMPA	
Answer	No
Document Name	2016-02_Virtualization_Unofficial Comment Form_FMPA_comments.docx
Comment	
Please see attached comments	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
CenterPoint Energy believes the requirement should be limited to the highest risk BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response	

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

Answer	No
Document Name	

Comment

TVA requests that any controls associated with the use of a CMS apply to individuals' access to the CMS itself, rather than the network traffic that may originate from a CMS to an applicable BES Cyber Asset. Network traffic traversing does not identify itself on a technical level as being interactive or machine-to-machine. Unless an entity has implemented software defined networking which can associate traffic flows to and process identity end-to-end, it is difficult to envision a technical solution that satisfies the draft language. As a case study, consider a CMS tool used to manage network devices (e.g., routers, firewalls, switches) via SSH. The tool may have a daily backup configured whereby it initiates an SSH session to a target device for the purposes of collecting a complete device backup. The SSH traffic, from a firewall and access control perspective, cannot be identified as “machine to machine”, even though no human is interactively driving the SSH session. However, the same CMS tool may facilitate real time, Interactive Remote Access to a target device where each command was issued by a human facilitated by an SSH connection. From a network perspective, the SSH session’s origin as human or machine-to-machine is indistinguishable.

TVA suggests a more effective manner to address these concerns would be to utilize controls similar to those used for gaining access to an Intermediate System for remotely gaining access to a CMS.

Finally, TVA suggests the concerns about “the gap between Interactive Remote Access and system-to-system communication” are not proprietary to virtualized environments. The use of CMS tools can be manifest with or without virtualized technologies.

Likes 0	
Dislikes 0	

Response

Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6

Answer	No
Document Name	

Comment

AZPS agrees that the gap should be addressed for the applicable systems that are high and medium impact BES systems, but does not agree that the gap should be addressed for low impact BES cyber systems.

Likes 0	
Dislikes 0	

Response

Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy

Answer	No
Document Name	

Comment	
The gap between Interactive Remote Access, and system-to-system communication does not need to be addressed for systems other than high and medium impact BES Cyber Systems. Outside of the multi-instance environment, the risk associated with system to system for individual discrete assets is limited to within the company's environment. Anything outside of the company's environment should be covered under CIP-012.	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4, Group Name FirstEnergy Corporation	
Answer	No
Document Name	
Comment	
There is not an inherent risk for system-to-system communication. If the gap is addressed, please ensure that the compliance Requirements do not apply to Low Impact BES Cyber Systems nor to systems that are out-of-scope.	
Likes 0	
Dislikes 0	
Response	
David Francis - Midcontinent ISO, Inc. - 2,3 - MRO,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG	
Answer	No
Document Name	
Comment	
IRA only applies to Cyber Assets within an ESP. Requiring this for EACMS will lead to the "hall of mirrors" issues. This is another reason that CMS devices should be classified as a BCA if they support a BCA.	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	No
Document Name	

Comment	
Comments: It would seem wise to resolve issues with high and medium impact BES Cyber Systems before addressing low if there is inherent risk to virtualization greatly exceeding that posed by any systems using shared resources whether physical or virtual. The idea occurs that the inherent potential reduction in risk provided by virtualization be properly weighed as well as so much redundancy can be built into these systems.	
Likes 0	
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
ERCOT notes that Interactive Remote Access only applies to Cyber Assets within an ESP. Requiring this for EACMS will lead to the “hall of mirrors” issues. This is another reason that CMS devices should be classified as a BCA if they support a BCA.	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	
Reclamation recommends the requirements addressing the risks inherent to virtualization apply only to high and medium impact BES Cyber Systems residing in Multi-Virtual Instance environments and their associated Virtual Centralized Management Systems (VCMS). Refer to the recommended terms and definitions in the responses to Questions 4 and 6.	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 3,5	
Answer	No

Document Name	
Comment	
AEP believes the existing requirements can be determined to be applicable in a virtual environment by a reasonable person. New requirements are not necessary.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE	
Answer	No
Document Name	
Comment	
The question incorporates the proposed CMS term. See our response to the proposed CMS definition, Question 4. Also, Standards are to address risk but cannot address every iteration of risk. To develop requirements to address every security risk is not sustainable and an unreasonable expectation. Security threats emerge more quickly than can be addressed by a process of law.	
Likes 0	
Dislikes 0	
Response	
John Tolo - Unisource - Tucson Electric Power Co. - 1	
Answer	No
Document Name	
Comment	
See comments for #10.	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	No

Document Name	
Comment	
Risk based assessment.	
Likes 0	
Dislikes 0	
Response	
Joel Charlebois - AESI - Acumen Engineered Solutions International Inc. - 5	
Answer	Yes
Document Name	
Comment	
It needs to be addressed for any virtualized PCA, PACS or EACMS as they pose similar risks. It should also be addressed for any similar communications in non-virtualized systems – e.g., a lights out management system for servers or a network management system. These pose similar risks to the BCS they support. This may not be enough to protect the BCS appropriately.	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Robert Ganley - Long Island Power Authority - 1	
Answer	Yes
Document Name	

Comment	
All Cyber Assets in a multi-instance environment and their associated CMS should rise to the highest watermark level in order minimize/mitigate potential risks of cross system compromise.	
Likes 0	
Dislikes 0	
Response	
Don Schmit - Nebraska Public Power District - 1,3,5	
Answer	Yes
Document Name	
Comment	
Refer to question #23 comments.	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	Yes
Document Name	
Comment	
Although N&ST is not necessarily convinced at this time that additional controls are needed for system-to-system communications between BES Cyber Systems and Cyber Assets outside of ESPs, we believe it nonetheless makes sense to examine the question while it is being considered for BES Cyber Systems running in virtual environments.	
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	
John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
Tacoma Power supports comments submitted by APPA.	
Likes 0	
Dislikes 0	
Response	
Shelby Wade - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company	
Answer	Yes
Document Name	
Comment	
We support the concept of reducing the risk associated with remote access (both system-to-system and Interactive); however, we believe those requirements should be appropriate to the risk level of the Cyber Assets (we believe you are looking to address EACM, PACS and Low Impact BES Cyber Systems).	
Likes 0	
Dislikes 0	
Response	
Lauren Price - ATCO Electric - 1 - MRO,RF	
Answer	Yes

Document Name	
Comment	
There is an opportunity to extend these controls out to the CMS of virtualized PACS and EACMS.	
Likes 0	
Dislikes 0	
Response	
Paul Haase - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light	
Answer	Yes
Document Name	
Comment	
City Light agrees additional known risks should be addressed, but disagrees that the virtualization changes are correct forum to make such changes (because of the complexity of the changes for virtualization and the great likelihood that the other changes will be lost in the chaff).	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Kinas - Orlando Utilities Commission - 3,5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chantal Mazza - Hydro-Qu?bec TransEnergie - 2 - NPCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - FRCC,MRO,WECC,Texas RE,SERC,SPP RE, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8,9 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	

Jack Cashin - American Public Power Association - 4	
Answer	
Document Name	
Comment	
The NERC standards should be written to address the known risks and not limited to risks associated with managing multi-instance environments.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE does not have comments on this question.	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	
Document Name	
Comment	
No comment at this time	
Likes 0	
Dislikes 0	
Response	

12. The SDT asserts that the new proposed CIP-004 Requirement R4, Part 4.5, provides additional security control to the electronic and unescorted physical access to multi-instance environment processes which reduces the "too much privilege" risk inherent to virtualization which has been identified. Do you agree with this assertion? If not, please provide a rationale to support your position.

Paul Haase - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light

Answer	No
Document Name	

Comment

City Light agrees with the general principles esoused in this new requirement but finds it, as worded, to be too vague and too subject to auditor intepretation.

Likes 0	
Dislikes 0	

Response

Ronald Donahey - TECO - Tampa Electric Co. - 1,3,5,6

Answer	No
Document Name	

Comment

We recommend the addition of "Per system capability" similar to "per device capability".

Does the SDT consider that AD provides enough of these controls? Can it do "need-to-know, least privilege, and separation of duties"?

Could this requirement part be include with the current CIP-004 R4 Part 4.3 review? Will the applicability extend to BCS and associated EACMs? Associated PACS?

We recommend that this become Requirement 4 Part 4.2 as the Authorization takes place in 4.1; implementation should become 4.2; then the quarterly review is 4.3, etc. We recommend that the SDT shift the CIP-004 R4 Parts to have the steps occur in order of operation. We recommend that the SDT provide guidance to small entities that they may identify each role but may need to (resource constrained) add the same person to each role

Likes 0	
Dislikes 0	

Response

Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE

Answer	No
Document Name	
Comment	
Current Standards Already Address Risk. Proposed Part 4.5 is not significantly different from existing CIP-004 Part 4.1 which already requires a process to authorize based on need. **Compliance Uncertainty.** The terms “need-to-know,” “least privilege,” and “separation of duties,” are currently used in the Standards and, also, open to a broad level of interpretation; as such, they create compliance uncertainty. It is expected that will not change. We do not believe additional prescriptive language or defining the terms is sufficient to mitigate the uncertainty.	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8,9 - WECC	
Answer	No
Document Name	
Comment	
SDG&E seeks to understand where ERC fits into this proposed requirement.	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 3,5	
Answer	No
Document Name	
Comment	
AEP believes the existing requirements can be determined to be applicable in a virtual environment by a reasonable person. New requirements are not necessary.	
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 ISO-NE NYISO NextERA Con-Ed and HQ

Answer	No
Document Name	

Comment

This Requirement seems to expand the scope of Requirements 4.1 – 4.4.

The question asks about “multi-instance.” We recommend the applicability section should be similar to CIP-005 R1.8

It is unclear why virtual systems need additional physical access to the virtual systems.

Request clarification of “separation of duties.”

The entity, as part of their “based on need” approval process for 4.1 could include need-to-know, least privilege, and separation of duties “. This added requirement seems like additional administrative tasks and extends to all BES Cyber systems and not just virtual systems.

Likes 0	
Dislikes 0	

Response

Lauren Price - ATCO Electric - 1 - MRO,RF

Answer	No
Document Name	

Comment

The proposed addition of CIP-004 Requirement R4, Part 4.5 is too broad, and applies to everything including virtualization. If the SDT is trying to reduce the “too much privilege” risk inherent to virtualization, the requirement should be specific about virtualization privileges. As proposed, entities would have to apply these security controls to all BES Cyber Systems.

Likes 0	
Dislikes 0	

Response

Wendy Center - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	
Reclamation does not support the addition of Part 4.5. Reclamation recommends that revising the definition of BES Cyber System and the Impact Rating Criteria will provide sufficient security controls and reduce the “too much privilege” risk inherent to virtualization. Refer to the principles, recommended definitions, rationale, and recommended Impact Rating Criteria described in the response to Question 24.	
Likes 0	
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
ERCOT asserts that the concept noted in this requirement should not be added at all. It is redundant and unneccessary. The proposal is too specific and will create adverse impact to many existing implementations without improving the security desired. Entities with high and medium impact BES Cyber Systems already have to provide justification for access at least every 15 months. Entities are required to provide evidence supporting that access is (1) necessary, and (2) for performing assigned work functions. These two criteria should be seen as the obligation to address the principles of need-to-know, least privilege, and separation of duties. Any further clarification should be made in implementation guidance.	
Likes 0	
Dislikes 0	
Response	
Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - FRCC,MRO,WECC,Texas RE,SERC,SPP RE, Group Name Southern Company	
Answer	No
Document Name	
Comment	
Southern disagrees with the need for this additional requirement under CIP-004-6 R4. First, existing CIP requirements under CIP-004-6 R4 already require the authorization of access based on need, and it is not necessary to repeat that tenant of cyber security in another requirement. When implementing ‘principles’ of least privilege and separation of duties, that can be exhibited in various ways to meet the needs of an Entity’s operations while maintaining adequate security. The currently proposed requirement leaves too broad a level of ambiguity to auditor interpretation regardless of an Entity’s efforts to comply. Additionally, as stated, “The SDT has identified “too much privilege” as an inherent risk in virtualization”, however the proposed requirement in not scoped to virtual environments and would be applicable across the board. All of CIP-004-6 R4 is currently scoped to High	

Impact BES Cyber Systems and Medium Impact BES Cyber Systems with ERC – and Southern requests explanation on why the ERC scoping for Mediums would be excluded in this context.

Likes 0	
Dislikes 0	

Response

sean erickson - Western Area Power Administration - 1,6

Answer	No
Document Name	

Comment

Comments: Singling virtualized environments out for special RBAC consider seems counter-productive. Certainly appropriate access should be justified and reviewed wherever it is granted.

Likes 0	
Dislikes 0	

Response

Shelby Wade - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company

Answer	No
Document Name	

Comment

The Applicable Systems of this requirement should be updated to say “high and medium impact BES Cyber Systems residing in a multi-instance environment and their associated CMS(s)”. Additionally, BES Cyber System Information should be changed to “designated storage locations for BES Cyber System Information” to align with CIP-004 Part 4.1, Part 4.4 and Part 5.3. Furthermore, the currently approved requirement CIP-004 Part 4.1 incorporates the concept of “need”. We feel that adding this new requirement is a duplication of the already existing requirement of need and provides a chance of double jeopardy for the entities and should be removed.

Likes 0	
Dislikes 0	

Response

David Francis - Midcontinent ISO, Inc. - 2,3 - MRO,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG

Answer	No
Document Name	

Comment	
The concept noted in this requirement should not be added at all. It is redundant and unneccessary. Entities with high and medium impact BES Cyber Systems already have to provide justification for access at least every 15 months. Entities are required to provide evidence supporting that access is (1) necessary, and (2) for performing assigned work functions. These two criteria should be seen as the obligation to address the principles of need-to-know, least privilege, and separation of duties. Any further clarification should be made in implementation guidance.	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	No
Document Name	
Comment	
As written, Part 4.5 goes beyond the scope of addressing virtualized environments.	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	No
Document Name	
Comment	
The SPP Standards Review Group has a concern that the proposed language presents redundancy issues. Additionally, we feel that the topic is already covered in the CIP-004 Standard section 4.1 and should not be added to the Virtualization process. Question: With this proposed language, who will be impacted by the applicability?	
Likes 0	
Dislikes 0	
Response	

Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
While Duke Energy agrees in principle, we cannot agree with the language proposed for Part 4.5. Currently, it isn't clear what duties would need to be separated under Part 4.5. We suggest adding language or providing additional rationale that would address specifically what is to be separated.	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	No
Document Name	
Comment	
While AZPS agrees with the intent to protect BES Cyber Assets and BCSI, it suggests that the proposed R4.5 is not as clear and unambiguous as it could be and, therefore, could result in confusion regarding applicability. To ensure that the scope of the requirement is clear, AZPS recommends that the language of R4.5 specifically reference virtual, multi-tenant environments. Additionally, while AZPS understands and acknowledges the value of the concepts of need-to-know, least privilege and separation of duties from a security perspective, AZPS cautions the drafting team regarding the cost/benefit ratio of including separation of duties in R4.5. In particular, AZPS is concerned that the inclusion of separation of duties would represent a significant cost impact to the Responsible Entity for very little attendant benefit to reliability.	
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	
Some organizations may lack staff to separate duties to multiple people. Additionally, the requirement does not establish a measureable span of control. The current CIP-004 requirements sufficiently address the need to implement an effective access control policy to limit privileges using these principles.	
Likes 0	

Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	
N&ST believes that “need-to-know” and “least privilege” are already addressed by CIP-004 R4. N&ST also believes that while separation of duties is an important security practice, it may be impractical or prohibitively costly for small entities with small IT or OT staffs.	
Likes 0	
Dislikes 0	
Response	
Don Schmit - Nebraska Public Power District - 1,3,5	
Answer	No
Document Name	
Comment	
Refer to question #23 comments.	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
CenterPoint Energy believes the proposed requirement is more of a best practice and should not be a requirement. Existing CIP-004 requirements already require authorization of access based on need. Similar to the language in proposed CIP-005 Requirement 1, Part 1.6, this requirement asserts an objective to the requirement, where evidence of objectives (or principles) is difficult to provide compared with evidence of activities. The proposed CIP-004 Requirement 4, Part 4.5 will be challenging to implement for smaller entities with limited staff, where the level of separation “in principle” cannot be achieved to satisfy the requirement.	

Likes 0

Dislikes 0

Response

Brandon McCormick - Florida Municipal Power Agency - 3,4,5,6 - FRCC, Group Name FMPA

Answer	No
Document Name	2016-02_Virtualization_Unofficial Comment Form_FMPA_comments.docx

Comment

Please see attached comments

Likes 0

Dislikes 0

Response

Bob Case - Black Hills Corporation - 1 - WECC

Answer	No
Document Name	

Comment

Part 4.5 does not address virtualization or segmentation of duties for virtualization management. However, in a shared environment, processes would need to be created or authorizations changed and documentation would need to spell out duties and access. There should be more guidance and direction on what is appropriate separation of duties.

Likes 0

Dislikes 0

Response

Janis Weddle - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Chelan PUD

Answer	No
Document Name	

Comment

Groups that manage CIP systems are often small and cannot easily address separation of duties or least privilege without undermining reliability. This would be a documentation exercise that would provide no additional security.

Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	No
Document Name	
Comment	
Please clarify if this proposed Part 4.5 is going to replace the current Part 4.1 since they are overlapped.	
Likes 0	
Dislikes 0	
Response	
John Tolo - Unisource - Tucson Electric Power Co. - 1	
Answer	Yes
Document Name	
Comment	
We agree with this as written explicitly because it allows us to make a determination of what “need-to-know” and “least privilege” means to us. If there will be additional guidance or directives then that guidance or directive might change our viewpoint. We support the concept as a basic security tenant.	
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	
Chantal Mazza - Hydro-Qu?bec TransEnergie - 2 - NPCC	
Answer	Yes
Document Name	
Comment	
We recommend the applicability section should be similar to CIP-005 R1.8 This Requirement seems to expand the scope of Requirements 4.1 – 4.4. Request clarification of “separation of duties.”	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
The terms “need-to-know,” “least privilege,” and “separation of duties” need to be defined in the Glossary or carefully explained in Implementation Guidance.	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
N/A	
Likes 0	

Dislikes 0	
Response	
Joel Charlebois - AESI - Acumen Engineered Solutions International Inc. - 5	
Answer	Yes
Document Name	
Comment	
We agree with this statement and it is good that it is not restricted to virtualized environments. This problem exists in many traditional environment as well, and it is addressed appropriately by the new requirement.	
Likes 0	
Dislikes 0	
Response	
Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4, Group Name FirstEnergy Corporation	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Robert Ganley - Long Island Power Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3,5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Richard Kinas - Orlando Utilities Commission - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
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	
Scott Downey - Peak Reliability - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	
Document Name	
Comment	
No comment at this time.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE does not have comments on this question.	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	

The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	

13. Do you agree with the SDT’s assertion that the definition of EACMS is too broad and does not differentiate the capabilities and risk(s) of the systems that fall within that definition scope? If not, please provide rationale to support your position.

Teresa Cantwell - Lower Colorado River Authority - 1,5	
Answer	No
Document Name	
Comment	
Existing definition is adequate.	
Likes 0	
Dislikes 0	
Response	
Richard Kinas - Orlando Utilities Commission - 3,5	
Answer	No
Document Name	
Comment	
We potentially agree given that it might require protection for some systems that do not require the higher level of protection. Electronic Access Control (real time) has more risk than Electronic Access Monitoring (after the fact)	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	No
Document Name	
Comment	
Actually the current EACMS definition implies that a Cyber Asset that has directly electronic access to the BCS is supposed to be identified as EACMS since it controls access to the BCS. We have proposed a modified EACMS definition in question 4 to include SDT proposed CMS.	
Likes 0	
Dislikes 0	

Response

Robert Ganley - Long Island Power Authority - 1

Answer	No
Document Name	

Comment

All EACMS's and CMS's, and ESZ's, etc. should be afforded equal protections to the highest watermark level within the associated environment. The compromise of one or more BCS's/BCS's (and/or associated systems) i.e. compromise of information, or ESP, or CMS can have an adverse effect on the BES regardless of the number or type of asset compromised.   The risks may seem different however; the BES would be impacted in some way.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

CenterPoint Energy believes the existing EACMS definition should be clarified for EACMS used for access monitoring. CenterPoint Energy proposes the following clarification:

"Cyber Assets that perform electronic access control **or are used for** electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems."

Some misinterpretation of EACMS is based on capability, rather than use, of tools where no access monitoring is intended. A system that is actually used and intended to capture all access activity should also be protected as other systems in scope for EACMS due to the risk posed by compromise of those systems. A tool used for monitoring configuration with no system management capability, antivirus, or security functions other than access control with some limited capability to pick up information related to access control should not be considered access control systems.

Likes 0	
Dislikes 0	

Response

Don Schmit - Nebraska Public Power District - 1,3,5

Answer	No
Document Name	

Comment

We do not believe that the EACMS definition is too broad.	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	
N&ST believes that both the current definition of EACMS and the requirements applicable to such devices are adequate and appropriate within the context of requirements applicable to high and medium impact BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	No
Document Name	
Comment	
The SPP Standard Review Group feels that the current definition gives the industry flexibility in this process. From our perspective, the proposed division of the definition will only cause confusion and put a huge burden on the industry to revise internal documentation as well as reclassifying their assets.	
Likes 0	
Dislikes 0	
Response	
David Francis - Midcontinent ISO, Inc. - 2,3 - MRO,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG	
Answer	No
Document Name	
Comment	

The EACMS definition is broad. However, the use of a single category allows entities to define a single set of controls for all systems in the category. This simplifies security and compliance obligations.	
Likes 0	
Dislikes 0	
Response	
Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	No
Document Name	
Comment	
All EACMS’s and CMS’s, and ESZ’s, etc. should be afforded equal protections to the highest watermark level within the associated environment. The compromise of one or more BCS’s/BCS’s (and/or associated systems) i.e. compromise of information, or ESP, or CMS can have an adverse effect on the BES regardless of the number or type of asset compromised. The risks may seem different however; the BES would be impacted in some way.	
Likes 0	
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
ERCOT agrees that the EACMS definition is broad. However, the use of a single category allows entities to define a single set of controls for all systems in the category. This simplifies security and compliance obligations.	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	

Reclamation supports the current definition of EACMS; applicable requirements that address risk(s) are determined by the Impact Rating Criteria.	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 3,5	
Answer	No
Document Name	
Comment	
AEP believes that fewer higher level definitions provide needed flexibility to responsible entities, employing a security mindset, in establishing required security for their BES Cyber Systems. We also agree that devices currently classified as EACMS, but with no ability to control access should be classifiable as BCSI repositories. We also agree with the introduction of the CMS definition. However, the other definitions are not necessary at this time.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE	
Answer	No
Document Name	
Comment	
The current EACMS elements are sufficient in providing implementation structure and flexibility to ensure security and address the differences found in entities' system designs without highly prescriptive Requirements. **Alternative.** Should the SDT seek to restrict the EACMS definition, we encourage any revisions maintain flexibility in consideration of different system designs to allow entities to address those differences in implementation and compliance activities.	
Likes 0	
Dislikes 0	
Response	
John Tolo - Unisource - Tucson Electric Power Co. - 1	
Answer	No

Document Name	
Comment	
This adds significant complexity to the discussion. We prefer to assign a higher and more consistent security strategy based on a single categorization rather than juggle requirements which are likely to be highly similar or even implemented to the higher level out of a desire to be more secure.	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3,5	
Answer	Yes
Document Name	
Comment	
Cowlitz supports BPA 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	

TVA supports the SDT's efforts to differentiate the categorizations of EACMS components based on the ability of such systems to affect access control and/or real time BES Cyber System functionality.	
Likes 0	
Dislikes 0	
Response	
Chantal Mazza - Hydro-Qu?bec TransEnergie - 2 - NPCC	
Answer	Yes
Document Name	
Comment	
We agree that the NERC standards need to allow for the level and type of monitoring described here. It seems that EACMS would need to be replaced by the combination of EAG, EACS and the BCSI changes and not left in place.	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
EACMS includes too many different functions to have prescriptive requirements applied broadly. Additionally, the requirements currently discourage entities from using vendor-based security monitoring services that could provide significant security benefit. At a minimum, monitoring systems (logging and event monitoring) that have no technical capacity or permission to configure BCSs should have risk assessed differently. There may also be value in separating security objectives between access control (authorization and permissions) and gateway functions (filter/forward traffic).	
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 ISO-NE NYISO NextERA Con-Ed and HQ	
Answer	Yes
Document Name	

Comment	
We agree that the NERC standards need to allow for the level and type of monitoring described here. It seems that EACMS would need to be replaced by the combination of EAG, EACS and the BCSI changes and not left in place.	
Likes 0	
Dislikes 0	
Response	
Ronald Donahey - TECO - Tampa Electric Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
We potentially agree given that it might require protection for some systems that do not require the higher level of protection. Electronic Access Control (real time) has more risk than Electronic Access Monitoring (after the fact) TEC recommends that the SDT consider guidance to explain what does pose a security threat. We suggest consideration that "Information to plan or execute an attack….." is appropriate, but that pose a security threat is too general." Starting point for definition: Information that is not on an asset that is afforded NERC protections. Where is the question on BCSI definition? We believe that the SDT should be asking for industry input on the proposed changes to BCSI as well as the proposed terms.	
Likes 0	
Dislikes 0	
Response	
Paul Haase - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light	
Answer	Yes
Document Name	
Comment	
City Light supports BPA's comments. City Light however remains concerned about the breadth and scope of the changes, and urges careful consideration by the SDT, by registered entities, and by NERC and the Regions that the impact of the proposed changes is well understood and mapped prior to adoption.	
Likes 0	
Dislikes 0	
Response	

Scott Downey - Peak Reliability - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joel Charlebois - AESI - Acumen Engineered Solutions International Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Janis Weddle - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Chelan PUD	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bob Case - Black Hills Corporation - 1 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brandon McCormick - Florida Municipal Power Agency - 3,4,5,6 - FRCC, Group Name FMPA	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jack Cashin - American Public Power Association - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4, Group Name FirstEnergy Corporation	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shelby Wade - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

sean erickson - Western Area Power Administration - 1,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - FRCC,MRO,WECC,Texas RE,SERC,SPP RE, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lauren Price - ATCO Electric - 1 - MRO,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8,9 - WECC	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE does not agree that the definition is too broad and suggests the current definition affords the necessary flexibility for registered entities to implement its cyber security program.	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	
Document Name	
Comment	
No comment at this time.	
Likes 0	

Dislikes 0	
Response	

14. Do you agree that the language of the proposed definitions of EACS provides better consistency and clarity to the CIP Standards? If not, please provide rationale to support your position and alternative language.

Ronald Donahey - TECO - Tampa Electric Co. - 1,3,5,6

Answer	No
Document Name	

Comment

The proposed definition provides more clarity but has its own set of issues: Hall of mirrors—“this includes Intermediate Systems” should be removed. The definition needs to be clear enough to indicate that an intermediate system needs to be covered.

That being said, the current definition of an Intermediate System states that it can’t be inside the ESP. The new EACS does not apply 5.1 correctly. We suggest adding a “one pass rule” so that entities don’t have to go through the requirements multiple times.

In addition, we believe that requirements should not put additional controls on top of a security control. If there is a need to do that, the additional controls need to be based on risk.

We also encourage the SDT to consider using an approach similar to that used for CIP-014 (NIST allows that as well…develop security controls): Requirement 1: Here are the minimum requirements. Requirement 2: address security risks that are not addressed that are not covered above.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE

Answer	No
Document Name	

Comment

We can see some value from the proposed EACS definition but struggle in identifying how it supports security and reliability issues that are already addressed in the current Standards. The concern is adding EACS as another NERC Glossary Term will create unnecessary compliance and implementation complexity. When taken in total with all the proposed new and revised Glossary Terms and Requirements presented in this commenting form, the cumulative and gross effect is increased complexity with, likely, marginal improvement in security or reliability.

Likes 0	
Dislikes 0	

Response

Aaron Austin - AEP - 3,5

Answer	No

Document Name	
Comment	
While the definition of EACS further refines an approved, AEP requests the SDT refer to our response to Question #13.	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	
Reclamation does not support a new definition of EACS. Reclamation recommends the SDT use existing industry-recognized terms to address the components of EACMS that control and authenticate electronic access, such as firewall, proxy server, router, etc. If the SDT decides to use the proposed definition of EACS, Reclamation recommends the proposed EACS definition be changed **from:** Cyber Assets that perform electronic access control of the BES Cyber Systems. This includes Intermediate Systems. **to:** Cyber Assets that control electronic access to BES Cyber Systems. Reclamation also recommends the SDT change the definition of BES Cyber System as described in the recommended definitions section of the response to Question 24.	
Likes 0	
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
ERCOT considers the EACS definition to be a good concept. However, the concept should be incorporated into a single comprehensive definition along with CMS and EAG.	
Likes 0	
Dislikes 0	

Response

Shelby Wade - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company

Answer	No
Document Name	

Comment

While we agree with the concept of separating out monitoring and control we do see some possible confusion with the EACS and EAG definitions. We believe that there may be instances where a system or asset performs both functions. How would you classify and protect this device? Additionally, it appears from the chart above, “Proposed Requirements Related to EACMS Changes”, that all updated requirements for EACS and EAGs are applicable to the same requirements. For simplicity purposes, we suggest that EACS and EAG be combined into one definition: “Cyber Assets that perform electronic access control of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems”.

Likes 0	
Dislikes 0	

Response

David Francis - Midcontinent ISO, Inc. - 2,3 - MRO,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG

Answer	No
Document Name	

Comment

This is a good concept and should be incorporated into a single comprehensive definition along with CMS and EAG

Likes 0	
Dislikes 0	

Response

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group

Answer	No
Document Name	

Comment

The SPP Standard Review Group feels that the current definition gives the industry flexibility in this process. From our perspective, the proposed division of the definition will only cause confusion and put a huge burden on the industry to revise internal documentation as well as reclassifying their assets.

Likes 0	
Dislikes 0	

Response

Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy

Answer	No
Document Name	

Comment

The proposed definition of EACS appears vague, and would benefit from additional language in the text of the definition. We recommend inserting some of the language used in the paragraph below the proposed definition, to be inserted in the text.

See example below:

- *Electronic Access Control System (EACS):*

Cyber Assets that perform electronic access control, and authentication and authorization of traffic or users of the BES Cyber Systems. This includes Intermediate Systems.

Likes 0	
Dislikes 0	

Response

Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6

Answer	No
Document Name	

Comment

While AZPS agrees with the proposal to differentiate control and monitoring, AZPS is concerned that monitoring includes more than data collection and storage. For example, alerting occurs utilizing inputs from monitoring and may occur concurrently in the same system. Accordingly, the alerting and monitoring systems may not be completely independent. For this reason, AZPS recommends that the SDT give some additional consideration to the proposal to ensure that all aspects of monitoring and dependent processes are fully evaluated and addressed.

Likes 0	
Dislikes 0	

Response

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

Answer	No

Document Name	
Comment	
TVA agrees that the language provides more clarity, but the term “pose a security threat” needs additional explanation. Does this term mean any security threat, or does the requirement allow the registered entity to determine a risk tolerance for the data? With all of the information that is excluded, what data remains to be considered BES Cyber System Information? The only remaining data for consideration would be user names, passwords, and security vulnerability information.	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	
N&ST believes the proposed definition of “EACS” is an unnecessary derivative of “EACMS” that provides no benefit. Furthermore, the proposed definition fails to address access control of Electronic Security Perimeters.	
Likes 0	
Dislikes 0	
Response	
Don Schmit - Nebraska Public Power District - 1,3,5	
Answer	No
Document Name	
Comment	
We do not believe a change is necessary.	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No

Document Name	
Comment	
CenterPoint Energy does not agree with the proposed definitions EACS or EAG. The existing definition of EACMS is sufficient with the added language suggested in #13. The intent, to distinguish authentication activity with packet inspection and filtering activity, is not stated in the proposed definitions. The separation into EACS and EAG might be better achieved by defining "access control" as either user/credential authentication or filtering performed at an EAP.	
Likes 0	
Dislikes 0	
Response	
Brandon McCormick - Florida Municipal Power Agency - 3,4,5,6 - FRCC, Group Name FMPA	
Answer	No
Document Name	2016-02_Virtualization_Unofficial Comment Form_FMPA_comments.docx
Comment	
Please see attached comments	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	No
Document Name	
Comment	
We disagree to break the EACMS into three terms. This change would cause more changes and more additional work for reclassification with little compliance work reduction.	
Likes 0	
Dislikes 0	
Response	
Richard Kinas - Orlando Utilities Commission - 3,5	
Answer	No

Document Name	
Comment	
The proposed definition provides more clarity but has its own set of issues: Hall of mirrors—“this includes Intermediate Systems” should be removed. The definition needs to be clear enough to indicate that an intermediate system needs to be covered. That being said, the current definition of an Intermediate System states that it can’t be inside the ESP. The new EACS does not apply 5.1 correctly. We suggest adding a “one pass rule” so that entities don’t have to go through the requirements in multiple pases as they are currently doing. In addition, we believe that requirements should not put additional controls on top of a security control. If there is a need to do that, the additional controls need to be based on risk. We also encourage the SDT to consider using an approach similar to that used for CIP-014 (NIST allows that as well…develop security controls): Requirement 1: Here are the minimum requirements. Requirement 2: address security risks that are not addressed that are not covered above.	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5	
Answer	No
Document Name	
Comment	
Keep current EACMS definition.	
Likes 0	
Dislikes 0	
Response	
Paul Haase - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light	
Answer	Yes
Document Name	
Comment	
City Light supports BPA's position and comments.	
Likes 0	
Dislikes 0	

Response	
John Tolo - Unisource - Tucson Electric Power Co. - 1	
Answer	Yes
Document Name	
Comment	
The definitions themselves seem reasonable and understandable.	
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 ISO-NE NYISO NextERA Con-Ed and HQ	
Answer	Yes
Document Name	
Comment	
Yes, as long as the concept of monitoring is also changed to solely be the classification of the monitoring data as BCSI, when applicable. We do not think the all monitoring data would meet the BCSI definition. Ie. video recording of a single door.	
Likes 0	
Dislikes 0	
Response	
Lauren Price - ATCO Electric - 1 - MRO,RF	
Answer	Yes
Document Name	
Comment	
While ATC agrees with the proposed definition of EACS, there is some concern that if there is a requirement to put an EACS inside the ESP, it could result in complex configurations making security more difficult.	
Likes 0	
Dislikes 0	
Response	

John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
Tacoma Power supports comments submitted by APPA.	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	Yes
Document Name	
Comment	
Yes, the proposed language provides more clarity, but public power would note that the change includes intermediate systems.	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
BPA also recommends clarifying that AAA clients that subscribe to EACS/AAA services (e.g., via a protocol such as LDAP, RADIUS or TACACS+) but do not maintain any account information are not EACS themselves.	
Likes 0	
Dislikes 0	
Response	
Chantal Mazza - Hydro-Qu?bec TransEnergie - 2 - NPCC	

Answer	Yes
Document Name	
Comment	
Yes, as long as the concept of monitoring is also changed to solely be the classification of the monitoring data as BCSI, when applicable. We do not think the all monitoring data would meet the BCSI definition.	
Likes 0	
Dislikes 0	
Response	
Robert Ganley - Long Island Power Authority - 1	
Answer	Yes
Document Name	
Comment	
Should be added as part of the EACMS definition.	
Likes 0	
Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3,5	
Answer	Yes
Document Name	
Comment	
Cowlitz supports BPA comment.	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	

Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8,9 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - FRCC,MRO,WECC,Texas RE,SERC,SPP RE, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4, Group Name FirstEnergy Corporation	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bob Case - Black Hills Corporation - 1 - WECC	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Janis Weddle - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Chelan PUD	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Joel Charlebois - AESI - Acumen Engineered Solutions International Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Downey - Peak Reliability - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	
Document Name	
Comment	
No comment at this time.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	

Comment	
Texas RE does not have comments on this question.	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	

15. Do you agree that the language of the proposed definitions of EAG provides better consistency and clarity to the CIP Standards? If not, please provide rationale to support your position and alternative language.

Teresa Cantwell - Lower Colorado River Authority - 1,5

Answer	No
Document Name	

Comment

Keep current EACMS definition.

Likes 0	
Dislikes 0	

Response

Richard Kinas - Orlando Utilities Commission - 3,5

Answer	No
Document Name	

Comment

Comments: We think that the SDT is attempting to differentiate hardware from virtual environment. The EAG hosts the EAP makes it seem that it is virtual. Some entities share a concern that the EACS and EAG are the same; is the EACS addressing lateral movement? Part 1.5 is applicable to EAPs for high & medium at control centers. With the new definition, will that no longer be applicable for EAPS?

Is the BES Cyber Asset an EACS? Is it physical or virtual? Is the implication there that it is both? (for example: Domain controllers/TACACS) This creates an implementation challenge for entities given the dual nature of some devices.

An Electronic Access Gateway hosts the EAP and performs the active function of filtering or forwarding traffic at the demarcation point (boundary protection). Primarily, these are firewalls and routers that perform gateway functions at the layer 3 ESP boundary demarcation point. Separation of duties issues here?

The EAG hosts the EAP…makes it sound as if it is virtual. Internal discussions raised the question of whether the Electronic Access Gateway term is required.

Cisco FW is more virtual; Checkpoint the language makes sense; Checkpoint offers IPS to run in parallel; or in line IPS appliance

Likes 0	
Dislikes 0	

Response

Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	No
Document Name	
Comment	
We disagree with this. See the same comments as in question 14.	
Likes 0	
Dislikes 0	
Response	
Bob Case - Black Hills Corporation - 1 - WECC	
Answer	No
Document Name	
Comment	
This appears to be an unnecessary segmentation of an EAP, unless there is clarification provided that this is referring to a virtual firewall and the EAG is the physical host and the EAP is the virtual firewall running on the host.	
Likes 0	
Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3,5	
Answer	No
Document Name	
Comment	
Cowlitz supports BPA comment.	
Likes 0	
Dislikes 0	
Response	
Brandon McCormick - Florida Municipal Power Agency - 3,4,5,6 - FRCC, Group Name FMPA	
Answer	No

Document Name	2016-02_Virtualization_Unofficial Comment Form_FMPA_comments.docx
Comment	
Please see attached comments	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
CenterPoint Energy does not agree with the proposed definitions EACS or EAG. The existing definition of EACMS is sufficient with CenterPoint Energy's added language in the response to Question No. 13. The proposed EAG definition creates a risk that requirements restricted in scope with the granular description of an EAP as a specific interface will be reinterpreted to apply an entire gateway or group of gateways. The EAG concept also encourages entities to employ dedicated CIP gateways to avoid confusion, which runs counter to the move to multi-instance environments.	
Likes 0	
Dislikes 0	
Response	
Don Schmit - Nebraska Public Power District - 1,3,5	
Answer	No
Document Name	
Comment	
We do not believe a change is necessary.	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No

Document Name	
Comment	
N&ST believes the current definition of EACMS adequately applies to devices that have one or more interfaces that act as Electronic Access Points.	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No
Document Name	
Comment	
TVA suggests the overlap between the term Electronic Access Point and EAG is unclear. Please consider consolidating the terms.	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
BPA believes the EAG definition is too similar to the EACS definition to be useful. The EAG definition should explicitly reference the filter/forward function rather than state “perform electronic access control.” Proposed: EAG - Cyber Assets that perform filtering or forwarding of traffic at the Electronic Security Perimeter(s) OR between ESZs. The EAG also hosts the EAP(s) if any.	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	

Answer	No
Document Name	

Comment

The use of the term “hosts” in the proposed language is vague. We suggest the following alternative language:

- *Electronic Access Gateway:*

  Cyber Assets that perform electronic access control of the Electronic Security Perimeter(s). The Electronic Access Gateway exists on the EAP(s).

We believe the phrase “exists on” rather than using the word “hosts” is more appropriate in this context.

Likes 0	
Dislikes 0	

Response

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group

Answer	No
Document Name	

Comment

The SPP Standard Review Group feels that the current definition gives the industry flexibility in this process. From our perspective, the proposed division of the definition will only cause confusion and put a huge burden on the industry to revise internal documentation as well as reclassifying their assets.

Likes 0	
Dislikes 0	

Response

David Francis - Midcontinent ISO, Inc. - 2,3 - MRO,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG

Answer	No
Document Name	

Comment

There is no need to have a separate definition for EACS and EAG if they are both providing access control functions. The differentiation of controls is not of a magnitude to really provide benefit.

Likes 0	
Dislikes 0	

Response	
Shelby Wade - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company	
Answer	No
Document Name	
Comment	
While we agree with the concept of separating out monitoring and control we do see some possible confusion with the EACS and EAG definitions. We believe that there may be instances where a system or asset performs both functions. How would you classify and protect this device? Additionally, it appears from the chart above, “Proposed Requirements Related to EACMS Changes”, that all updated requirements for EACS and EAGs are applicable to the same requirements. For simplicity purposes, we suggest that EACS and EAG be combined into one definition: “Cyber Assets that perform electronic access control of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems”.	
Likes 0	
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
ERCOT does not see a need to have a separate definition for EACS and EAG if they are both providing access control functions. The differentiation of controls is not of a magnitude to really provide benefit in separating the definitions. The concept should be incorporated into a single comprehensive definition along with CMS and EACS.	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	

Reclamation does not support the proposed definition of EAG. EAPs may exist without an EAG. Reclamation recommends the SDT use existing industry-recognized terms to address the components of EACMS that control and authenticate electronic access, such as firewall, proxy server, router, etc.

If the SDT decides to use the proposed definition of EAG, Reclamation recommends the proposed EAG definition be changed

from: Cyber Assets that perform electronic access control of the Electronic Security Perimeter(s). The Electronic Access Gateway also hosts the EAP(s)

to: Cyber Assets (including Electronic Access Points) that control electronic access to and from virtual and non-virtual Electronic Security Perimeter(s).

Reclamation also recommends the SDT change the definition of BES Cyber System as described in the recommended definitions section of the response to Question 24.

Likes 0	
Dislikes 0	

Response

Aaron Austin - AEP - 3,5

Answer	No
Document Name	

Comment

While the definition of EAG further refines an approved, AEP requests the SDT refer to our response to Question #13.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE

Answer	No
Document Name	

Comment

We can see some value from the proposed EAG definition but struggle in identifying how it supports security and reliability issues that are already addressed in the current Standards. The concern is adding EAG as another NERC Glossary Term will create unnecessary compliance and implementation complexity. When taken in total with all the proposed new and revised Glossary Terms and Requirements presented in this commenting form, the cumulative and gross effect is increased complexity with, likely, marginal improvement in security or reliability.

Alternative. If the SDT concludes the proposed definition is required to address the identified issues, an alternative approach is to remove electronic access control from the definition and include language that addresses the function of the EAG:

Electronic Access Gateway: Cyber Assets that perform electronic access control of the Electronic Security Perimeter(s) the active function of filtering or forwarding traffic at the demarcation point (boundary protection). The Electronic Access Gateway also hosts the EAP(s).

Likes 0	
Dislikes 0	

Response

Ronald Donahey - TECO - Tampa Electric Co. - 1,3,5,6

Answer	No
Document Name	

Comment

We think that the SDT is attempting to differentiate hardware from virtual environment.   The EAG hosts the EAP makes it seem that it is virtual. Some entities share a concern that the EACS and EAG are the same; is the EACS addressing lateral movement? Part 1.5 is applicable to EAPs for high & medium at control centers. With the new definition, will that no longer be applicable for EAPS?

Is the BES Cyber Asset an EACS? Is it physical or virtual? Is the implication there that it is both? (for example: Domain controllers/TACACS) This creates an implementation challenge for entities given the dual nature of some devices.

An Electronic Access Gateway hosts the EAP and performs the active function of filtering or forwarding traffic at the demarcation point (boundary protection). Primarily, these are firewalls and routers that perform gateway functions at the layer 3 ESP boundary demarcation point. Separation of duties issues here?

The EAG hosts the EAP…makes it sound as if it is virtual. Internal discussions raised the question of whether the Electronic Access Gateway term is required.

Likes 0	
Dislikes 0	

Response

Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric

Answer	Yes
Document Name	

Comment

N/A

Likes 0	
Dislikes 0	

Response	
Robert Ganley - Long Island Power Authority - 1	
Answer	Yes
Document Name	
Comment	
Should be added as part of the EACMS definition.	
Likes 0	
Dislikes 0	
Response	
Chantal Mazza - Hydro-Qu?bec TransEnergie - 2 - NPCC	
Answer	Yes
Document Name	
Comment	
Yes, as long as the concept of monitoring is also changed to solely be the classification of the monitoring data as BCSI, when applicable.	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	Yes
Document Name	
Comment	
The SDT used EAG Systems in the example for the changes to the BCSI definition. Public power is unsure if this should be EAG or EAGS.	
Likes 0	
Dislikes 0	
Response	

John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
Tacoma Power supports comments submitted by APPA.	
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 ISO-NE NYISO NextERA Con-Ed and HQ	
Answer	Yes
Document Name	
Comment	
As stated in other comments, the SDT used EAG Systems in the example for the changes to the BCSI definition. I am unsure if this should be EAG or EAGS.	
Likes 0	
Dislikes 0	
Response	
Scott Downey - Peak Reliability - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joel Charlebois - AESI - Acumen Engineered Solutions International Inc. - 5	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Janis Weddle - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Chelan PUD	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4, Group Name FirstEnergy Corporation	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - FRCC,MRO,WECC,Texas RE,SERC,SPP RE, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lauren Price - ATCO Electric - 1 - MRO,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8,9 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Tolo - Unisource - Tucson Electric Power Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	

Document Name	
Comment	
Texas RE does not have comments on this question.	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	
Document Name	
Comment	
No comment at this time.	
Likes 0	
Dislikes 0	
Response	

16. Do you agree that the current compliance requirements related to EACMS monitoring systems are precluding or discouraging solutions that could reduce risk to security and reliability? Please provide your rationale in support or against this assertion.

John Tolo - Unisource - Tucson Electric Power Co. - 1	
Answer	No
Document Name	
Comment	
We feel all the requirements are reasonable as-is and would rather see consistency, even if the standard is increased.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE	
Answer	No
Document Name	
Comment	
The current EACMS parameters are sufficient in providing implementation structure and flexibility to ensure security and address the differences found in entities' system designs without highly prescriptive Requirements.	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 3,5	
Answer	No
Document Name	
Comment	
AEP agrees that the current requirements related to EACMS systems may preclude the optimal security and reliability solutions. AEP requests the SDT refer to our response to Question #13.	
Likes 0	
Dislikes 0	

Response	
Lauren Price - ATCO Electric - 1 - MRO,RF	
Answer	No
Document Name	
Comment	
ATC already treats our enterprise level monitoring systems as EACMS devices.	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	
Reclamation supports the current compliance requirements related to EACMS. The Impact Rating Criteria provides the necessary clarity to reduce security and reliability risks. Reclamation recommends simplifying the Impact Rating Criteria in CIP-002 and changing the definition of BES Cyber System, as described in the recommended definitions section of the response to Question 24.	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	No
Document Name	
Comment	
no strong opinion	
Likes 0	
Dislikes 0	

Response	
Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	No
Document Name	
Comment	
The current compliance requirements related to EACMS monitoring systems do not differentiate, preclude or discourage solutions that could reduce risk to security and reliability.	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	No
Document Name	
Comment	
The SPP Standard Review Group feels that the current compliance requirements give the industry flexibility in this process. From our perspective, the proposed division of the definition will only cause confusion and put a huge burden on the industry to revise internal documentation as well as reclassifying their assets.	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	
N&ST has not encountered situations with its Bulk Electric System clients wherein an entity has avoided using security event monitoring and analysis systems due to concerns related to EACMS requirements.	
Likes 0	
Dislikes 0	

Response	
Don Schmit - Nebraska Public Power District - 1,3,5	
Answer	No
Document Name	
Comment	
We do not believe a change is necessary.	
Likes 0	
Dislikes 0	
Response	
Robert Ganley - Long Island Power Authority - 1	
Answer	No
Document Name	
Comment	
The current compliance requirements related to EACMS monitoring systems do not differentiate, preclude or discourage solutions that could reduce risk to security and reliability.	
Likes 0	
Dislikes 0	
Response	
Janis Weddle - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Chelan PUD	
Answer	No
Document Name	
Comment	
We have not encountered difficulty implementing enterprise grade security solutions with the current requirements.	
Likes 0	
Dislikes 0	
Response	

Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	No
Document Name	
Comment	
We disagree with this. See the same comments as in question 14.	
Likes 0	
Dislikes 0	
Response	
Richard Kinas - Orlando Utilities Commission - 3,5	
Answer	No
Document Name	
Comment	
We believe that current compliance requirements may be hindering the use of cloud sourcing the SIEM function. We recommend consideration of removing the controls devices away from the BES Cyber Systems….can that be broken out of the applicability section? We also recommend separate controls for the electronic monitoring systems	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5	
Answer	No
Document Name	
Comment	
Separating monitoring controls from EACMS definition reduces security posture.	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8,9 - WECC	

Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Paul Haase - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light	
Answer	Yes
Document Name	
Comment	
City Light supports BPA's position and comments.	
Likes 0	
Dislikes 0	
Response	
Ronald Donahey - TECO - Tampa Electric Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
We believe that current compliance requirements may hindering the use of cloud sourcing the SIEM. We recommend consideration of removing the controls devices away from the BES Cyber Systems….can that be broken out of the applicability section? We also recommend separate controls for the electronic monitoring 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 ISO-NE NYISO NextERA Con-Ed and HQ	
Answer	Yes
Document Name	

Comment	
Yes. The existing standards would make it difficult or maybe impossible to be compliant and use services like Dell Secureworks.	
Likes 0	
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
ERCOT agrees that the current compliance requirements related to EACMS monitoring systems are precluding or discouraging solutions that could reduce risk to security and reliability. The current requirements are written to an asset level that requires the entities to be the ones managing the devices. With vendors going to more hosted service based solutions, the asset focus of the CIP requirements for EACMS pose serious problems when picking security solutions that provide more event correlation and expertise.	
Likes 0	
Dislikes 0	
Response	
Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - FRCC,MRO,WECC,Texas RE,SERC,SPP RE, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern Company agrees that the compliance burden currently placed on systems only used for electronic access monitoring and alarm response as per CIP-007-6 R4 are a hindrance to reaping the full security benefit of integrated SIEM systems. Southern supports the SDTs direction in this regard and agrees that the proper scoping of such systems as BCSI repositories is accurate.	
Likes 0	
Dislikes 0	
Response	
Shelby Wade - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company	

Answer	Yes
Document Name	
Comment	
We do agree that current requirements on EACMS that perform access monitoring discourage entities from using enterprise wide solutions that could, if in use, provide better visibility into trends and emerging threats.	
Likes 0	
Dislikes 0	
Response	
David Francis - Midcontinent ISO, Inc. - 2,3 - MRO,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG	
Answer	Yes
Document Name	
Comment	
The current requirements are written to an asset level that requires the entities to be the ones managing the devices. With vendors going to more hosted service based solutions, the asset focus of the CIP requirements for EACMS pose serious problems when picking security solutions that provide more event correlation and expertise.	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	Yes
Document Name	
Comment	
The classification of monitoring systems as an EACMS currently limits the ability of utilizing enterprise solutions to provide this function. By eliminating this restriction a more enterprise wide approach can be evaluated to increase correlation and improve overall security monitoring.	
Likes 0	
Dislikes 0	
Response	
John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	

Answer	Yes
Document Name	
Comment	
Tacoma Power supports comments submitted by APPA.	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
AZPS currently separates CIP monitoring systems from corporate monitoring systems and therefore, data analytics are impacted. With the SDT's proposal that the information contained within EACMS be protected as a BCSI repository, this would allow Responsible Entities to have more flexibility to incorporate data from multiple monitoring sources to better evaluate risks to security and reliability.	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	Yes
Document Name	
Comment	
Yes. The existing standards would make it difficult or potentially impossible to be compliant and use services like Dell Secureworks.	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes

Document Name	
Comment	
Entities have made decisions based upon this compliance uncertainty in the past. Solutions that could reduce risk are hampered by this outdated model as noted by industry security advocates.	
Likes 0	
Dislikes 0	
Response	
Chantal Mazza - Hydro-Qu?bec TransEnergie - 2 - NPCC	
Answer	Yes
Document Name	
Comment	
Yes. The existing standards would make it difficult or maybe impossible to be compliant and use services like Dell Secureworks.	
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	
TVA suggests security monitoring should be implemented in a manner that avoids any adverse operational impact on security event discovery and prevents introduction of a path that attackers could compromise to introduce malware.	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	

Comment	
Tools that provide great benefit by monitoring system events, performance and health often collect access information also, sometimes by default. These systems, not used as EACMS, are considered as such for regulatory purposes and that discourages the use of all but the most necessary tools.	
Likes 0	
Dislikes 0	
Response	
Brandon McCormick - Florida Municipal Power Agency - 3,4,5,6 - FRCC, Group Name FMPA	
Answer	Yes
Document Name	2016-02_Virtualization_Unofficial Comment Form_FMPA_comments.docx
Comment	
Please see attached comments	
Likes 0	
Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3,5	
Answer	Yes
Document Name	
Comment	
Cowlitz supports BPA comment.	
Likes 0	
Dislikes 0	
Response	
Bob Case - Black Hills Corporation - 1 - WECC	
Answer	Yes
Document Name	
Comment	

Utilizing enterprise-wide monitoring and alerting systems may allow a better picture of a security threat.	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Joel Charlebois - AESI - Acumen Engineered Solutions International Inc. - 5	
Answer	Yes
Document Name	
Comment	
Entities are choosing to deploy a second monitoring solution (e.g., SIEM) for monitoring BCS only, in order to avoid expanding compliance obligations to enterprise systems. Due to the smaller scope of this second monitoring solution, the chosen application may be inferior to existing enterprise solutions to reduce costs. Additionally, the entity now loses the ability to correlate enterprise and BCS events, reducing the effectiveness of both monitoring solutions.	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Downey - Peak Reliability - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	
Document Name	
Comment	
No Comment at this time.	
Likes 0	
Dislikes 0	
Response	

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE does not have comments on this question.	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	

17. Should the security requirements for the access control portion of the EACMS to be different from the monitoring portion of the EACMS? If you do, please provide your rationale.

Teresa Cantwell - Lower Colorado River Authority - 1,5	
Answer	No
Document Name	
Comment	
These requirements should be the same.	
Likes 0	
Dislikes 0	
Response	

Richard Kinas - Orlando Utilities Commission - 3,5	
Answer	No
Document Name	
Comment	
We raise the question: would it be problematic if we don't apply different access control standards? We recommend consideration that the requirements be expanded as noted in comments above to address gaps in standards/risks.	
Likes 0	
Dislikes 0	
Response	

Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	No
Document Name	
Comment	
We disagree with this. See the same comments as in question 14.	
Likes 0	
Dislikes 0	
Response	

Robert Ganley - Long Island Power Authority - 1

Answer	No
Document Name	

Comment

All cyber assets in support of the BES should be afforded the highest level of protections as the highest watermark to reduce/mitigate any potential risks that can impact the systems directly or indirectly.

Likes 0	
Dislikes 0	

Response

Don Schmit - Nebraska Public Power District - 1,3,5

Answer	No
Document Name	

Comment

We believe that it is just as important to protect the monitoring systems as it is to protect the access control systems. Monitoring systems have extremely valuable information to attackers. They could even mask an attack if the monitoring system were compromised.

Likes 0	
Dislikes 0	

Response

Nicholas Lauriat - Network and Security Technologies - 1

Answer	No
Document Name	

Comment

N&ST believes that within the context of the existing CIP Standards, it is reasonable for the same set of security requirements to be applied to both access control and monitoring functions. Moreover, N&ST believes that trying to establish two different sets of requirements, one for each major function addressed by the existing definition of EACMS, could lead to confusion over how to identify and apply CIP-mandated controls to systems that perform both functions.

N&ST is strongly opposed to the idea of allowing systems that perform security event monitoring to be categorized as BSCI repositories rather than EACMS and disagrees with the assertion it would “result in improved security and reliability.” At the present time, systems acting as “designated storage locations” for BSCI and performing no other reliability function are not subject to any CIP requirements other than CIP-004 R4 and R5.

Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	No
Document Name	
Comment	
The SPP Standard Review Group feels that the current compliance requirements give the industry flexibility in this process. From our perspective, the proposed division of the definition will only cause confusion and put a huge burden on the industry to revise internal documentation as well as reclassifying their assets.	
Likes 0	
Dislikes 0	
Response	
Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	No
Document Name	
Comment	
All cyber assets in support of the BES should be afforded the highest level of protections as the highest watermark to reduce/mitigate any potential risks that can impact the systems directly or indirectly.	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	
Reclamation supports the current definition of EACMS. Existing requirements that equally address access control and monitoring are adequately defined. The Impact Rating Criteria appropriately determines the protection each system requires.	

Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 3,5	
Answer	No
Document Name	
Comment	
AEP believes the current definition of EACMS allows for independent Cyber Assets to perform the separate functions as well as a combined function and that there is little to no difference in the risks presented. If the access control portion and the access monitoring portion can be separated, then yes security requirements for the access monitoring portion should be less restrictive (e.g. classifying the access monitoring portion as a BCSI repository).	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE	
Answer	No
Document Name	
Comment	
The EACMS access control and monitoring portions each play crucial roles protecting the security and reliability of the BES. Creating a dichotomy between the EACMS access control and monitoring requirements does not necessarily improve either and only creates added operational and compliance complexity.	
Likes 0	
Dislikes 0	
Response	
Ronald Donahey - TECO - Tampa Electric Co. - 1,3,5,6	
Answer	No
Document Name	
Comment	

We raise the question: would it be problematic if we don’t apply different access control standards? We recommend consideration that the requirements be expanded as noted in comments for Question 16 to address gaps in standards/risks.	
Likes 0	
Dislikes 0	
Response	
Joel Charlebois - AESI - Acumen Engineered Solutions International Inc. - 5	
Answer	Yes
Document Name	
Comment	
The risks presented by the two types of systems are different. Compromise of the control portion gives the attacker immediate access to the systems being protected. Compromise of the monitoring portion may provide the attacker the ability to mask their actions and it may also provide them with information they can use to breach the control portion, but it does not grant them immediate access to the protected systems. The requirements should be different, but should take into account the risks posed by each system and address them appropriately.	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	

The ability to control access to essential systems carries a far greater risk than the ability to log events related to essential systems. Both should be protected, but the protections for access control systems should be held to the highest level feasible.	
Likes 0	
Dislikes 0	
Response	
Janis Weddle - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Chelan PUD	
Answer	Yes
Document Name	
Comment	
We agree with the SDT that the risk exposed by monitoring systems is lower than the risk exposed by access control systems.	
Likes 0	
Dislikes 0	
Response	
Bob Case - Black Hills Corporation - 1 - WECC	
Answer	Yes
Document Name	
Comment	
Monitoring systems should not have the same compliance regulations for BCS, so use of enterprise-wide systems can be utilized rather than discouraged.	
Likes 0	
Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3,5	
Answer	Yes
Document Name	
Comment	

Cowlitz supports BPA comment.	
Likes 0	
Dislikes 0	
Response	
Brandon McCormick - Florida Municipal Power Agency - 3,4,5,6 - FRCC, Group Name FMPA	
Answer	Yes
Document Name	2016-02_Virtualization_Unofficial Comment Form_FMPA_comments.docx
Comment	
Please see attached comments	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
CenterPoint Energy agrees with the differentiation between access control and monitoring and the relative risk is different for monitoring and active control.	
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	

TVA supports the SDT’s efforts to implement graduated levels of controls aligned with the functions executed by EACMS subsystems. Access control and access monitoring are separate security control functions, and consequently have different security requirements that should be considered separately. Access control systems inherently pose a greater risk if compromised than a monitoring system.	
Likes 0	
Dislikes 0	
Response	
Chantal Mazza - Hydro-Qu?bec TransEnergie - 2 - NPCC	
Answer	Yes
Document Name	
Comment	
The security controls for monitoring do not need to be a rigid since the BES cannot be negatively impacted solely by a compromise of a monitoring system.	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
BPA believes the option should be available based upon an entity’s assessment of different risks and controls specific to individual technology choices. Handling of log/monitoring information is different than control of access methodology.	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	Yes
Document Name	
Comment	

The security controls for monitoring need to be flexible. This is because the BES cannot be negatively impacted solely by a compromise of a monitoring system.

Likes 0	
Dislikes 0	

Response

Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6

Answer	Yes
Document Name	

Comment

As the SDT highlighted, there are different risks associated with both portions of the EACMS. The risk associated with the monitoring portion of the EACMS is information leakage, whereas the risk associated with the access control portion is unauthorized access to BES Cyber Systems and modifications of their operational parameters. Therefore, AZPS agrees that different security requirements should apply to different portion of the EACMS.

Likes 0	
Dislikes 0	

Response

John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6

Answer	Yes
Document Name	

Comment

Tacoma Power supports comments submitted by APPA.

Likes 0	
Dislikes 0	

Response

Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy

Answer	Yes
Document Name	

Comment

Yes, the current language drives entities to separate CIP and non-CIP monitoring environments, increasing costs and slowing adoption of better monitoring systems. Requiring CIP004-5 protections for EACMS allows for monitoring environment consolidation, deeper threat analysis, and quicker security event response times.	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	Yes
Document Name	
Comment	
Access control has a direct impact on who can access the system and what they can do in the system, whereas monitoring is constrained to visibility to what is happening in the system (less risk on the monitoring side as it is typically read only).	
Likes 0	
Dislikes 0	
Response	
David Francis - Midcontinent ISO, Inc. - 2,3 - MRO,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG	
Answer	Yes
Document Name	
Comment	
We agree with the SDT assertions that these are only collecting information about the BCS and not necessary to the operations of the BCS.	
Likes 0	
Dislikes 0	
Response	
Shelby Wade - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company	
Answer	Yes
Document Name	
Comment	

We agree that there are differing risks based on the functionality of EACMS. The risk associated with monitoring access is greatly reduced compared to the risk of controlling access. If a system that controls access to a BES Cyber System or Asset is compromised, the real-time ability to operate or control the BES could be reduced or severed altogether. Conversely, if a system the monitor's access to a BES Cyber System or Asset is compromised, the real-time ability to operate or control the BES is not compromised. Therefore, we agree that the requirements for the access control portion of the EACMS should be different from the monitoring portion.

Likes 0	
Dislikes 0	

Response

Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2

Answer	Yes
Document Name	

Comment

ERCOT agrees with the SDT assertions that the access monitoring systems are only collecting information about the BCS and not necessary to the operations of the BCS. This distinction does support consideration as a repository of BES Cyber System Information.

Likes 0	
Dislikes 0	

Response

Lauren Price - ATCO Electric - 1 - MRO,RF

Answer	Yes
Document Name	

Comment

We agree with the SDTs rationale for differentiation between access control functions and monitoring functions and therefore support the proposed adjustments to the controls associated to EACS vs EAMS.

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 ISO-NE NYISO NextERA Con-Ed and HQ

Answer	Yes
Document Name	

Comment	
The security controls for monitoring do not need to be a rigid since the BES cannot be negatively impacted solely by a compromise of a monitoring system.	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8,9 - WECC	
Answer	Yes
Document Name	
Comment	
The systems logically lend themselves to be separated.	
Likes 0	
Dislikes 0	
Response	
John Tolo - Unisource - Tucson Electric Power Co. - 1	
Answer	Yes
Document Name	
Comment	
We feel all the requirements are reasonable as-is and would rather see consistency, even if the standard is increased. That said, out of all the categories being proposed, the access control and monitoring are the most disparate in security needs.	
Likes 0	
Dislikes 0	
Response	
Paul Haase - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light	
Answer	Yes
Document Name	
Comment	

City Light supports BPA position and comments.	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4, Group Name FirstEnergy Corporation	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - FRCC,MRO,WECC,Texas RE,SERC,SPP RE, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE does not have comments on this question.	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	

Document Name	
Comment	
No comment at this time.	
Likes 0	
Dislikes 0	
Response	

18. Should CIP-011 Requirement R2 scope be expanded to include designated storage locations for access monitoring systems? If not, please provide rationale to support your position.

Paul Haase - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light	
Answer	No
Document Name	
Comment	
City Light believes the existing BCSI definition does not need to be modified. It is sufficiently broad as written to include access monitoring information. Guidance or outreach might be provided to make this point clear, but, again, the existing definition is adequate as is.	
Likes 0	
Dislikes 0	
Response	
John Tolo - Unisource - Tucson Electric Power Co. - 1	
Answer	No
Document Name	
Comment	
Storage needs to be specifically addressed as part of the ESZ conversation or—even more realistic—as part of its own standard set. How do we treat NFS volumes in a shared environment?	
Likes 0	
Dislikes 0	
Response	
Ronald Donahey - TECO - Tampa Electric Co. - 1,3,5,6	
Answer	No
Document Name	
Comment	
The CIP-011 discussion on the SIEM (re-use and disposal) may be a separate concern; a recent FRCC workshop comment made by RE auditors put forth the concept that all BCAs contain BCSI; by addressing CIP-011 R2 have to protect the SIEM even if it was not identified as an EACMS. The scope might need to be reduced.	
Likes 0	

Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE	
Answer	No
Document Name	
Comment	
We believe the full magnitude of the impact to a change in definition has not fully been identified to provide substantive comments on expanding CIP-011 R2 to include designated storage locations for access monitoring systems.	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 3,5	
Answer	No
Document Name	
Comment	
AEP believes the existing CIP-011 requirement R2 language is specific enough to allow responsible entities to assess the vulnerability of any storage location they have chosen for BCSI and understand the security controls that are needed in the event that the access-monitoring portion of an EACMS is classified as a BCSI repository.	
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 ISO-NE NYISO NextERA Con-Ed and HQ	
Answer	No
Document Name	
Comment	
Request clarification. Is this question asking about only hosted systems?	

Likes 0	
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
ERCOT does not agree with expanding CIP-011 R2 to include a all repositories of BCSI. The context of removing “monitoring” from the EACMS was to address information that may be with a third party. As such, the Responsible Entity cannot provide asset-level compliance evidence for a third part.	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	No
Document Name	
Comment	
Comments: Seems unnecessarily prescriptive	
Likes 0	
Dislikes 0	
Response	
Shelby Wade - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company	
Answer	No
Document Name	
Comment	
BES Cyber System Information, whether stored in a “designated storage location for access monitoring systems” or stored in a “designated storage location for BES Cyber System Information”, is at its core BES Cyber System Information. Adding levels of BES Cyber System Information risk based on storage location will cause confusion within the industry and provides no reliability benefit.	

Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4, Group Name FirstEnergy Corporation	
Answer	No
Document Name	
Comment	
Monitoring systems if they store information with context, would be covered under existing CIP Requirements. If monitoring systems do not store information with context, then there is no risk.	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	No
Document Name	
Comment	
The SPP Standard Review Group feels that the current definition gives the industry flexibility in this process. From our perspective, the proposed division of the definition will only cause confusion and put a huge burden on the industry to revise internal documentation as well as reclassifying their assets.	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
While Duke Energy can support this in theory, we believe that if the drafting team is intending to include data storage that is already a part of the EACMS, that a method will need to be provided on how the data should be stored and tracked, prior to disposal of said data.	

Likes 0	
Dislikes 0	
Response	
John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	No
Document Name	
Comment	
Tacoma Power supports comments submitted by APPA.	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	No
Document Name	
Comment	
BCSI outside the entities environment should be dealt with in the CIP standards apart from the existing Requirement R2.	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No
Document Name	
Comment	
This information does not pose sufficient risk to the BES to warrant additional protections.	
Likes 0	
Dislikes 0	

Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	
N&ST believes it may be appropriate to extend the applicability of CIP-011 Requirement R2 to all so-called “designated storage locations” for BES Cyber System Information.	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
The scope of CIP-011 Requirement R2 should not be expanded and is sufficient as written.	
Likes 0	
Dislikes 0	
Response	
Brandon McCormick - Florida Municipal Power Agency - 3,4,5,6 - FRCC, Group Name FMPA	
Answer	No
Document Name	2016-02_Virtualization_Unofficial Comment Form_FMPA_comments.docx
Comment	
Please see attached comments	
Likes 0	
Dislikes 0	
Response	

Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	No
Document Name	
Comment	
We disagree with this. We opined that the access monitoring system should be part of EACMS rather than becoming a BCSI repository.	
Likes 0	
Dislikes 0	
Response	
Richard Kinas - Orlando Utilities Commission - 3,5	
Answer	No
Document Name	
Comment	
Some auditors are already putting forth the concept that all BCAs contain BCSI; by addressing CIP-011 R2 have to protect the SIEM even if it was not identified as an EACMS. The scope might need to be reduced. Need to provide more clarificaiton and the security benefit on the definition of BCSI as it relates to various information. It is not all a the same risk level. Need to use words like "information uesful to plan a cyber attack? Simply useful, or does the information provide just about eveything you need.	
Likes 0	
Dislikes 0	
Response	
Don Schmit - Nebraska Public Power District - 1,3,5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 1,5	

Answer	Yes
Document Name	

Comment

Reclamation does not support additional requirements created in CIP-011. Reclamation recommends the required level of protection be determined for all systems based on each system's impact rating as described in the recommended Impact Rating Criteria in the response to Question 24.

Likes 0	
Dislikes 0	

Response

Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - FRCC,MRO,WECC,Texas RE,SERC,SPP RE, Group Name Southern Company

Answer	Yes
Document Name	

Comment

Yes – because there is current ambiguity in the "Applicable Systems" assigned to CIP-011-2 R2. The requirement currently states "Prior to the release for reuse (or R2.2 disposal) of applicable Cyber Assets", which only includes High Impact BES Cyber Systems and Medium Impact BES Cyber Systems, and their associated EACMS, PACS, and PCAs; however, BCSI could reside in other places besides on those applicable systems. The requirement should be made clearer to direct the sanitization requirements to BCSI, regardless of where it resides, prior to the release for reuse or disposal.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

BPA believes that this should be a security objective, not a prescriptive technical requirement, and secure storage of SIEM information can be accomplished contractually. FedRAMP published guidance for outsourced storage services.

Likes 0	
Dislikes 0	

Response

Robert Ganley - Long Island Power Authority - 1	
Answer	Yes
Document Name	
Comment	
To prevent leakage of BCSI.	
Likes 0	
Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3,5	
Answer	Yes
Document Name	
Comment	
Cowlitz supports BPA comment.	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Joel Charlebois - AESI - Acumen Engineered Solutions International Inc. - 5	

Answer	Yes
Document Name	
Comment	
Yes – access monitoring systems can potentially contain BCSI and should be protected as such. That being said, monitoring systems also pose an additional risk that BCSI on its own does not: i.e. compromise of a monitoring system can be used to mask attempts to compromise the access control systems and the BCS itself. This additional risk needs to be addressed.	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8,9 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lauren Price - ATCO Electric - 1 - MRO,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chantal Mazza - Hydro-Qu?bec TransEnergie - 2 - NPCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Bob Case - Black Hills Corporation - 1 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Janis Weddle - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Chelan PUD	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Scott Downey - Peak Reliability - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	
Document Name	
Comment	
No comment at this time.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE does not have comments on this question.	
Likes 0	
Dislikes 0	

Response	
David Francis - Midcontinent ISO, Inc. - 2,3 - MRO,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG	
Answer	
Document Name	
Comment	
No Comment	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5	
Answer	
Document Name	
Comment	
Yes.	
Likes 0	
Dislikes 0	
Response	

19. Do you agree with assignment of CIP Standard requirements to each of the EACS, EAG, and CMS categories as presented in the table above? If not, please provide rationale to support your position.

Richard Kinas - Orlando Utilities Commission - 3,5

Answer	No
Document Name	

Comment

We believe that the table is incomplete and confusing by incorporate differnt concepts and definitions on the same table.

To address the splitting out of EACMS create table with:

- EACS, EAMS, and EACMS to clearly see what the diffrences would be

To address the new requirements for CMS and EAG place on a seperate table

Likes 0	
Dislikes 0	

Response

Mike Smith - Manitoba Hydro - 1,3,5,6

Answer	No
Document Name	

Comment

We disagree with this. See the same comments as in question 14.

Likes 0	
Dislikes 0	

Response

Janis Weddle - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Chelan PUD

Answer	No
Document Name	

Comment

Other than the requirement to segregate EACS systems into an Electronic Security Perimeter which is the whole point of this exercise, the requirements for EACS and EAG should be subsets of the existing EACMS requirements. The SDT should not be adding new requirements for these devices, such as CIP-009-6 R2.3 and CIP-010-2 R3.2, which do not currently apply to them.	
Likes 0	
Dislikes 0	
Response	
Robert Ganley - Long Island Power Authority - 1	
Answer	No
Document Name	
Comment	
All cyber assets in support of the BES should be afforded the highest level of protections as the highest watermark to reduce/mitigate any potential risks that can impact the systems directly or indirectly.	
Likes 0	
Dislikes 0	
Response	
Don Schmit - Nebraska Public Power District - 1,3,5	
Answer	No
Document Name	
Comment	
We do not believe a change is necessary.	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	

N&ST’s “No” entry reflects “No” entries for questions 4, 14, and 15.

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

CIP-004 R1.1 Awareness messages should not be limited by system type or function. All employees have a role to play in the BES security and should receive awareness.

CIP-004 R2 Cyber Security training should not be limited by system type of function.

CIP-004 R3.1 This requirement should not apply to EAGs as some work is done by a collection of analysts and reported on as a group such as a watch floor.

CIP-004 R3.4 Service providers should be able to provide evidence of their employee risk assessment process as an alternative to risk assessment conducted by the registered entity.

CIP-004 R4.2 CMS, EACS, EAGs should be able to show a process for granting and removing access, but a quarterly review should not be required.

CIP-004 R4.4 EACS & EAGs should not be labeled as BES Cyber System Information and a 15-month review should not be required.

CIP-004 R5.5 This should only apply to systems with ERC.

CIP-007, CIP-009, CIP-010, and CIP-011 should be modified to reflect the risk/impact of these systems to the BES.

Likes 0

Dislikes 0

Response

Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6

Answer No

Document Name

Comment

AZPS disagrees with the inclusion of CMS and EACS to the Applicable Systems of CIP-005 R1.x because both systems types may reside outside of an ESP and would not be applicable to R1.x.

AZPS proposes the addition of EACS to the Applicable Systems of CIP-005 R2.x because EACS responsible for authenticating Interactive Remote Access should be accessed through or be a part of an Intermediate System.

Likes 0	
Dislikes 0	

Response

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group

Answer	No
Document Name	

Comment

The SPP Standard Review Group feels that the current definition gives the industry flexibility in this process. From our perspective, the proposed division of the definition will only cause confusion and put a huge burden on the industry to revise internal documentation as well as reclassifying their assets.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Xcel Energy believes CMS should also be included in CIP-009 R2.3. CIP-010 R3.2 has many questions around how it would be implemented and frequency of reviews, specifically for EACS.

Likes 0	
Dislikes 0	

Response

David Francis - Midcontinent ISO, Inc. - 2,3 - MRO,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG

Answer	No
Document Name	

Comment

- Awareness is not a good means of providing necessary content to SMEs managing these assets. The existing training requirements are more beneficial.
- The 36 month operational recovery exercise is limited to BES Cyber Systems and should remain with that scope.
- Recovery plans should be required for all assets other than PCA.
- See comments on question 18 regarding CIP-011 requirements.

Likes 0	
Dislikes 0	

Response

Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs

Answer	No
Document Name	

Comment

All cyber assets in support of the BES should be afforded the highest level of protections as the highest watermark to reduce/mitigate any potential risks that can impact the systems directly or indirectly.

Likes 0	
Dislikes 0	

Response

Shelby Wade - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company

Answer	No
Document Name	

Comment

While we agree that many requirements will need to be updated based on the changes proposed in this comment form, there is some confusion on how the Applicable Systems will look based on the chart above. For instance, are the systems in the chart associated with high or medium impact BES Cyber Systems? Also, it is unclear how the CIP-005 Part 1 requirements will be applied to EACS. Furthermore, based on risk and current Applicable Systems, it is unclear what the justification is for adding EACS and EAGS to CIP-004 Part 1, CIP-009 Part 2.3 and CIP-010 Part 3.2 considering that EACMS are not currently part of the requirements.

Likes 0	
Dislikes 0	

Response

sean erickson - Western Area Power Administration - 1,6

Answer	No
Document Name	

Comment

Comments: Any CMS requirements need to be evaluated much more broadly than just in the context of virtualization. It doesn't make sense to singling out virtualization for special treatment that non-virtualized systems with similar risk-profiles do not get.

Likes 0	
Dislikes 0	

Response

Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2

Answer	No
Document Name	

Comment

ERCOT does not agree with the assignments of the requirements as shown in the table. First, ERCOT does not see the need to define EACS, EAG, and CMS. With regards to the table, there are several concerns noted. (1) Awareness is not a good means of providing necessary content to SMEs managing these assets. The existing training requirements are more beneficial and appropriate. (2) The 36 month operational recovery exercise is limited to BES Cyber Systems. This should remain as the scope. (3) Recovery plans should be required for all assets other than PCA. This is the current requirement level. (4) See comments on question 18 regarding CIP-011 requirements.

Likes 0	
Dislikes 0	

Response

Wendy Center - U.S. Bureau of Reclamation - 1,5

Answer	No
Document Name	

Comment

With the exception of CIP-002, Reclamation does not support modifying the existing standards.

Reclamation recommends adding new or appropriate industry-recognized definitions to the NERC Glossary of Terms and revising the BES Cyber System definition as described in the recommended definitions section of the response to Question 24.	
Likes 0	
Dislikes 0	
Response	
Lauren Price - ATCO Electric - 1 - MRO,RF	
Answer	No
Document Name	
Comment	
The table does not provide enough detail to fully understand the compliance requirements for each Cyber Asset category. For example, does an EACS need to be in an ESP re: CIP-005 R1 Part 1.1?	
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 ISO-NE NYISO NextERA Con-Ed and HQ	
Answer	No
Document Name	
Comment	
Since the question is about “access monitoring systems" it would include both electronic and physical access monitoring data. It is our view that not all monitoring data would need to be included since this information does not meet the BCSI definition.	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 3,5	
Answer	No
Document Name	
Comment	

AEP requests the SDT refer to our response to Question #13.

Likes 0

Dislikes 0

Response

Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8,9 - WECC

Answer	No
Document Name	

Comment

SDG&E does not agree that CIP-005 2.3 could/should apply to CMS, EAGs and EACS if technically feasible.

Likes 0

Dislikes 0

Response

Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE

Answer	No
Document Name	

Comment

The question is asking for support of the assignment of CIP Standards to proposed EACS, EAG, and CMS definitions in which we have concerns. We are unable to analyze the assignments with uncertainty around the definitions.

We would note that the table illustrates how the proposed Glossary Terms—EACS, EAG, and CMS—potentially create more questions than clarity regarding compliance requirements and may present an undesirable effect of obscuring compliance obligations.

Likes 0

Dislikes 0

Response

Ronald Donahey - TECO - Tampa Electric Co. - 1,3,5,6

Answer	No
Document Name	

Comment

We believe that the table is incomplete. Some redlines and comments are provided for the table itself. One example is to add to the CMS column for CIP-009. We recommend adding a column for EAMS since there is an option for the EACMS Glossary Term to be continued as it stands.	
Likes 0	
Dislikes 0	
Response	
John Tolo - Unisource - Tucson Electric Power Co. - 1	
Answer	No
Document Name	
Comment	
Definitions are clear; the guidance is complex. Prefer consistency.	
Likes 0	
Dislikes 0	
Response	
Joel Charlebois - AESI - Acumen Engineered Solutions International Inc. - 5	
Answer	Yes
Document Name	
Comment	
The new categories of EACS, EAG, and CMS will be more descriptive and work better for the utilities as long as the definition of EACMS is retired. Combination of EACMS, EACS, EAG, and CMS may cause confusion and frustration for anyone trying to adequately define cyber assets into their proper category.	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	

N/A	
Likes 0	
Dislikes 0	
Response	
Bob Case - Black Hills Corporation - 1 - WECC	
Answer	Yes
Document Name	
Comment	
Conceptually, yes, but mapping table provided was not thoroughly vetted for this question.	
Likes 0	
Dislikes 0	
Response	
Chantal Mazza - Hydro-Qu?bec TransEnergie - 2 - NPCC	
Answer	Yes
Document Name	
Comment	
There are requirements, specifically those found in R4 of CIP-007 about security event log retention and review. Does the SDT intend to have BCSI, designated storage location as the applicable systems for these requirements or remove these requirements for the monitoring systems altogether?	
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

Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - FRCC,MRO,WECC,Texas RE,SERC,SPP RE, Group Name Southern Company

Answer	Yes
Document Name	

Comment

As long as the definition of CMS is modified as previously stated to scope it to virtual multi-instance environments.

Likes 0	
Dislikes 0	

Response

Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Russell Noble - Cowlitz County PUD - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brandon McCormick - Florida Municipal Power Agency - 3,4,5,6 - FRCC, Group Name FMPA	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5	
Answer	
Document Name	
Comment	
No. - Keep existing EACMS definition – do not create EAG and EACS.	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	
Document Name	
Comment	
See comments in response to Question Nos. 13 – 17.	
Likes 0	
Dislikes 0	

Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE does not have comments on this question.	
Likes 0	
Dislikes 0	
Response	
Paul Haase - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light	
Answer	
Document Name	
Comment	
City Light is undecided at this time.	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	
Document Name	
Comment	
No comment at this time.	
Likes 0	
Dislikes 0	
Response	

20. As the standards today do not prohibit the use of virtualization technologies, do you support an approach where no changes are made to the CIP Standards in response to the virtualization issue identified by the V5 TAG? Please provide a rationale to support your position.

Paul Haase - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light	
Answer	No
Document Name	
Comment	
City Light believes new approaches are necessary to accomodate virtualization with the CIP Standards, and generally supports the comments of APPA and BPA. City Light, however, would prefer the a more general cyber security approach be used for virtualization. NIST or PCI provide useful frameworks, rather than the VM Ware-centric approach proposed here.The VM Ware approach is not unreasonable, but aligns with a particular vendor.	
Likes 0	
Dislikes 0	
Response	
John Tolo - Unisource - Tucson Electric Power Co. - 1	
Answer	No
Document Name	
Comment	
Virtualization security needs to be addressed because security and operational gains are both important goals. We support addressing the concerns directly.	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8,9 - WECC	
Answer	No
Document Name	
Comment	
SDG&E contends that changes to the CIP standards must be implemented for virtualization in order to protect the integrity and safety of the Bulk Electric System as captured in our responses above.	
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 ISO-NE NYISO NextERA Con-Ed and HQ

Answer	No
Document Name	

Comment

The current CIP standards do not explicitly prohibit all types of virtualization but require “high water marking” of the impact level even where this is not the most secure and reliable control. For example the separation of data plane and management plane between hypervisor and guest is a more effective control than applying high water mark CIP Requirements and keeping hypervisors inside the same security zone.

Also, CIP Requirements do not separate the electronic access controls from the electronic access monitoring to allow for different requirements when only monitoring is done. This has a high risk of misallocating scarce resources (money, time, manpower) that could be more effectively applied elsewhere for increased reliability.

Compliance Guidance is written to show one or more compliant solutions in order to clarify and help in applying the Requirements. It does not supersede Requirements language. The Guidance cannot show all possible solutions and is therefore inadequate because it is specific and limited, rather than a framework one can apply to generate new and unique solutions. Solutions currently known to the SDT are only a snapshot in time that may become obsolete at any moment due to technical innovation or changes in the threat environment, while security objectives are more enduring than requirements for a specific solution. Entities may be aware of or devise a solution unknown to the SDT that provides equal or greater security but if the Requirements language doesn’t allow for the solution, it is not compliant. For these reasons, I think that the issues must be dealt with by revisions to the standards that emphasize security objectives and allow the Entity to demonstrate and explain how the solution meets the objective.

Likes 0	
Dislikes 0	

Response

Lauren Price - ATCO Electric - 1 - MRO,RF

Answer	No
Document Name	

Comment

ATC believes that there is merit to this concept; however, we answered “No” because guidance alone cannot solve the specific subject of virtualization due to the current construct of the CIP Requirements and its reliance on prescriptive controls that lean toward less advanced technological solutions. ATC could support ERO Enterprise-endorsed Compliance Guidance as an alternative if it were complimented by a paradigm shift to reshape the CIP Standards such that they are focused on technology agnostic security objectives and written with flexibility so Registered Entities are able to define and implement an adaptive risk-based cybersecurity program that timely detects, responds to, and mitigates emerging threats. ATC welcomes thought leadership on the subject of ERO Enterprise-endorsed Compliance Guidance as an alternative to mandatory regulations to position the industry for a more nimble, sustainable, and mature security posture. While there has been improvement in the requirement language as the CIP Standards have evolved, they continue to suffer because prescriptive mandatory regulations cannot keep pace with emerging technologies and the rapidly changing cybersecurity threat landscape. Until this paradigm shift occurs, the industry will continue to face the unintended consequences of the current construct, be distracted by the conundrum, divided between security and compliance, limited in our ability to leverage advances in technology, and will continue to be hindered by the antiquated ideals of a regulation that is chasing cybersecurity.

Likes 0	
Dislikes 0	

Response

Wendy Center - U.S. Bureau of Reclamation - 1,5

Answer	No
Document Name	

Comment

With the exception of CIP-002, Reclamation does not support modifying the existing standards.

Reclamation recommends that simplifying the Impact Rating Criteria in CIP-002 and adding new or appropriate industry-recognized definitions to the NERC Glossary of Terms to address virtualization technologies will resolve industry concerns (refer to the recommended definitions and revised Impact Rating Criteria sections of the response to Question 24).

Likes 0	
Dislikes 0	

Response

Shelby Wade - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company

Answer	No
Document Name	

Comment

Even though the requirements today do not prohibit the use of virtualization, the implementation of virtualization in today’s CIP regulatory construct discourages an entity from realizing the full potential of virtualization. Making the right changes to the requirements will allow entities the ability to fully utilize emerging technologies while supporting the reliable operations of the BES.

Likes 0	
Dislikes 0	

Response

Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	No
Document Name	
Comment	
More definition is needed around virtualization. There is too much risk to the utility as it is left up to interpretation.	
Likes 0	
Dislikes 0	
Response	
John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	No
Document Name	
Comment	
Tacoma Power supports comments submitted by APPA. Tacoma Power supports comments submitted by BPA.	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	No
Document Name	
Comment	
The SDT should explicitly address virtualization in the CIP Standard to provide clarity for securely separating CIP assets in virtualized environments.	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	

Answer	No
Document Name	

Comment

The current CIP standards do not explicitly prohibit all types of virtualization but require “high water marking” of the impact level even where this is not the most secure and reliable control. For example, the separation of data plane and management plane between hypervisor and guest is a more effective control than applying rigorous CIP Requirements and keeping hypervisors inside the same security zone.

Also, CIP Requirements do not separate the electronic access controls from the electronic access monitoring to allow for different requirements when only monitoring is done. This has a high risk of misallocating scarce resources (money, time, manpower) that could be more effectively applied elsewhere for increased reliability.

Compliance guidance is written to show one or more compliant solutions to clarify and help in applying the Requirements. Such guidance does not supersede standard requirements language. Moreover, such guidance cannot show all possible solutions and is specific and limited, rather than a framework where one can generate new and unique solutions. Solutions currently known to the SDT are only a snapshot in time that may become obsolete at any moment due to technical innovation or changes in the threat environment, while security objectives are more enduring than requirements for a specific solution. Entities may be aware of, or devise a solution unknown to the SDT that provides equal or greater security, that the Requirements language finds the solution non-compliant. Therefore, the proposed standard must emphasize security objectives that allow entities to demonstrate and explain how solutions meets the objective.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

BPA believes that changes to the standards language are required to enable virtualization in a secure and reliable manner and that implementation should allow for secure shared infrastructure.

The NERC CIP SDT has a responsibility to evolve the standards language with our industry and not restrict its progress in adopting new, more efficient, fiscally responsible, secure, and reliable technology solutions. The current CIP reliability standards, as written, are not easily applied to new technologies, such as virtualization. They are written specific to dated industrial control systems of our industry and do not address virtualization technologies. If NERC uses only guidance rather than security objectives standards language, we can expect significant impacts, such as compliance violations, costly rework of in-flight and future planned upgrade projects, and slowing the adoption of new technologies that can better secure and improve the reliability of the Bulk Electric System.

- Guidance outside of the standards does not address the V5TAG mandate from the SAR to address virtualization in the standards language
- Without direct guidance in standards, entities can find themselves at risk of compliance violations due to individual different interpretations.
- It is clear from the debate regarding virtualization implementations that there is no universal agreement about shared infrastructure being allowed.

- Virtual Technology that is already in the near-term pipeline and deployed in other industries would benefit the energy industry.
- Without transitioning to a security objective-based standard, flexibility to adapt to new technology is lost.
- Presidential directives for government agencies already require aggressive moves to cloud computing for reasons of common secure platforms, scalability and cost benefit.

Likes 0	
Dislikes 0	

Response

Chantal Mazza - Hydro-Qu?bec TransEnergie - 2 - NPCC

Answer	No
Document Name	

Comment

The current CIP standards do not explicitly prohibit all types of virtualization but require “high water marking” of the impact level even where this is not the most secure and reliable control. For example the separation of data plane and management plane between hypervisor and guest is a more effective control than applying high water mark CIP Requirements and keeping hypervisors inside the same security zone.

Also, CIP Requirements do not separate the electronic access controls from the electronic access monitoring to allow for different requirements when only monitoring is done. This has a high risk of misallocating scarce resources (money, time, manpower) that could be more effectively applied elsewhere for increased reliability.

Compliance Guidance is written to show one or more compliant solutions in order to clarify and help in applying the Requirements. It does not supersede Requirements language. The Guidance cannot show all possible solutions and is therefore inadequate because it is specific and limited, rather than a framework one can apply to generate new and unique solutions. Solutions currently known to the SDT are only a snapshot in time that may become obsolete at any moment due to technical innovation or changes in the threat environment, while security objectives are more enduring than requirements for a specific solution. Entities may be aware of or devise a solution unknown to the SDT that provides equal or greater security but if the Requirements language doesn’t allow for the solution, it is not compliant. For these reasons, I think that the issues must be dealt with by revisions to the standards that emphasize security objectives and allow the Entity to demonstrate and explain how the solution meets the objective.

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

To properly apply the standards to a virtual environment, they must be changed to adequately enforce the required security practices.	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	
N&ST believes would be appropriate to modify the CIP Standards in order to both clarify the applicability of requirements to virtual devices and, in some instances, to define new requirements (such as for ESZs) that would apply to virtual devices.	
Likes 0	
Dislikes 0	
Response	
Brandon McCormick - Florida Municipal Power Agency - 3,4,5,6 - FRCC, Group Name FMPA	
Answer	No
Document Name	2016-02_Virtualization_Unofficial Comment Form_FMPA_comments.docx
Comment	
Please see attached comments	
Likes 0	
Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3,5	
Answer	No
Document Name	
Comment	
Cowlitz supports APPA comment.	

Likes 0	
Dislikes 0	
Response	
Bob Case - Black Hills Corporation - 1 - WECC	
Answer	No
Document Name	
Comment	
We support changes being explicit.	
Likes 0	
Dislikes 0	
Response	
Janis Weddle - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Chelan PUD	
Answer	No
Document Name	
Comment	
The current CIP reliability standards as written are far too open to interpretation and not easily applied to new technologies, such as virtualization. New or modified CIP Standards surrounding virtualization will bring clarity and objective criteria to evaluate against such implementations.	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	No
Document Name	
Comment	
The current Cyber Asset doesn't clearly state that the programmable device includes virtual machine. Also current EACMS definition doesn't include the cyber system that can alter the configuration of BCS explicitly even though it implies that. As long as these definitions are modified, all applicable virtual devices would be protected by the current CIP standards.	

Likes 0	
Dislikes 0	
Response	
Joel Charlebois - AESI - Acumen Engineered Solutions International Inc. - 5	
Answer	No
Document Name	
Comment	
Currently, the standards require a bit of “common sense” interpretation to be applied to virtualized systems appropriately. Different entities may have different interpretations, some of which may not result in an appropriate level of security for the relevant BCS. Providing guidance may help in this regard, but adjusting the standards to address virtualization will ensure that a minimum enforceable level of security is applied by all entities without relying on interpretation.	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Downey - Peak Reliability - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Ronald Donahey - TECO - Tampa Electric Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
We agree with an approach that does not change the standards. We also recommend that the GTB should go into the Compliance Guidelines. We also recommend that the SDT yay just need to modify the definition of Cyber Asset. There is a concern that the number of unanticipated consequences could be much more damaging than anything we are fixing with changes to the requirement parts and glossary terms. .	
Likes 0	
Dislikes 0	
Response	
Mark Riley - Associated Electric Cooperative, Inc. - 1,3,5,6, Group Name AECI & Member G&Ts	
Answer	Yes
Document Name	
Comment	
The current CIP standards can apply to a virtual environment. Some guidance and examples would assist Registered Entities in identifying a compliant approach when implementing virtualization technologies. More specifically, ERO Enterprise-endorsed Compliance Guidance could be used to address the implementation of virtualization.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE	
Answer	Yes
Document Name	
Comment	

KCP&L supports using current CIP Standards to address risk posed by virtualization.

Complexity Defeats Security

Some of the offered concepts may have merit but when considered independently or in total, the consequence of implementing and managing the proposed idea will assuredly add significant complexity to already complex systems.

By most any measure, complexity defeats security through obfuscation of vulnerabilities and can provide a false sense of security.

Promotes Flexibility. Virtualization technology will continue to evolve at a rate faster than the Standards can address. Compliance guidance provides a path for implementation and the Standards' role to be objective. Additionally, compliance guidance allows the flexibility to relieve compliance burdens on entities choosing not to implement virtual technologies.

Likes 0	
Dislikes 0	

Response

Aaron Austin - AEP - 3,5

Answer	Yes
Document Name	

Comment

AEP believes a reasonable person can apply the existing CIP requirements in a virtual environment. A reasonable audit approach is possible as well. Implementation (Compliance) Guidance would be helpful.

Likes 0	
Dislikes 0	

Response

Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2

Answer	Yes
Document Name	

Comment

ERCOT agrees with making no revisions to the standards as proposed. See comments provided in response to questions 1-12. The concepts of virtualization have been contemplated since CIP version 1 requirements. Example implementations would be very beneficial to industry and suffice to provide the clarity needed irrespective of the technology implemented.

Likes 0	
Dislikes 0	

Response	
Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - FRCC,MRO,WECC,Texas RE,SERC,SPP RE, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Given the current regulatory landscape and massive compliance challenges recently with evolving CIP Standards, Southern Company would be open to exploring, given the appropriate level of industry input and acceptance, ERO Enterprise-endorsed Compliance Guidance to address the proper implementation of virtualization.	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	Yes
Document Name	
Comment	
Comments: There are so many CMS-like systems that don't involve virtualization that singling out virtualization seems counterproductive. Certainly there is benefit to guidance as to how host systems/hypervisors are treated, but the guest systems seem to be straight-forward with regard to relevant controls.	
Likes 0	
Dislikes 0	
Response	
Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
All cyber assets in support of the BES should be afforded the highest level of protections as the highest watermark to reduce/mitigate any potential risks that can impact the systems directly or indirectly.	
Likes 0	

Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Rather than changing the requirements, Texas RE suggests modifying the definition of Cyber Asset to also specifically include virtual devices. Virtual devices should be handled the same as physical Cyber Assets. Texas RE is concerned the proposed changes to the requirement language by the SDT appear too prescriptive.	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	
The current CIP standards, allow for virtual environments as CIP assets. Adding the changes above will make it more complex and add more confusion to the environments.	
Likes 0	
Dislikes 0	
Response	
Don Schmit - Nebraska Public Power District - 1,3,5	
Answer	Yes
Document Name	
Comment	
See comment #23.	
Likes 0	

Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
CenterPoint Energy believes the current CIP standards can apply to a virtual environment. Some guidance and examples for workable solutions for hosted systems, virtual LANs, and even cloud based systems could help Registered Entities be more comfortable with their compliance approach when implementing virtualization technologies.	
Likes 0	
Dislikes 0	
Response	
Robert Ganley - Long Island Power Authority - 1	
Answer	Yes
Document Name	
Comment	
All cyber assets in support of the BES should be afforded the highest level of protections as the highest watermark to reduce/mitigate any potential risks that can impact the systems directly or indirectly.	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Virtualization is not prohibited by the present version of the CIP Standards. Each hardware platform is considered a device and each VM running on the hardware is considered software and data on the device. This means that the hardware device and each VM running on that device must be protected at the level of the highest-impact VM running on the device. This is seldom an issue in a Control Center, where all Cyber Assets are protected at the level of the “high-water-mark.”	

Economic considerations seem to be the biggest driving force in pushing forward “mixed-trust” virtual systems. These considerations will primarily benefit relatively the relatively few companies that can justify the large-scale systems needed for a significant economic return. Other companies will be required to wade through a number of new requirements that may have little benefit to them.

In addition, properly securing mixed-trust virtual systems requires a staff with substantial skills and training. The staff of mid-size and small companies may be ill-equipment to succeed in that endeavor.

Likes 0	
Dislikes 0	

Response

Richard Kinas - Orlando Utilities Commission - 3,5

Answer	Yes
Document Name	

Comment

We agree with an approach that does not change the standards. We also recommend that the GTB should go into the Compliance Guidelines. We also recommend that the SDT may just need to modify the definition of Cyber Asset.

There is a concern that the number of unanticipated consequences could be much more damaging than anything we are fixing with changes to the requirement parts and glossary terms.

Likes 0	
Dislikes 0	

Response

Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	
Document Name	
Comment	
No comment at this time.	
Likes 0	
Dislikes 0	
Response	
David Francis - Midcontinent ISO, Inc. - 2,3 - MRO,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG	
Answer	
Document Name	
Comment	
No Comment	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5	

Answer	
Document Name	
Comment	
No. Keep standards up to date with existing technologies else future revisions will take tremendous time to be developed.	
Likes 0	
Dislikes 0	
Response	

21. Is your organization in support of Concept 1: Modifications to allow use of secure multi-instance? Please provide rationale to support your position.

Richard Kinas - Orlando Utilities Commission - 3,5	
Answer	No
Document Name	
Comment	
Maybe If the changes were made per the comments above, we might be able to support the concept. If there are no changes made related to concept 1, we do not support it.	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	
Modifications to allow the secure use of multi-instance will add a large amount of complexity and ambiguity to the CIP Standards while providing a significant benefit to only a small number of entities.	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	No
Document Name	
Comment	
We never use multi-instance concept. It is not clear whether it only applies to the virtual machines or physical devices as well.	
Likes 0	
Dislikes 0	

Response	
Bob Case - Black Hills Corporation - 1 - WECC	
Answer	No
Document Name	
Comment	
Modifications are not required for secure multi-instance environments. What the SDT is proposing is secure, and non-secure, multi-instance environments. We support exploring how multi-instance environments could be allowed in a secure manner, but this appears to be a change to save costs, not necessarily increase security.	
Likes 0	
Dislikes 0	
Response	
Brandon McCormick - Florida Municipal Power Agency - 3,4,5,6 - FRCC, Group Name FMPA	
Answer	No
Document Name	2016-02_Virtualization_Unofficial Comment Form_FMPA_comments.docx
Comment	
Please see attached comments	
Likes 0	
Dislikes 0	
Response	
Robert Ganley - Long Island Power Authority - 1	
Answer	No
Document Name	
Comment	
Unless properly designed, configured and implemented multi-instance environments can lead to potential unknown/unrealized risks, added complexity, and added compliance exposure for systems not associated with BCA's. Segregated environments can be more beneficial in reducing overall risk and compliance exposure.	
Likes 0	
Dislikes 0	

Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
See comments in response to Question Nos. 1-12.	
Likes 0	
Dislikes 0	
Response	
Don Schmit - Nebraska Public Power District - 1,3,5	
Answer	No
Document Name	
Comment	
Our position is that it would be difficult to secure a multi-instance environment and difficult to audit and thus too much risk to BES Cyber Systems to be utilized.	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	No
Document Name	
Comment	
See comments to questions (1 – 12) referencing the Concept 1 Section.	
Likes 0	
Dislikes 0	
Response	

Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	No
Document Name	
Comment	
Xcel Energy believes that further development of concepts and terms is needed before support can be given to any of the proposed options.	
Likes 0	
Dislikes 0	
Response	
David Francis - Midcontinent ISO, Inc. - 2,3 - MRO,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG	
Answer	No
Document Name	
Comment	
See comments provided in response to each question under Concept 1.	
Likes 0	
Dislikes 0	
Response	
Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	No
Document Name	
Comment	
Unless properly designed, configured and implemented multi-instance environments can lead to potential unknown/unrealized risks, added complexity, and added compliance exposure for systems not associated with BCA's. Segregated environments can be more beneficial in reducing overall risk and compliance exposure.	
Likes 0	
Dislikes 0	
Response	

Shelby Wade - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company	
Answer	No
Document Name	
Comment	
While we are in support of the modifications to allow the use of secure multi-instance we have some concerns, questions and suggestions on the current approach. Please see our comment on question 24.	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	No
Document Name	
Comment	
Comments: Clarity should be provided on the equivalence between virtual cyber assets and physical cyber assets. Systems involving multiple cyber assets (physical or virtual), or centralized management systems (VMs, SDNs, SANS, Antivirus, etc.), should be addressed as a whole in a risk-based way. Virtualization should not be singled out for special scrutiny.	
Likes 0	
Dislikes 0	
Response	
Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - FRCC,MRO,WECC,Texas RE,SERC,SPP RE, Group Name Southern Company	
Answer	No
Document Name	
Comment	
The concepts and definitions proposed need additional clarification to ensure proper scoping and applicability of any subsequent requirements. Southern appreciates the SDTs work in this regard, and views this as a step in the right direction, but additional refinement appears to be needed.	
Likes 0	
Dislikes 0	

Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
See comments provided in response to questions 1-12.	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	
With the exception of CIP-002, Reclamation does not support modifying the existing standards. Reclamation recommends that simplifying the Impact Rating Criteria in CIP-002 and adding new or appropriate industry-recognized definitions, including Virtual Instance and Multi-Virtual Instance, to the NERC Glossary of Terms to address the use of secure multi-instance (refer to the responses to Questions 6 and 24).	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 3,5	
Answer	No
Document Name	
Comment	
AEP believes the existing RS requirement language and the definition language with minor modifications is sufficient.	
Likes 0	
Dislikes 0	

Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8,9 - WECC	
Answer	No
Document Name	
Comment	
SDG&E seeks resolution to comments posted regarding Concept 1 before it moves forward.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE	
Answer	No
Document Name	
Comment	
Modifying the Requirements to allow use of secure multi-instance is not necessary. Entities require flexibility to address the spectrum of systems within the entity and external to the entity. Adding Requirements unfavorably impacts the desired flexibility implementing Standards and managing the security of Cyber Systems.	
Likes 0	
Dislikes 0	
Response	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	
Comment	
In virtualization terminology, "instance" is used to describe a single *instance* of a resource. If the SDT means "multi-tenant" in their use of "multi-instance", it is suggested to use the former term. It is easier to explain that an organization can internally have many "tenants" that for whom shared resources are compartmentalized then to explain having multiple instances of environments which in turn have multiple instances of computing resources. It's difficult to communicate about compliance and virtualization even amongst people who understand the distinction between the two types of instances.	

The CMS is a good approach. It would be preferable to only be applicable to Virtualized Systems, at least at first, in effort to address the systemic risk introduced by virtualization.

The ESZ concept does not reflect how virtualization systems work and adds an extra level of unnecessary and confusing complexity to the CIP standards. What is needed is requirements that, if met, let virtual cyber assets be treated as “normal” cyber assets. And similarly, virtual networks the same as “normal” physical networks. Then the existing body of CIP Standards can be leveraged to mitigate additional virtualization risks without adding undo complexity and exceptions.

Suggest requirements to the effect of:

> Virtualization host environments must have mechanisms to ensure virtual machines or virtual components of machines (compute, network interface, storage) utilize mechanisms to ensure they are unable to interact with each other except as necessitated by design to fulfill their function. Ie: no direct compute node to compute node interaction, storage node to storage node interaction. Compute nodes can only access the storage resources they are specifically assigned. Virtual network interfaces are constrained to one virtual network (VLAN). Etc. The specific interaction being allowed and the details how this is enforced must be documented (IE VLAN#, etc).
>
> Possibly a requirement to test that the configuration needed for above requirement correctly isolates/segregates virtual resources (again, only for virtualization).
>
> CMS used for managing virtualization hosts (ie. the management plane) must reside in a ESP that is distinct from the ESP of the virtual cyber assets it hosts (which still allows, incidentally, self hosting of management virtual machines)

Likes 0	
Dislikes 0	

Response

Ronald Donahey - TECO - Tampa Electric Co. - 1,3,5,6

Answer	No
Document Name	

Comment

Maybe

If the changes were made per the comments above, we might be able to support the concept. If there are no changes made related to concept 1, we do not support it.

Likes 0	
Dislikes 0	

Response

Scott Downey - Peak Reliability - 1

Answer	Yes
Document Name	
Comment	
The current version fo the standard is too open for individual interpretation. The effort to provide consistency is welcome.	
Likes 0	
Dislikes 0	
Response	
Joel Charlebois - AESI - Acumen Engineered Solutions International Inc. - 5	
Answer	Yes
Document Name	
Comment	
In general this concept addresses virtualization in a more consistent manner and avoids reliance on individual entities' interpretation. There may be areas which can be improved, but in general this is a step in the right direction.	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Janis Weddle - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Chelan PUD	
Answer	Yes
Document Name	

Comment	
While we generally support the approach outlined in Concept 1, it requires further refinement and needs to be explicitly drafted to truly understand the ramifications of the changes proposed. The current form is unacceptable, and needs revision Additionally, the concept addresses storage in its explanation, but does not address it in the requirements and definitions.	
Likes 0	
Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3,5	
Answer	Yes
Document Name	
Comment	
Cowlitz supports BPA comment.	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	Yes
Document Name	
Comment	
N&ST believes would be appropriate to modify the CIP Standards in order to both clarify the applicability of requirements to virtual devices and, in some instances, to define new requirements (such as for ESZs) that would apply to virtual devices.	
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	
Properly implemented security controls, monitoring, and processes can afford protections of a multi-instance virtual environment.	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Lack of language addressing virtualization leaves significant risk of misunderstanding between auditors and entities on proper implementation of multi-instance infrastructure. The problem of auditors and entities interpreting current standards applied to virtual implementations differently exists already even when using virtualization in a single-instance environment.	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	Yes
Document Name	
Comment	
Yes, provided that comments herein, are taken into consideration.	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	

Comment	
AZPS is a proponent of virtualization, but wants to do so in a safe and reliant manner. The allowed use of multi-instance environments would help to maximize resources and minimize costs.	
Likes 0	
Dislikes 0	
Response	
John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
Tacoma Power supports comments submitted by APPA.	
Likes 0	
Dislikes 0	
Response	
John Tolo - Unisource - Tucson Electric Power Co. - 1	
Answer	Yes
Document Name	
Comment	
Virtual architecture is important and must be directly addressed. If no regulations occur, we will still apply a high standard of security to these systems.	
Likes 0	
Dislikes 0	
Response	
Paul Haase - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light	
Answer	Yes
Document Name	
Comment	

City Light supports the comments of APPA and BPA, but encourages continued careful development, modification, and clarification of the concepts before they become enforceable Standards.	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chantal Mazza - Hydro-Qu?bec TransEnergie - 2 - NPCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4, Group Name FirstEnergy Corporation	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Lauren Price - ATCO Electric - 1 - MRO,RF	
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 ISO-NE NYISO NextERA Con-Ed and HQ	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5	
Answer	
Document Name	
Comment	
Yes.	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	

Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE suggests the current definitions and requirements are sufficient to protect virtual devices as virtual devices should be afforded the same protection as physical devices.	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	
Document Name	
Comment	
No comment at this time.	
Likes 0	
Dislikes 0	
Response	

22. Is your organization in support of Concept 2: Modifications to the EACMS definition? Please provide rationale to support your position.	
John Tolo - Unisource - Tucson Electric Power Co. - 1	
Answer	No
Document Name	
Comment	
We prefer consistency to the compliance complexity of dividing the roles into three and tracking requirements separately.	
Likes 0	
Dislikes 0	
Response	
Ronald Donahey - TECO - Tampa Electric Co. - 1,3,5,6	
Answer	No
Document Name	
Comment	
Industry could support it if it allowed entities to use cloud based SIEM. If it does not allow for cloud based SIEM support, they need to modified. This introduces more complexity and ambiguity due to unanticipated consequences	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE	
Answer	No
Document Name	
Comment	
The current EACMS elements are sufficient in providing implementation structure and flexibility to ensure the differences found in entities’ system designs address security without requiring highly prescriptive Standards.	
Likes 0	
Dislikes 0	
Response	

Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8,9 - WECC	
Answer	No
Document Name	
Comment	
SDG&E seeks resolution to comments posted regarding Concept 2 before it moves forward.	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 3,5	
Answer	No
Document Name	
Comment	
AEP agrees there is value in EACMS definition to allow the access-monitoring portion of the EACMS to be reclassified as a BSCI repository and the introduction of the CMD definitions, but does not support the additional definitions. We also believe that a revised definition of EACMS is all that is necessary to address the concerns.	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	
With the exception of CIP-002, Reclamation does not support modifying the existing standards. Reclamation recommends that simplifying the Impact Rating Criteria in CIP-002 and adding new or appropriate industry-recognized definitions to the NERC Glossary of Terms will resolve industry concerns (refer to the recommended definitions section of the response to Question 24).	
Likes 0	
Dislikes 0	

Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
ERCOT recognizes the value and supports only the changes related to monitoring systems. See comments provided for questions 13-19.	
Likes 0	
Dislikes 0	
Response	
David Francis - Midcontinent ISO, Inc. - 2,3 - MRO,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG	
Answer	No
Document Name	
Comment	
See comments provided in response to each question under Concept 2. Other than the monitoring part.	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	No
Document Name	
Comment	
Xcel Energy believes that further development of concepts and terms is needed before support can be given to any of the proposed options. Further granularity around 3rd party/off the shelf software would be helpful.	
Likes 0	
Dislikes 0	
Response	

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	No
Document Name	
Comment	
The SPP Standard Review Group feels that the drafting team has potentially added complexity to the process with the proposed language as well as an additional burden for the process to be implemented.	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	
N&ST believes modifications are not necessary and notes further that the so-called “hall of mirrors” problem that is put forth as a possible reason to modify the EACMS definition is not an inherent problem in either the existing EACMS definition or the current applicable CIP requirements.	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
See comments in response to Question Nos. 13-19.	
Likes 0	
Dislikes 0	
Response	
Brandon McCormick - Florida Municipal Power Agency - 3,4,5,6 - FRCC, Group Name FMPA	

Answer	No
Document Name	2016-02_Virtualization_Unofficial Comment Form_FMPA_comments.docx
Comment	
Please see attached comments	
Likes 0	
Dislikes 0	
Response	
Janis Weddle - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Chelan PUD	
Answer	No
Document Name	
Comment	
While the idea of splitting the definition of EACMS to allow broader implementation of security controls is appealing, that does not appear to be what the SDT is proposing. The SDT does remove most requirements for EAMS, but ramps up the requirements on EACS and EAG. For entities who have already implemented a SIEM in their CIP environment, there is little benefit, as we have already borne the burden of implementing CIP on our SIEM. While declassification might remove some of the burden, it is far outweighed by the increased obligation proposed by the SDT.	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	No
Document Name	
Comment	
We disagree with the modification to the EACMS definition and we proposed a different way to modify the EACMS definition (see question 4 feedback).	
Likes 0	
Dislikes 0	
Response	
Richard Kinas - Orlando Utilities Commission - 3,5	

Answer	No
Document Name	
Comment	
Industry could support it if it allowed entities to use cloud based SIEM. If it does not allow for cloud based SIEM support, they need to modified. This introduces more complexity and ambiguity due to unanticipated consequences	
Likes 0	
Dislikes 0	
Response	
Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - FRCC,MRO,WECC,Texas RE,SERC,SPP RE, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern Company agrees with the SDT that the current construct of the EACMS definition and associated requirements does not differentiate controls based on the functionality and risk of the system. Southern Company supports the SDTs efforts to address this by breaking up the EACMS categorization of applicable systems by function so that the appropriate requirements for each can be applied.	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	Yes
Document Name	
Comment	
Comments: In general, we agree with the rationale provided.	
Likes 0	
Dislikes 0	
Response	

Shelby Wade - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company	
Answer	Yes
Document Name	
Comment	
We are in support of the concept to modify the EACMS definition. The current definition does not take in account the types of assets contained with the EACMS definition and the risk of each type of asset.	
Likes 0	
Dislikes 0	
Response	
Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
To be more inclusive and defined.	
Likes 0	
Dislikes 0	
Response	
John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
Tacoma Power supports comments submitted by APPA.	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	

Answer	Yes
Document Name	
Comment	
The proposed modifications will increase the visibility for monitoring of CIP and other unrelated systems, but should be provided with an additional thorough evaluation to ensure that no unintended gaps or consequences could result as discussed above.	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	Yes
Document Name	
Comment	
Yes, provided that comments herein, are taken into consideration.	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
The term EACMS is too broad and not well defined. It does not address actual risk or available technical controls.	
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	
TVA welcomes the distinctions allowed by the modification to the EACMS definition. Changing the definition and revising the applicable standards will allow utilities to better protect the BES, and reduce the compliance burden on these systems.	
Likes 0	
Dislikes 0	
Response	
Robert Ganley - Long Island Power Authority - 1	
Answer	Yes
Document Name	
Comment	
To be more inclusive and defined	
Likes 0	
Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3,5	
Answer	Yes
Document Name	
Comment	
Cowlitz supports BPA comment.	
Likes 0	
Dislikes 0	
Response	
Bob Case - Black Hills Corporation - 1 - WECC	
Answer	Yes
Document Name	

Comment	
Provided the goal is to promote using enterprise wide monitoring systems to monitor BCS.	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
The proposed changes will permit entities to protect electronic access control systems commensurate with the risk of those systems to the BES.	
Likes 0	
Dislikes 0	
Response	
Joel Charlebois - AESI - Acumen Engineered Solutions International Inc. - 5	
Answer	Yes
Document Name	
Comment	
We support the new definition of EACS, EAG, and CMS, so long as EACMS is retired. This concept allows for improved use of enterprise monitoring solutions which should lead to better risk mitigation. However, only applying the BCSI requirements to monitoring solutions may not sufficiently address the risk that a compromised monitoring solution could be used to mask additional attacks. This additional risk needs to be addressed appropriately.	
Likes 0	
Dislikes 0	
Response	
Paul Haase - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light	
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 ISO-NE NYISO NextERA Con-Ed and HQ	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lauren Price - ATCO Electric - 1 - MRO,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4, Group Name FirstEnergy Corporation	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Chantal Mazza - Hydro-Qu?bec TransEnergie - 2 - NPCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Don Schmit - Nebraska Public Power District - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Scott Downey - Peak Reliability - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	
Document Name	
Comment	
No comment at this time.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE suggests the current definitions and requirements are sufficient to protect virtual devices as virtual devices should be afforded the same protection as physical devices.	
Likes 0	

Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5	
Answer	
Document Name	
Comment	
No. Existing EACMS definition provides adequate security controls to access control systems and monitoring systems.	
Likes 0	
Dislikes 0	
Response	

23. Is your organization in support of Concept 3: Compliance Guidance? Please provide rationale to support your position.	
Joel Charlebois - AESI - Acumen Engineered Solutions International Inc. - 5	
Answer	No
Document Name	
Comment	
Relying on guidance allows for too much interpretation on behalf of the entities and may lead to an inconsistent level of security between entities. In addition, implementation guidance is just as the name suggest, guidance, and is meant to describe one or more methods of being compliant, but is not meant to be the only method to be compliant. An entity is free to choose an alternative implementation that is not described by implementation guidance, and wether or not that alternative implementation is compliant is still subject to interpretation. Adjusting the standards instead of just providing guidance should ensure correct and consistent interpretation of requirements across the industry, while providing entities with sufficient assurance that their methods of implementation are compliant.	
Likes 0	
Dislikes 0	
Response	
Janis Weddle - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Chelan PUD	
Answer	No
Document Name	
Comment	
The current CIP reliability standards as written are far too open to interpretation and not easily applied to new technologies, such as virtualization. New or modified CIP Standards surrounding virtualization will bring clarity and objective criteria to evaluate against such implementations.	
Likes 0	
Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3,5	
Answer	No
Document Name	
Comment	
No answer supports previous comment above.	

Likes 0	
Dislikes 0	
Response	
Brandon McCormick - Florida Municipal Power Agency - 3,4,5,6 - FRCC, Group Name FMPA	
Answer	No
Document Name	2016-02_Virtualization_Unofficial Comment Form_FMPA_comments.docx
Comment	
Please see attached comments	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	
N&ST considers Compliance Guidance on various topics an important and useful tool, and would support the creation and dissemination of guidance that addresses some of the myriad security and compliance issues that may be associated with the use of virtual technology. However, N&ST does not consider it an adequate substitute for modified CIP Standards that clarify the applicability of requirements to virtual environments.	
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	
The language of the standard should address the use of virtualization technologies. Compliance guidance is insufficient to address the issues that have been identified.	

Likes 0	
Dislikes 0	
Response	
Chantal Mazza - Hydro-Qu?bec TransEnergie - 2 - NPCC	
Answer	No
Document Name	
Comment	
No. Compliance Guidance would not be appropriate because it only shows one or more methods of compliance and not all. It also does not resolve the issues of high-water marking of impact levels and allow for the separation of monitoring from EACMS.	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
BPA strongly believes that standard language is necessary for all facets of virtualization. See response to question 20 above.	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	No
Document Name	
Comment	
APPA believes that the Compliance Guidance would not be appropriate because it only shows limited compliance. Moreover, it does not resolve the issues of high-water marking of impact levels and nor does it allow for the separation of monitoring from EACMS.	
Likes 0	

Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	No
Document Name	
Comment	
The SDT should explicitly address virtualization in the CIP Standard to provide clarity for securely separating CIP assets in virtualized environments.	
Likes 0	
Dislikes 0	
Response	
John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	No
Document Name	
Comment	
Tacoma Power supports comments submitted by APPA.	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
Duke Energy agrees that Compliance Guidance is helpful to industry for understanding and implementation, however, we request further clarification on whether industry stakeholders will be provided an opportunity to comment on any compliance guidance that is drafted, and ultimately approved by NERC.	
Likes 0	

Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	No
Document Name	
Comment	
The CIP Standards doesn’t currently allow mixed trust in the virtual environment. From our perspective, this will require changes to CIP Standards to help implement virtualization technologies and have a positive impact on the industry.	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	No
Document Name	
Comment	
Xcel Energy believes that further development of concepts and terms is needed before support can be given to any of the proposed options.	
Likes 0	
Dislikes 0	
Response	
Shelby Wade - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company	
Answer	No
Document Name	
Comment	
Even though the requirements today do not prohibit the use of virtualization, the Compliance Guidance and the current requirements discourages an entity from realizing the full potential of virtualization. Making the right changes to the requirements will allow entities the ability to fully utilize emerging technologies while supporting the reliable operations of the BES.	

Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	
Reclamation does not support the use of separate Compliance Guidance documents. Reclamation recommends that existing standards be revised with sufficient clarity to endure changing technologies and provide necessary guidance within the requirements and measures. Reclamation also recommends that adding new or appropriate industry-recognized definitions to the NERC Glossary of Terms will resolve industry concerns with the implementation of virtualization (refer to the recommended definitions section of the response to Question 24).	
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 ISO-NE NYISO NextERA Con-Ed and HQ	
Answer	No
Document Name	
Comment	
No. Compliance Guidance would not be appropriate because it only shows one or more methods of compliance and not all. It also does not resolve the issues of high-water marking of impact levels and allow for the separation of monitoring from EACMS.	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8,9 - WECC	
Answer	No
Document Name	
Comment	

SDG&E seeks resolution to comments posted regarding Concept 3 before it moves forward.	
Likes 0	
Dislikes 0	
Response	
Ronald Donahey - TECO - Tampa Electric Co. - 1,3,5,6	
Answer	No
Document Name	
Comment	
This could be resolved by improving the definition of Cyber Asset. Given that Compliance Guidance is for the auditors without input from industry, there would be no need for changes if no changes are made to the standards. Implementation Guidance on virtualization infrastructure would be beneficial.	
Likes 0	
Dislikes 0	
Response	
Paul Haase - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light	
Answer	No
Document Name	
Comment	
City Light supports the positions and comments of APPA and BPA.	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	No
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Richard Kinas - Orlando Utilities Commission - 3,5	
Answer	Yes
Document Name	
Comment	
This could be resolved by improving the definition of Cyber Asset. Given that Compliance Guidance is for the auditors without input from industry, there would be no need for changes if no changes are made to the standards. Implementation Guidance on virtualization infrastructure would be beneficial.	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Using Implementation Guidance, and CMEP Practice Guides if necessary, to clarify the permitted uses of virtual systems in a CIP environment should reduce an entity’s uncertainty about employing such systems.	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	Yes
Document Name	

Comment	
We support this compliance guidance since it explains what constitutes a programmable device.	
Likes 0	
Dislikes 0	
Response	
Bob Case - Black Hills Corporation - 1 - WECC	
Answer	Yes
Document Name	
Comment	
Having it defined is better than not having it detailed and explained.	
Likes 0	
Dislikes 0	
Response	
Robert Ganley - Long Island Power Authority - 1	
Answer	Yes
Document Name	
Comment	
More guidance affords greater understanding and clearer interpretations.	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	

See comments in response to Question No. 20.	
Likes 0	
Dislikes 0	
Response	
Don Schmit - Nebraska Public Power District - 1,3,5	
Answer	Yes
Document Name	
Comment	
The current standard is sufficient; there is no need to change it. We think that guidance helping entities better understand the intent of the standard and how to be compliant is good. Regional Entities have written Standard Application Guides to assist with this very issue.	
Likes 0	
Dislikes 0	
Response	
Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
More guidance affords greater understanding and clearer interpretations.	
Likes 0	
Dislikes 0	
Response	
Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - FRCC,MRO,WECC,Texas RE,SERC,SPP RE, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	

Given the current regulatory landscape and massive compliance challenges recently with evolving CIP Standards, Southern Company would be open to exploring, given the appropriate level of industry input and acceptance, ERO Enterprise-endorsed Compliance Guidance to address the proper implementation of virtualization. However, if pursued, Compliance Guidance should be accompanied by the changes to the Standards proposed in Concept 2 to differentiate controls based on the functionality and risk of current EACMS systems.	
Likes 0	
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
ERCOT asserts that ERO-endorsed implementation guidance would be the most appropriate means to address the various mean of implementing virtual technologies. See comments provided in response to question 20.	
Likes 0	
Dislikes 0	
Response	
Lauren Price - ATCO Electric - 1 - MRO,RF	
Answer	Yes
Document Name	
Comment	
ATC supports the concept of Compliance Guidance. That said, where the requirements are written in a prescriptive manner such that the guidance is at odds with the requirements, Registered Entities cannot leverage that guidance without risking non-compliance. This condition renders even the soundest guidance unusable. ATC could support ERO Enterprise-endorsed Compliance Guidance as an alternative if it were complimented by a paradigm shift to reshape the CIP Standards such that they are focused on technology agnostic security objectives and written with flexibility so Registered Entities are able to define and implement an adaptive risk-based cybersecurity program that timely detects, responds to, and mitigates emerging threats. ATC welcomes thought leadership on the subject of ERO Enterprise-endorsed Compliance Guidance as an alternative to mandatory regulations to position the industry for a more nimble, sustainable, and mature security posture. While there has been improvement in the requirement language as the CIP Standards have evolved, they continue to suffer because prescriptive mandatory regulations cannot keep pace with emerging technologies and the rapidly changing cybersecurity threat landscape. Until this paradigm shift occurs, the industry will continue to face the unintended consequences of the current construct, be distracted by the conundrum, divided between security and compliance, limited in our ability to leverage advances in technology, and will continue to be hindered by the antiquated ideals of a regulation that is chasing cybersecurity.	
Likes 0	
Dislikes 0	

Response	
Aaron Austin - AEP - 3,5	
Answer	Yes
Document Name	
Comment	
AEP believes Implementation (Compliance) guidance is important to provide industry, auditors and regulators sufficient insight into the concepts of virtualization and how the existing requirements are applicable in a virtual environment. We also agree that modifications are needed to the CIP standards along with additional compliance guidance.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE	
Answer	Yes
Document Name	
Comment	
Compliance guidance that informs “a way” for compliance has value. Guidance establishing compliance thresholds, bright-line requirements, incents entities to meet only the minimum compliance threshold and inhibits viewing compliance through a risk lens. The optimal guidance provides entities ideas and the flexibility to address identified risks.	
Likes 0	
Dislikes 0	
Response	
John Tolo - Unisource - Tucson Electric Power Co. - 1	
Answer	Yes
Document Name	
Comment	
With caveats listed in-section.	

Likes 0	
Dislikes 0	
Response	
Mark Riley - Associated Electric Cooperative, Inc. - 1,3,5,6, Group Name AECI & Member G&Ts	
Answer	Yes
Document Name	
Comment	
The current CIP standards can apply to a virtual environment. Some guidance and examples would assist Registered Entities in identifying a compliant approach when implementing virtualization technologies. More specifically, ERO Enterprise-endorsed Compliance Guidance could be used to address the implementation of virtualization.	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Francis - Midcontinent ISO, Inc. - 2,3 - MRO,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

sean erickson - Western Area Power Administration - 1,6	
Answer	Yes
Document Name	2016-02_Virtualization_Unofficial Comment Form_11022017.docx
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5	
Answer	
Document Name	
Comment	
Yes.	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	

Document Name	
Comment	
Texas RE suggests the current definitions and requirements are sufficient to protect virtual devices as virtual devices should be afforded the same protection as physical devices.	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	
Document Name	
Comment	
No comment at this time.	
Likes 0	
Dislikes 0	
Response	

24. If you have additional comments that you have not provided in response to the questions above, please provide them here.	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	
Document Name	
Comment	
No comment at this time.	
Likes 0	
Dislikes 0	
Response	
John Tolo - Unisource - Tucson Electric Power Co. - 1	
Answer	
Document Name	
Comment	
We are confused about VLANs. The current guidance has been to avoid VLANs, ostensibly over concerns that their “software-based nature” is somewhat insecure. We don’t disagree that they are “less secure” than physical LANs, however we believe they have a place within the environment to separate CIP and NON-CIP assets as they traverse into the firewall. This allows us a multi-instance network environment as opposed to dedicated network hardware for CIP. This confusion arises because software-derived separations for the server-side of multi-instance environments seems to be your specific intent. In summary, NSX to separate VMs is acceptable but VLANs to separate networks is not. That seems inconsistent to us. In fact, VLANs have well-known ways in which to secure them while products like NSX are much less well-known and proven. We would view VLANs as a good way to achieve the data plane and management plane separation, in conjunction with a firewall. We need to have efficiency of network equipment as well as server equipment.	
Likes 0	
Dislikes 0	
Response	
Ronald Donahey - TECO - Tampa Electric Co. - 1,3,5,6	
Answer	
Document Name	
Comment	
Suggest adding the following from the BCSI section:	

Co-location of BCSI on virtual multi-instance shared environment may be an issue. Are the same requirements applicable there as well?   SIEM tool (no requirement for ESP)

Likes 0

Dislikes 0

Response

Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE

Answer

Document Name

Comment

Reflected in our responses is a genuine concern that BES security is not well served by increasing complexity of implementation, operating practices, and compliance obligations. We are not advocating for a lesser security posture but a clear view of the law.

The concern arises from the nature and impact of the proposed revisions and new Standards and Glossary Terms, individually and in total.

If entities cannot understand the obligations, their ability to successfully operate the BES in a responsible, secure, and reliable manner are adversely impacted.

Entities have built their compliance programs and security posture incorporating the existing definitions. To revise programs will cost time and use resources with little associated benefit--redirecting resources from the very security activities on which they need to focus.

We would appreciate if the SDT would assist industry in understanding what security objective is trying to be fulfilled and to better leverage current Standards to minimize complexity, ensure clarity, and promote implementation flexibility.

Likes 0

Dislikes 0

Response

Aaron Austin - AEP - 3,5

Answer

Document Name

Comment

AEP believes the existing structure of CIP requirements and definitions is sufficient to permit entities to be compliant when using “virtualization” techniques. The proposed definition of Cyber Asset clarifies that the CIP requirements are applicable in a virtual environment.

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 ISO-NE NYISO NextERA Con-Ed and HQ

Answer

Document Name

Comment

There were no questions on the revision to the BCSI definition.

Is there a difference between the “data about” in the new BCSI definition and the “data in” that is part of the Cyber Asset Definition? Network traffic is neither about or in but in transit. Is network traffic considered BCSI? If not, the change in BCSI definition and the elimination of the EACMS term could cause the monitoring of this traffic to be out of CIP scope.

Likes 0

Dislikes 0

Response

Lauren Price - ATCO Electric - 1 - MRO,RF

Answer

Document Name

Comment

For our industry to maintain security and reliability, we need to break out of the mold of creating new or revised reliability standards that chase cybersecurity. Thought leadership is necessary to position the industry for a more nimble, sustainable, and mature security posture. The industry needs to recognize and accept a paradigm shift to reshape the CIP Standards such that they are written with flexibility and are focused on technology agnostic security objectives to incent Registered Entities to define and implement an adaptive, layered, risk-based cybersecurity program that timely detects, responds to, and mitigates emerging threats. While there has been improvement in the requirement language as the CIP Standards have evolved, they continue to suffer because prescriptive mandatory regulations cannot keep pace with emerging technologies and the rapidly changing cybersecurity threat landscape. Until this paradigm shift occurs, the industry will continue to face the unintended consequences of the current construct, be distracted by the conundrum where security and compliance are at odds, limited in our ability to leverage advances in technology, and will continue to be hindered by the antiquated ideals of a regulation that is chasing cybersecurity.

Likes 0

Dislikes 0

Response

Wendy Center - U.S. Bureau of Reclamation - 1,5

Answer	
Document Name	

Comment

Reclamation recommends the SDT consider the following:

Principles

The impact rating of a BES Cyber System is determined by its possible impact on the Bulk Electric System, not where it resides (Control Center or any other location) or how it is identified (virtual, non-virtual, hardware, software, etc.), and regardless of a Responsible Entity's functional registration. Following this principle, phrases such as "performing the functional obligations of" are unnecessary.

Instances created within a virtual environment must meet the requirements of the impact rating of that instance.

Hardware used in virtual environments must meet the physical security requirements for the impact rating of the highest rated instance or partition within the hardware.

Recommended Definitions

Reclamation recommends to revise the definition of BES Cyber System as follows:

BES Cyber System – One or more BES Cyber Assets logically grouped to perform one or more reliability tasks. A BES Cyber System may include, but is not limited to:

PCA*

PACS*

EACMS*

Intermediate Systems*

Electronic Access Control Systems: Cyber Assets that control electronic access to BES Cyber Systems.

Virtual Centralized Management System: A centralized system used to administer or configure virtual BES Cyber System(s) or virtual BES Cyber Asset(s).

Virtual Electronic Security Zone: A boundary housing one or more Virtual Machines logically separated from other BES Cyber Systems or other non-BES Cyber Systems using partitioned and isolated service set identifiers (SSIDs), virtual local area networks (VLANs), or other technologies.

Electronic Access Gateway: Cyber Assets (including Electronic Access Points) that control electronic access to and from virtual and non-virtual Electronic Security Perimeter(s).

*Currently defined in the NERC Glossary of Terms.

If the SDT adopts Reclamation's recommended terms and definitions, each term must be added to the NERC Glossary of Terms.

In addition to the recommended terms identified in responses to previous questions, Reclamation also recommends adding the following definition to the NERC Glossary of Terms:

BES Data – Configurations necessary for the operation and security (physical and logical) of the BES.

Rationale

Reclamation recommends virtualization be addressed from the top down, by changing the definition of BES Cyber System.

If each of the new recommended terms is properly described within the recommended revised BES Cyber System definition, the CIP-002 Attachment 1 Impact Rating Criteria will accurately determine the applicable requirements.

Implementation

Reclamation recommends the SDT provide a 24-month implementation plan timeline for entities to comply with the virtualization concepts.

Recommended Impact Rating Criteria

Reclamation recommends simplifying the Impact Rating Criteria using the methodology described below.

BES Cyber Systems are to be rated as high, medium, or low impact as follows:

1. A high impact BES Cyber System has one or more of the following characteristics:

    - Is used to operate transmission lines of 500kV or above
    - Supports a sum greater than 2500kV of transmission lines above 230kV
    - Supports generation with an aggregate capacity greater than 3000MW
    - Is identified as supporting an IROL or is necessary to avoid an Adverse Reliability Impact

2. A medium impact BES Cyber System has one or more of the following characteristics:

    - Supports generation with the aggregate capacity between 1500 – 3000MW
    - Supports a sum between 1500 – 2500kV of transmission lines above 230kV
    - Supports a RAS that could negatively affect an IROL or that can perform automatic Load shedding of 300MW or more

3. A low impact BES Cyber System has one or more of the following characteristics:

    - Supports a sum less than 1500kV of transmission lines above 230kV
    - Supports transmission only between 110 – 230kV
    - Supports generation with an aggregate capacity between 75 – 1500MW
    - Supports any single generator greater than 20MW not already identified as a Medium Impact BES Cyber System
    - Supports any Facilities that are designated a blackstart resource
    - Supports any other RAS not already identified as a medium impact BES Cyber System

Likes 0	
Dislikes 0	

Response

Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2

Answer	
Document Name	

Comment	
: ERCOT notes that all requirements regarding multi-instance are identified only for BCS. There is not information provided regarding multi-instance used for other asset categories like EACMS and PACS.	
Likes 0	
Dislikes 0	
Response	
Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - FRCC,MRO,WECC,Texas RE,SERC,SPP RE, Group Name Southern Company	
Answer	
Document Name	
Comment	
Ensure consistency in the use of terms, such as virtual, hypervisor, host, etc., and be cautious not to use terms that would lock an Entity into a single type of technology.	
Likes 0	
Dislikes 0	
Response	
Shelby Wade - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company	
Answer	
Document Name	
Comment	
The “instance” and “multi-instance” concept presented throughout the new requirements is not clear. If there is one physical box with multiple virtual Cyber Assets that are a part of the same BES Cyber System, is that considered “multi-instance” and all the new requirements apply or could this be considered one “instance” and be able to protect the entire physical box under the currently approved standards without the additional burdens? For example, an entity has one physical box that houses two virtual High Impact Cyber Assets, a virtual applications server and a virtual database server. Both virtual Cyber Assets are part of one High Impact BES Cyber System. Would the entity be able to protect that physical box as they would today or would they need to also apply the new requirements CIP-005 Part 1.5, Part 1.6, etc.? We believe that the risk associated with the example above is significantly lower compared to a “mixed-mode” environment (CIP/non-CIP or High Impact/EACMS). Additionally, for clarification, if an entity has on physical box that has a High Impact Cyber Asset “instance” and a Medium Impact BES Cyber Asset “instance”, could they continue to protect the physical box at the High Impact level without these additional new requirements? We fully support the concepts presented, but believe having clearer, approved NERC Glossary of Terms definitions of “instance” and “multi-instance” is necessary. Based on risk, the current CIP requirements provide sufficient protections when virtual CIP systems at the same Impact level reside on one physical box and that physical infrastructure is protected at the same level. Clearly stating that gives the entity the flexibility of no additional burden from	

the new requirements, but also allows “mixed-mode” environments. Please consider the following when constructing the definition of *multi-instance:* Virtual systems where the separate instances are a combination of CIP and non-CIP systems or the mixture of BES Cyber System Impact levels.	
Likes 0	
Dislikes 0	
Response	
David Francis - Midcontinent ISO, Inc. - 2,3 - MRO,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG	
Answer	
Document Name	
Comment	
See comments provided in response to each question under Concept 3. All requirements regarding multi-instance are identified only for BCS. There is not information provided regarding multi-instance used for EACMS.	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	
Document Name	
Comment	
Xcel Energy believes that storage virtualization is not adequately addressed above.	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	
Document Name	
Comment	

The SPP Standard Review Group agrees with the proposed change in the definition of “Cyber Asset”. However, as we reviewed the document, we noticed that the background information talked about addressing Virtualization, ironically, the proposed language doesn’t discuss or include the term. We would recommend that the drafting team revised the propose language to include the term “Virtualization” and the concepts around it. We feel that this would provide more clarity on what the drafting team’s intents are in reference to the virtualization process.

Additionally, we would suggest adding the management systems to the EACMS Definition instead of breaking them up separately. From our perspective, this provides more stability and reliability when talking about the security of the virtualization process.

Likes 0	
Dislikes 0	

Response

John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6

Answer	
Document Name	

Comment

The definition of Electronic Security Zone is challenging due to the fact that virtualization utilizes shared resources within the hypervisor. There can be shared memory space and shared physical network connections. So virtual machines that are within a shared hypervisor could potentially be sharing resources from non-BES assets. There are very few vendors that can truly create logical separation in a virtualized environment. To mitigate the security risk, any hardware used to host a BES cyber asset virtual machine, should be considered a part of the ESP. Hosting ESP and non-ESP assets on the same hardware introduces the opportunity for code injection into the hypervisor from less stringent environments. With that said, there are vendors that are able to isolate the resources utilized between VM’s of various classifications. One vendor capable of segmentation is Lynx Software Technologies. VMware and Microsoft HyperV are not among the vendors capable of this level of segmentation.

Tacoma Power recommends utilizing industry standards (e.g., NIST) for guidance on mandating policy. Due to the constantly changing nature of virtualization, the slow update process of CIP standards would limit entities from following industry best practices for virtualization security.

Tacoma Power recommends caution in mandating specific security requirements in a virtualized environment. An overarching policy would be far more effective in securing a virtualized environment.

Likes 0	
Dislikes 0	

Response

Jack Cashin - American Public Power Association - 4

Answer	
Document Name	

Comment

The existing NERC standards were not developed to consider the technology that currently exists or may be available in the future. In part, this contributes to more constant changes than the NERC standards process can potentially handle. Additionally, in the proposed BCSI definition, it is unclear what the term “pose a security threat” means.	
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	
Chantal Mazza - Hydro-Qu?bec TransEnergie - 2 - NPCC	
Answer	
Document Name	
Comment	
There were no questions on the revision to the BCSI definition. Can you provide information about the added value of “processed, organized, structured, or presented in a context” We think that this part could be removed.	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	

Document Name	
Comment	
(None)	
Likes 0	
Dislikes 0	
Response	
Don Schmit - Nebraska Public Power District - 1,3,5	
Answer	
Document Name	
Comment	
Use of virtualized environments within an ESP is fine, but we disagree with splitting the hypervisor between a control environment (OT) and a business environment. The hypervisor is based on software and it susceptible to zero day exploits and attacks. To be clear, each security zone should have a separate hypervisor (virtualized environment).	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	
Document Name	
Comment	
In consideration of each proposed requirement and definition, entities are asking not only does the idea make sense from a security perspective, but also, what evidence will need to be provided to show compliance with the requirement. The requirements proposed, in many cases, ask for an abstract set of objectives, intent, or principles, all of which may be challenging to demonstrate to an auditor. This should be avoided. Also, any requirement intended for a virtual environment should either be obviously applicable and adaptable to single use physical systems or explicitly exclude those systems from the scope of applicability. None of the proposed requirements consider the possibility of existing systems not being technically capable of meeting the requirement as written. Additionally, the proposed definition of BES Cyber System Information (BCSI) adds the terms “individual security logs,” which is unclear. Does this include single log entries? Further clarification needs to be provided on what is meant by “individual security logs.” The proposed definition of BCSI examples also adds “with network addresses” to network topologies. This implies that network diagrams without network addresses would not be considered BCSI. Is this the SDT’s intent?	
Likes 0	

Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3,5	
Answer	
Document Name	
Comment	
Cowlitz PUD strongly encourages the SDT to continue if efforts in developing standard requirements that support effective implementation of virtual environments with adequate protections.	
Likes 0	
Dislikes 0	
Response	
Janis Weddle - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Chelan PUD	
Answer	
Document Name	
Comment	
Please address storage in a multi-instance environment.	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	

Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	
Document Name	
Comment	
We have proposed the modified EACMS definition to include the management cyber system that can alter the configuration of BCS. Given that the EACMS have been well protected by the current CIP standards, all above requirements regarding CMS may not be necessary if our proposed modification to EACMS is used.	
Likes 0	
Dislikes 0	
Response	
Richard Kinas - Orlando Utilities Commission - 3,5	
Answer	
Document Name	
Comment	
Suggest adding the following from the BCSI section: Co-location of BCSI on virtual multi-instance shared environment may be an issue. Are the same requirements applicable there as well? SIEM tool (no requirement for ESP)	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	
Document Name	
Comment	
N/A	

Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5	
Answer	
Document Name	
Comment	
None.	
Likes 0	
Dislikes 0	
Response	

Comments received from Brandon McCormick – FMPA

1. Do you agree that the proposed change to the Cyber Asset definition makes it inclusive of both physical and virtual devices, including treatment of each virtual machine and hypervisor? If you do not agree, please provide rationale to support your position.

☐ Yes
☒ No

Comments: FMPA follows APPA's comments:

APPA does not agree that the proposed change is inclusive and believes that there is a better way to include both physical and virtual devices. Therefore, public power proposes the following:

> "Programmable electronic devices, including the hardware, software, and data in those devices.
> Virtualized systems or devices are distinct devices."

This proposed change would help in "future-proofing" the definition.

2. Do you agree that the term programmable in the Cyber Asset definition does not need further clarification at this time? If yes, please provide rationale to support your position.

   ☒ Yes
   □ No
   Comments:

3. If programmable does need further clarification, how would you prefer it to be addressed? Use comments to detail necessary definition changes or guidance that could be developed.

   Comments:

Centralized Management Systems (CMS)

As the SDT worked through issues related to virtual systems, it became clear that there was no straightforward way within the current CIP Standards to adequately address the risk of systems used to manage virtual environments. Management systems in virtual environments, through their consolidated interfaces and automation, can modify and delete entire infrastructures including virtual servers, networks, and storage. Given the broad capabilities of management systems in a virtual environment, they present specific and significant risk to the reliability of the BES Cyber Systems associated with those management systems.

The SDT considered several options to address the risks of management systems such as grouping management systems into the existing EACMS definition. This, however, would place these assets inappropriately in the EACMS category when they do not perform access control or access monitoring. Using the EACMS category in this manner creates a one-size-fits-all approach to requirements that does not consider the degree of risk or technical constraints posed by the particular system. For example, a system that only monitors and logs access does not pose the same level of risk as a management system for a large virtualized Control Center with the capability to modify or delete a complete infrastructure. Technical controls to mitigate the risk may differ depending on the capabilities of the management system. An electronic access monitoring system presents a risk of leaking BES Cyber System Information; an electronic access control system presents a risk of unauthorized access to, or modification of, a BES Cyber System's operational parameters; and a management system presents a risk of unwanted or unintended modification or deletion of a complete infrastructure. Proposed requirements related to this definition are detailed below.

The SDT determined a more appropriate option was to create a new definition for Centralized Management System (CMS) and apply appropriate and specific security requirements. The SDT seeks comment on the following conceptual definition of Centralized Management System in the Glossary of Terms Used in NERC Reliability Standards (NERC Glossary).

> **Centralized Management System (CMS):**
> A centralized system used for administration or configuration of BES Cyber System(s) through which the configuration of the BES Cyber System can be altered.

4. Do you agree with the proposed definition of Centralized Management Systems (CMS)? If not, please provide rationale to support your position.

☐ Yes
☒ No
Comments:

FMPA agrees with the concept of separating the management plane from the data plane. The definition as proposed should be revised to only include the administration of the BES Cyber System. The current definition may expand the scope to other tools with unintended consequences. Based on group discussions, we have concerns over what is meant by administration or configuration. There were different interpretations based on individual understanding. This should be resolved with a defined term that can be plugged in to the requirements and be implemented by industry.

Virtualization Terms and Requirements

The foundational pieces have now been set for the use of virtualization solutions. However, these solutions still pose risk. These risks and the nature of virtual systems may require some modifications to Standards. The concepts being proposed include additional access control and separation of the management plane from the data plane. This can help to prevent users of the applications on a virtualized system gaining access to the management system that can modify and delete the underlying infrastructure including virtual servers, networks, and storage.

The SDT uses the terms “instance” and “multi-instance” within the proposed requirements below. For the purposes of these proposed changes, the SDT intends for “instance” and “multi-instance” to be understood as:

- Instance: Discrete organizational environments with specific privileges or security levels, consisting of functions that consume resources from the shared infrastructure. Instances are logically isolated but physically interconnected.
- Multi-instance: An environment where a shared infrastructure provides containers for more than one instance.

In reviewing the risks that are unique and inherent to the use of virtualization technologies, the SDT identified the following risks:

1) Shared infrastructure,
2) Span of control, insider threats, and lateral privilege expansion,
3) Misconfiguration, excessive privileges, and capability of administrators, and
4) Escalation of privilege.

The SDT proposes the following definition and requirements in support of the use of virtual technologies.

Electronic Security Zone (ESZ)

The SDT contends that the Electronic Security Perimeter (ESP) definition does not accurately describe the proper isolation of virtual systems within shared infrastructure. Details of the analysis are captured in network isolation portion of the industry webinar presented on March 21, 2017. To address the concerns noted, the SDT seeks comment on the following conceptual definition of Electronic Security Zone (ESZ) in the Glossary of Terms Used in NERC Reliability Standards (NERC Glossary).

Electronic Security Zone:
The area defined by the logical separation of one or more Cyber Asset(s).

5. Do you agree that the proposed definition of ESZ more adequately applies to proper isolation of multi-instance environments, regardless of OSI layer? If not, please provide a rationale to support your position.

☐ Yes
☒ No
Comments:

FMPA is concerned that there is not enough clarity in the definition of ESZ to separate it from the ESP. ESZs seem to apply in different areas – sometimes they can encompass things like PACS/EACMs that might already fit under different requirements. This confusion of the term will lead to different interpretations and applications of the standard. What does sufficient mean in the "proper isolation of multi-instance environments"?

6. Do you agree that the proposed definition of ESZ would aid the development of future CIP Standards by providing a more relevant level of separation? If not, please provide a rationale to support your position.

☐ Yes
☒ No
Comments:

FMPA does not believe that the proposed definition for ESZ would provide the relevant level of separation needed. "Logical separation" is based on current technology and may not be applicable to future controls. VLANs have been a subject of contention in the past with NERC – are these now considered acceptable segregations/boundaries?

New Requirement CIP-005 Requirement 1, Part 1.6

The SDT proposes a new requirement part 1.6 for CIP-005 Requirement R1. This requirement part is for Responsible Entities to implement one or more Electronic Security Zones (ESZ) to meet the security objective of separating the management plane and the data plane of high and medium impact BES Cyber Systems in a multi-instance environment. Part 1.6 would also require Responsible Entities to implement one or more ESZs to meet the security objective of protecting the infrastructure associated with high and medium impact BES Cyber Systems in a multi-instance environment by limiting access to the Centralized Management Systems using a management plane ESZ.
Responsible Entities maintain the flexibility for grouping by cyber system function, by risk, by type of applicable security controls, or other logical groupings. The ESZ contains a distinct subset of the Responsible Entity's Cyber Assets. These are characterized as requiring (or benefiting from) similar security controls and separation from other distinct Cyber Assets. Properly implemented ESZs can limit damage and impact to availability to other surrounding ESZs, specifically by helping protect against span-of-control risks, insider threats, and lateral privilege expansion.
Again, the requirement would only be applicable to high and medium impact BES Cyber Systems residing in a multi-instance environment and their associated CMS.

Part 1.6:
Logically separate all Applicable Systems into defined groups of one or more Cyber Asset(s) to achieve the objective of mitigating the risks of span-of-control, insider threats, and lateral privilege expansion. At a minimum:
1. The management plane and the data plane of the applicable BES Cyber System shall be separated;
2. The CMS of the applicable BES Cyber System shall be separated from its data plane

7. Do you agree that the proposed CIP-005 Requirement R1, Part 1.6 provides sufficient security controls for the high and medium impact BES Cyber Systems residing in a multi-instance environment and their associated CMS to reduce the stated risks inherent to virtualization? If not, please provide a rationale to support your position.

   □ Yes
   ☒ No
   Comments:

   FMPA is concerned that neither minimum inclusions outlined in Part 1.6 deal with mitigation of span-of-control. In addition, not all vendor solutions may be able to address Part 1.6. The use of the word "achieve" in the draft standard sets a requirement that could be impossible to maintain as new risks emerge. This Requirement should also have the "per device capability" clause.

   We recommend changing it as follows:
   Logically separate all Applicable Systems, per device capability, into defined groups of one or more Cyber Asset(s) to address potential risks related to span-of-control, insider threats, and lateral privilege expansion.

New Requirement CIP-005 Requirement 1, Part 1.7

Similarly to CIP-005 Requirement R1, Part 1.3, the SDT proposes new requirement Part 1.7. Part 1.7 requires Responsible Entities to identify, control, and explicitly allow only necessary inbound and outbound communication between ESZs of high and medium impact BES Cyber Systems residing in a multi-instance environment. Part 1.7 would be added to CIP-005 to reduce the risks inherent to virtualization related to misconfiguration, excessive privileges, capability of administrators, as well as information protection and data leakage.

The requirement would be applicable to high and medium impact BES Cyber Systems residing in a multi-instance environment and their associated CMS(s).

Part 1.7:
Implement technical controls that enforce separation between ESZs by allowing only necessary inbound and outbound communication between the separated Cyber Asset(s) residing in a multi-instance environment.

8. Do you agree that the proposed CIP-005 Requirement R1, Part 1.7 provides a necessary security control to the high and medium impact BES Cyber Systems residing in a multi-instance environment and their associated CMS(s) to reduce risks inherent to virtualization? If not, please provide a rationale to support your position.

   □ Yes
   ☒ No
   Comments:

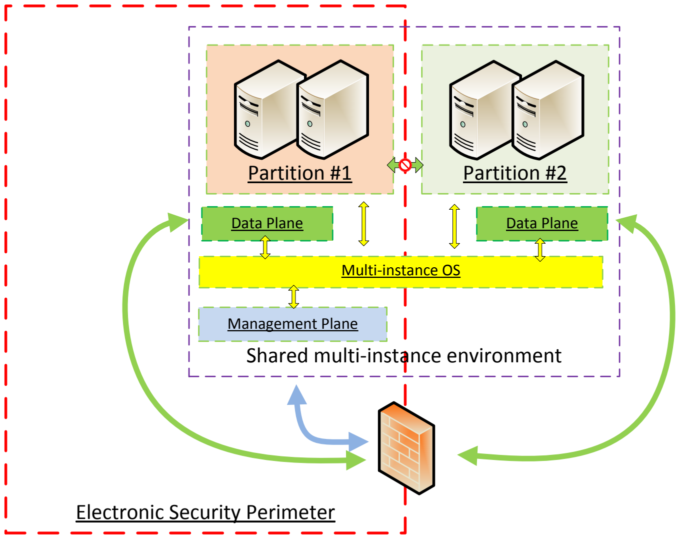
   FMPA recommends that the SDT consider the scoping on this requirement part. Would this be identified in the applicability table since it only applies to multi-instance? At the top of the standard/requirement? Or as shown within the requirement?   We recommend the SDT provide additional clarity on the ability to have technical controls for other layers (aside from the communication layer) and with shared memory space. We would also like the

SDT to consider the ramifications on the use of a cloud based SIEM vendor who is most likely using a virtualized environment. In the cloud environment, an entity would be transferring risk as well as trust

New Requirement CIP-005 Requirement 1, Part 1.8

Through the SDT work on virtualization, situations have been identified where a Responsible Entity may choose to share the same system infrastructure between applicable Cyber Assets and other programmable devices. As the footprint of cyber assets outside the scope of the CIP Standards in an organization might be significantly larger in size from the Cyber Assets in scope of the CIP Standard, a Responsible Entity may invest in its IT infrastructure with greater capability and more robust features. As presented in the third webinar on virtualization, this is particularly true with storage virtualization implementations. Under certain circumstances, leveraging enterprise infrastructure solutions will provide a better security posture for applicable Cyber Assets. Part 1.8 has been drafted with the objective of allowing such leverage as long as controls mitigating the additional risks are implemented.

A CIP Standard requiring the complete physical separation of applicable Cyber Assets and other programmable devices might adversely affect the overall security posture and reduce operational efficiency for the Responsible Entity through unnecessary expense and complexity of processes or technical implementation. Security controls exist to manage secure logical separation in multi-instance environments and there are operational benefits to sharing a common infrastructure as well. Technological advancements are often coupled with new security mechanisms which often benefit legacy infrastructure.



The diagram above shows an example of a shared multi-instance environment. The green arrows in the diagram represent the data communication. To exchange data between Partition 1 and 2, communication has to go through an EAP represented in the diagram by a firewall. The blue arrows in the diagram represent the management communication. In order to manage Partition 2, or any Cyber Asset hosted by the multi-instance environment and outside the ESP, IP communication to the management plane from outside the ESP has to go through the EAP since the management plan of shared multi-instance environment has to reside inside the ESP. The yellow arrows in the diagram represent the resource management activities performed by the multi-instance operating system necessary to ensure separation of data plane and management plane as well as partitions between Cyber Assets inside the ESP and Cyber Assets outside the ESP.

The SDT proposes CIP-005 Requirement 1, Part 1.8 to provide protection where the infrastructure used in a multi-instance environment is shared between applicable Cyber Assets and other programmable devices. This allows Responsible Entities to leverage the investments and protection of infrastructure shared between applicable Cyber Assets and other programmable devices. The requirement would be applicable to high and medium impact BES Cyber Systems residing in a multi-instance environment and their associated CMS(s).

Part 1.8:

When an infrastructure is shared between BES Cyber Systems and other Cyber Assets not part of a BES Cyber System:

1. The BES Cyber System, the management plane of the shared infrastructure, and any hosted Cyber Assets not part of a BES Cyber Systems shall all be separated; and
2. Communications between the BES Cyber System and any hosted Cyber Assets not part of a BES Cyber System shall all be denied by default

9. Do you agree that the proposed CIP-005 Requirement R1, Part 1.8 provides sufficient security control to reduce the risks associated with shared multi-instance environments? If not, please provide a rationale to support your position.

☐ Yes
☒ No
Comments:

There are discrepancies between the language in the Part 1.8 and in the question. Question identifies “shared multi-instance environments “ where the requirement does not. We recommend that the SDT provide guidance on what is infrastructure (possibly using language such as BES related infrastructure) and suggest that the SDT define “Multi-instance”.

If a Jump-host (a required security control for IRA for High BESCS) which is outside of the ESP, then requirement would not be applicable. If the Jump-host was on the VM infrastructure is this a multi-instance environment?

The word “infrastructure” is not defined in the proposed Standard. Consequently, the “infrastructure” on page 4 appears to only include virtual components. APPA questions if this would also include the UPS systems, equipment racks, HVAC systems, floors, lighting, etc.? The “management plane of the shared infrastructure” seems to limit and define “infrastructure” to be components only of the virtual environment.

New Requirement CIP-005 Requirement 3, Part 3.1

In reviewing the risks associated with communications in a virtual environment, the SDT identified a gap with remote access used to perform CMS functions. These communications using a CMS do not align appropriately to Interactive Remote Access. Tasks may be performed from outside the ESP that are a blend of interactive and automated tools, allowing for misinterpretation and unjustified relaxation of security mechanisms required for Interactive Remote Access. Using jump servers to perform CMS functions might not be the most effective or the most secure. Also, remote access to a Cyber Asset inside an ESP could benefit from other methods besides Interactive Remote Access for performing CMS functions.

CIP-005 Requirement R3, Part 3.1 allows for a new type of remote access to be used to perform CMS functions from outside of an ESP. Part 3.1 allows the CMS function to be performed outside an ESP using an access method other than an Intermediate Systems to fix the gap that may exist between

Interactive Remote Access and system-to-system communication. It does this by introducing requirements that are commensurate with the risk inherent to the management function in a multi-instance environment.

The SDT proposes new requirement CIP-005 Requirement 3, Part 3.1. Part 3.1 would be applicable to high and medium impact BES Cyber Systems.

> Part 3.1:
> Require authentication, integrity and non-repudiation controls for all sessions initiated outside of the ESZ, whether user initiated or system-to-systems communications, used to perform CMS functions.

10. The SDT asserts that the proposed CIP-005 Requirement 1, Part 3.1 provides additional security controls for remote access when performing CMS functions. These are necessary to reduce the risk associated with remote access to multi-instance environments. Do you agree with this assertion? If not, please provide a rationale to support your position.

☐ Yes
☒ No
Comments:

FMPA believes that this Requirement conflicts with the implied requirement identified in comments to question 8 that the management plane of the BCS must be inside the ESZ. APPA recommends replacing the proposed language with: “Require authentication, integrity and non-repudiation controls for all CMS functions, per device capability.”

If the suggested modification is not used, in the alternative FMPA proposes that this Requirement have the “per device capability” clause.

Encryption of network traffic from CMS to device could make compliance with this Requirement impossible to achieve.

11. Should the gap between Interactive Remote Access and system-to-system communication that was exposed by the examination of the risks inherent to virtualization be addressed for systems other than high and medium impact BES Cyber Systems residing in a multi-instance environment and their associated CMS? If not, please provide a rationale to support your position.

☐ Yes
☒ No
Comments:

The NERC standards should be written to address the known risks and not limited to risks associated with managing multi-instance environments.

New Requirement CIP-004 Requirement 4, Part 4.5

The SDT has identified “too much privilege” as an inherent risk in virtualization. This risk can be reduced by adding controls in CIP-004. Limiting of the privileges granted to the minimum necessary is only present in the guidance. It is not a requirement. This security risk can be mitigated, however, by implementation of least privilege access and separation of duties in the requirement language. This means fewer people get high level privileges, and no single individual gets privileges that are too broad. For efficiency, it can be implemented via role-based access control (RBAC), which requires an initial effort to define roles properly. But also provides an opportunity for internal review of the span-of-control risk. Role-based access control and separation of duties are both available in virtual environments. Implementation of RBAC varies by vendor but is generically the same in principle.

The SDT proposes new requirement CIP-004 Requirement 4, Part 4.5. Part 4.5 would be applicable to high and medium impact BES Cyber Systems.

Part 4.5:
The Responsible Entity shall document and implement process(es), except under CIP Exceptional Circumstances, to authorize electronic and unescorted physical access to BES Cyber Systems and BES Cyber Systems Information that implements the principles of need-to-know, least privilege, and separation of duties as determined by the Responsible Entity, as per system capability.

12. The SDT asserts that the new proposed CIP-004 Requirement R4, Part 4.5, provides additional security control to the electronic and unescorted physical access to multi-instance environment processes which reduces the "too much privilege" risk inherent to virtualization which has been identified. Do you agree with this assertion? If not, please provide a rationale to support your position.

□ Yes
☒ No
Comments:

FMPA recommends that this become Requirement 4 Part 4.2 as the Authorization takes place in 4.1; implementation should become 4.2; then the quarterly review is 4.3, etc. FMPA recommends guidance to small entities that they may identify each role but may need to (resource constrained) add the same person to each role

Concept 2: Modifications to the EACMS definition

As noted above, the SDT reviewed the scope of the current definition, the requirements, and risk of the types of assets contained within EACMS. The current construct does not differentiate controls based on the functionality and risk of the system. The current construct does, however, create what is known as the "hall of mirrors" effect. Specifically, there may be some types of EACMS that should be required to be inside an ESP and behind a firewall. An example could be the management system of a firewall that is categorized in such a way that it must reside within an ESP. That requirement, however, cannot exist for all EACMS because a firewall is itself an EACMS. Without defining a new category, the result would be that every EACMS would need to be inside an ESP and therefore protected by another EACMS. This creates the recursive "hall of mirrors" effect.

There are a number of systems that both monitor and provide part of the solution of controlling access, but do not actually control traffic at the point of entry. These devices or systems may or may not benefit from being inside a protected boundary, or they may form part of the strategy that protects BES Cyber Assets. The technical means of implementing some multi-part systems may require components to be outside, or span the ESP.

To address this, the SDT proposes breaking up the EACMS categorization of applicable systems by function so that the appropriate requirements for each can be applied. The SDT does not, however, want to create a reclassification and documentation exercise for Responsible Entities who would not see benefit and would try to create a way for those Responsible Entities to continue to use EACMS with no changes. There are also other options in addition to these two.

Electronic Access Control System (EACS)

The SDT seeks comment on the following conceptual definition of Electronic Access Control System in the Glossary of Terms Used in NERC Reliability Standards (NERC Glossary).

Electronic Access Control System (EACS):

Cyber Assets that perform electronic access control of the BES Cyber Systems. This includes Intermediate Systems.

An Electronic Access Control System performs authentication and authorization of traffic or users. This is the "gatekeeper" function or the classic authentication and authorization functions of standard AAA. In many cases these systems do not perform any active filtering of the traffic passing through any particular interface. The primary duty of EACS is to authenticate and authorize. EACS move beyond the risk of unauthorized access to meta-information about an environment, to unauthorized access to BES Cyber Systems and modification of their operational parameters.

Electronic Access Gateway (EAG)

The SDT seeks comment on the following conceptual definition of Electronic Access Gateway in the Glossary of Terms Used in NERC Reliability Standards (NERC Glossary).

Electronic Access Gateway:
Cyber Assets that perform electronic access control of the Electronic Security Perimeter(s). The Electronic Access Gateway also hosts the EAP(s).

An Electronic Access Gateway hosts the EAP and performs the active function of filtering or forwarding traffic at the demarcation point (boundary protection). Primarily, these are firewalls and routers that perform gateway functions at the layer 3 ESP boundary demarcation point.

Electronic Access Monitoring Systems

As technologies and cyber attacks advance and become more complex, Responsible Entities are becoming increasingly interested in collecting and correlating electronic access monitoring events across their enterprises. This broad-based information collection provides Responsible Entities with more visibility into emerging threats and trends. Responsible Entities can then analyze and share this information more readily and take action to improve the overall cybersecurity and reliability of the BES through early detection of compromise.

Under the currently effective CIP Reliability Standards, if a Responsible Entity uses enterprise wide electronic access monitoring tools, the Cyber Assets used to perform the monitoring may meet the definition of EACMS and become subject to the CIP Reliability Standards applicable to EACMS. This may discourage or prevent Responsible Entities from using enterprise wide electronic access monitoring due to the device level requirements of an EACMS. Responsible Entities may be discouraged from providing and correlating security events across enterprise and control networks, even though cyber-attacks against control systems could enter through business networks. The SDT concludes there is value in correlating security events across both control and enterprise networks.

The SDT proposes that the information within the electronic access monitoring systems should be protected as a BCSI repository, rather than having the system categorized as an EACMS. The systems performing electronic access monitoring are used to monitor and collect information about BES Cyber Systems or Electronic Security Perimeter(s) and pose a risk of information leakage. These monitoring systems are not used to control access to the BES Cyber Systems or Electronic Security Perimeter(s). The monitoring function has been in scope of the EACMS definition due to the sensitivity of certain information that may be collected. The proposed change is to treat the data collected through the monitoring capability as BCSI rather than having the monitoring systems categorized as EACMS. This change will enable Responsible Entities to better leverage enterprise-wide monitoring to improve overall situational awareness, and in the process more proactively address security events.

This will result in improved security and reliability. This does not change a Responsible Entity's obligations to monitor under CIP-007 R4.

To transition electronic access monitoring from EACMS to BCSI, the SDT seeks comment on the following conceptual modification to the definition of BES Cyber System Information in the Glossary of Terms Used in NERC Reliability Standards (NERC Glossary).

Clean:

BES Cyber System Information:

Data about the BES Cyber System that is processed, organized, structured, or presented in a context that could be used to gain unauthorized access or pose a security threat to the BES Cyber System.

BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to gain unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual or collections of IP addresses without context of location and purpose, ESP names, individual security logs, or policy statements.

Examples of BES Cyber System Information may include, but are not limited to: security procedures, collections of security logs, or security configuration information about BES Cyber Systems, Physical Access Control Systems, Electronic Access Control Systems, Electronic Access Gateway Systems, Centralized Management Systems, and Electronic Access Control or Monitoring Systems that are not publicly available; and network topology with network addresses of the BES Cyber System.

Redline:

BES Cyber System Information:

Data ~~Information~~ about the BES Cyber System that is processed, organized, structured, or presented in a context could be used to gain unauthorized access or pose a security threat to the BES Cyber System.

BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual or collections of IP addresses without context of location and purpose, ESP names, individual security logs, or policy statements.

Examples of BES Cyber System Information may include, but are not limited to:~~,~~ security procedures, collections of security logs, or security configuration information about BES Cyber Systems, Physical Access Control Systems, Electronic Access Control Systems, Electronic Access Gateway Systems, Centralized Management Systems, and Electronic Access Control or Monitoring Systems that is not publicly available ~~and could be used to allow unauthorized access or unauthorized distribution~~; ~~collections of network addresses~~; and network topology with network addresses of the BES Cyber System.

Current:

BES Cyber System Information:

Information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context, ESP names, or policy statements. Examples of BES Cyber System Information may include, but are not limited to, security procedures or security information about BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber System.

Proposed Requirements Related to EACMS Changes

Based on the concepts presented above, the table below lists the current requirement scope of EACMS and those proposed for CMS, EACS, and EAG. In the table below, the "X" indicates where the requirement currently applies to the system category in the Applicable Systems column of CIP Standards. The "+" sign indicates an additional requirements being considered to address risk for that specific system category in the Applicable Systems column of CIP Standards. To the extent that there is no difference in requirement applicability, the SDT would look to consolidate the terms into as few classifications as necessary.

Please keep in mind that the SDT does not want to create a reclassification and documentation exercise for Responsible Entities who would not see sufficient benefit and would look to create a way for those Responsible Entities to continue to use EACMS with no changes.

Requirement	EACMS	CMS (+)	EACS (+)	EAG (+)
CIP-004 R1.x		+	+	+
CIP-004 R2.x	X	X	X	X
CIP-004 R3.x	X	X	X	X
CIP-004 R4.x	X	X	X	X
CIP-004 R5.x	X	X	X	X
CIP-005 R1.x		+	+	X (Part 1.5)
CIP-005 R2.x		+		
CIP-005 R3		+		
CIP-007 R1.1	X	X	X	X
CIP-007 R2.x	X	X	X	X
CIP-007 R3.x	X	X	X	X
CIP-007 R4.x	X	X	X	X
CIP-007 R5.x	X	X	X	X
CIP-009 R1.x	X		X	X
CIP-009 R2.1	X		X	X
CIP-009 R2.2	X		X	X
CIP-009 R2.3			+	+
CIP-009 R3.x	X		X	X
CIP-010 R1.x	X	X	X	X

Requirement	EACMS	CMS (+)	EACS (+)	EAG (+)
CIP-010 R2.x	X	X	X	X
CIP-010 R3.1	X	X	X	X
CIP-010 R3.2		X	+	+
CIP-010 R3.3	X	X	X	X
CIP-010 R3.4	X	X	X	X
CIP-010 R3.5	X	X	X	X
CIP-011 R1.x	X	X	X	X
CIP-011 R2.x	X	X	X	X

13. Do you agree with the SDT's assertion that the definition of EACMS is too broad and does not differentiate the capabilities and risk(s) of the systems that fall within that definition scope? If not, please provide rationale to support your position.

☒ Yes
☐ No
Comments:

14. Do you agree that the language of the proposed definitions of EACS provides better consistency and clarity to the CIP Standards? If not, please provide rationale to support your position and alternative language.

☐ Yes
☒ No
Comments: FMPA agrees that the language provides more clarity. However, we are concerned that the change includes intermediate systems, which cannot be inside of the ESP.

15. Do you agree that the language of the proposed definitions of EAG provides better consistency and clarity to the CIP Standards? If not, please provide rationale to support your position and alternative language.

☐ Yes
☒ No
Comments: We agree that the proposed definitions of EAG provides better consistency and clarity; however, the SDT used EAG Systems in the example for the changes to the BCSI definition. Should this be EAG or EAGS?

The SDT used EAG Systems in the example for the changes to the BCSI definition. FMPA is unsure if this should be EAG or EAGS.

16. Do you agree that the current compliance requirements related to EACMS monitoring systems are precluding or discouraging solutions that could reduce risk to security and reliability? Please provide your rationale in support or against this assertion.

☒ Yes
☐ No
Comments:

Yes. The existing standards would make it difficult or potentially impossible to be compliant and use services like Dell Secureworks.

17. Should the security requirements for the access control portion of the EACMS to be different from the monitoring portion of the EACMS? If you do, please provide your rationale.

☒ Yes
☐ No
Comments:

The security controls for monitoring need to be flexible. This is because the BES cannot be negatively impacted solely by a compromise of a monitoring system.

18. Should CIP-011 Requirement R2 scope be expanded to include designated storage locations for access monitoring systems? If not, please provide rationale to support your position.

☐ Yes
☒ No
Comments:

BCSI outside the entities environment should be dealt with in the CIP standards apart from the existing Requirement R2.

19. Do you agree with assignment of CIP Standard requirements to each of the EACS, EAG, and CMS categories as presented in the table above? If not, please provide rationale to support your position.

☒ Yes
☐ No
Comments:

Concept 3: Compliance Guidance

The SDT has explored the idea that no changes are necessary to the CIP Standards to address virtualization. ERO Enterprise-endorsed Compliance Guidance could be used to address many industry concerns with the proper implementation of virtualization.

20. As the standards today do not prohibit the use of virtualization technologies, do you support an approach where no changes are made to the CIP Standards in response to the virtualization issue identified by the V5 TAG? Please provide a rationale to support your position.

☐ Yes
☒ No
Comments:

The current CIP standards do not explicitly prohibit all types of virtualization but require “high water marking” of the impact level even where this is not the most secure and reliable control. For example, the separation of data plane and management plane between hypervisor and guest is a more effective control than applying rigorous CIP Requirements and keeping hypervisors inside the same security zone.

Also, CIP Requirements do not separate the electronic access controls from the electronic access monitoring to allow for different requirements when only monitoring is done. This has a high risk of misallocating scarce resources (money, time, manpower) that could be more effectively applied elsewhere for increased reliability.

Compliance guidance is written to show one or more compliant solutions to clarify and help in applying the Requirements. Such guidance does not supersede standard requirements language. Moreover, such guidance cannot show all possible solutions and is specific and limited, rather than a framework where one can generate new and unique solutions. Solutions currently known to the SDT are only a snapshot in time that may become obsolete at any moment due to technical innovation or changes in the threat environment, while security objectives are more enduring than requirements for a specific solution. Entities may be aware of, or devise a solution unknown to the SDT that provides equal or greater security, that the Requirements language finds the solution non-compliant. Therefore, the proposed standard must emphasize security objectives that allow entities to demonstrate and explain how solutions meets the objective.

Summary

The SDT has provided very diverse concepts for your consideration. Each of these concepts can be moved forward in the drafting process independently. Please provide your responses to each of the questions below.

21. Is your organization in support of Concept 1: Modifications to allow use of secure multi-instance? Please provide rationale to support your position.

□ Yes
☒ No
Comments:

We would support Concept 1: Modifications to allow use of secure multi-instance provided that comments herein are taken into consideration.

22. Is your organization in support of Concept 2: Modifications to the EACMS definition? Please provide rationale to support your position.

□ Yes
☒ No
Comments:

We would support Concept 2: Modifications to the EACMS definition provided that comments herein are taken into consideration.

23. Is your organization in support of Concept 3: Compliance Guidance? Please provide rationale to support your position.

□ Yes
☒ No
Comments:

FMPA believes that the Compliance Guidance would not be appropriate because it only shows limited compliance. Moreover, it does not resolve the issues of high-water marking of impact levels and nor does it allow for the separation of monitoring from EACMS.

24. If you have additional comments that you have not provided in response to the questions above, please provide them here.

Comments:

The existing NERC standards were not developed to consider the technology that currently exists or may be available in the future. In part, this contributes to more constant changes than the NERC standards process can potentially handle.

Additionally, in the proposed BCSI definition, it is unclear what the term “pose a security threat” means.