Comment Report

Project Name:	2016-02 Modifications to CIP Standards | Virtualization
Comment Period Start Date:	3/14/2017
Comment Period End Date:	4/11/2017
Associated Ballots:	

There were 54 sets of responses, including comments from approximately 136 different people from approximately 89 companies representing 10 of the Industry Segments as shown in the table on the following pages.

Questions

1. Version 5 introduced the BES Cyber System concept, and requirements reference applicability at the *BES Cyber System* level. However, language in the measures shows that, implicitly, many controls are expected to be implemented at the *BES Cyber Asset* or *device* level. The SDT assumes that most auditors expect entities to demonstrate compliance at the device level. Do you agree with the SDT's assumption? If so, how should the SDT address these inconsistencies?

(Refer to the Unofficial Comment Form for more information on this question)

2. The SDT proposes that each virtual machine and hypervisor are separate Cyber Assets. Do you agree with this position? Please provide a rationale to support your position.

(Refer to the Unofficial Comment Form for more information on this question)

3. Do you agree that the proposed Cyber Asset definition clarifies the term *programmable*? Please provide a rationale to support your position.

(Refer to the Unofficial Comment Form for more information on this question)

4. In virtualized environments, the physical infrastructure can be shared between BES Cyber Systems and other non-CIP Cyber Assets while maintaining isolated virtualized environments for each.

Such configurations are not addressed explicitly in CIP-005-5. Are modifications required to address the issue? Please provide your rationale.

5. The SDT asserts that VLANs providing logical isolation are not addressed explicitly in CIP-005-5, and controls may be necessary to isolate BES Cyber Systems. Are the current requirements of CIP-005-5 sufficient to address logical isolation using VLANs? Please provide your rationale.

(Refer to the Unofficial Comment Form for more information on this question)

6. Do you agree with the proposed definition of CMS? If not, please provide alternative language for the definition and your rationale.

(Refer to the Unofficial Comment Form for more information on this question)

7. Do you agree with the SDT's approach to reference the CMS specifically as a type of applicable system in the CIP standards? Please provide your rationale.

(Refer to the Unofficial Comment Form for more information on this question)

8. Do you agree with the SDT's approach to require the isolation between the data plane and the management plane? Please provide your rationale.

(Refer to the Unofficial Comment Form for more information on this question)

9. Do you agree with limiting the applicability to high and medium impact Control Centers? Please provide your rationale.

(Refer to the Unofficial Comment Form for more information on this question)

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		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
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	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
Seattle City Light	Ginette Lacasse	1,3,4,5,6	WECC	Seattle City Light Ballot Body	Pawel Krupa	Seattle City Light	1	WECC
					Hao Li	Seattle City Light	4	WECC
					Bud (Charles) Freeman	Seattle City Light	6	WECC
					Mike Haynes	Seattle City Light	5	WECC
					Michael Watkins	Seattle City Light	1,4	WECC
					Faz Kasraie	Seattle City Light	5	WECC
					John Clark	Seattle City Light	6	WECC
					Tuan Tran	Seattle City Light	3	WECC
					Laurrie Hammack	Seattle City Light	3	WECC
Entergy	Julie Hall	6		Entergy/NERC Compliance	Oliver Burke	Entergy - Entergy Services, Inc.	1	SERC
					Jaclyn Massey	Entergy - Entergy Services, Inc.	5	SERC
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
BC Hydro and Power Authority	Patricia Robertson	1,3,5		BC Hydro	Patricia Robertson	BC Hydro and Power Authority	1	WECC
					Venkataramakrishnan Vinnakota	BC Hydro and Power Authority	2	WECC
					Pat G. Harrington	BC Hydro and Power Authority	3	WECC

					Clement Ma	BC Hydro and Power Authority	5	WECC
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	RSC no Dominion and ISO-NE	Paul Malozewski	Hydro One.	1	NPCC
					Guy Zito	Northeast Power Coordinating Council	NA - Not Applicable	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
					Sylvain Clermont	Hydro Quebec	1	NPCC
					Si Truc Phan	Hydro Quebec	2	NPCC
					Helen Lainis	IESO	2	NPCC
					Laura Mcleod	NB Power	1	NPCC
					MIchael Forte	Con Edison	1	NPCC
					Kelly Silver	Con Edison	3	NPCC
					Peter Yost	Con Edison	4	NPCC
					Brian O'Boyle	Con Edison	5	NPCC
					Greg Campoli	NY-ISO	2	NPCC
					Michael Schiavone	National Grid	1	NPCC
					Michael Jones	National Grid	3	NPCC
					David Ramkalawan	Ontario Power Generation Inc.	5	NPCC

					Quintin Lee	Eversource Energy	1	NPCC
					Silvia Mitchell	NextEra Energy - Florida Power and Light Co.	6	NPCC
Dominion - Dominion Resources, Inc.	Sean Bodkin	3,5,6		Dominion	Connie Lowe	Dominion - Dominion Resources, Inc.	3	NA - Not Applicable
					Lou Oberski	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
					Larry Nash	Dominion - Dominion Virginia Power	1	NA - Not Applicable
Southwest Power Pool, Inc. (RTO)	Shannon Mickens	2	SPP RE	SPP Standards Review Group	Shannon Mickens	Southwest Power Pool Inc.	2	SPP RE
					Steven Keller	Southwest Power Pool Inc.	2	SPP RE
					John Allen	City Utilities of Springfield, Missouri	4	SPP RE
PSEG	Sheranee Nedd	1,3,5,6	NPCC,RF	PSEG REs	Tim Kucey	PSEG - PSEG Fossil LLC	5	RF
					Karla Jara	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
AEP	Warren Cross	1,3,4,5	MRO,RF,SERC,SPP RE,Texas RE,WECC	ACES Standards Collaborators	Prairie Power, Inc.	PPI	1,3	SERC
					Arizona Electric Power Cooperative, Inc.	AEPC	1	WECC
					Hoosier Energy Rural Electric Cooperative, Inc.	HE	1	RF
					Sunflower Electric Power Corporation	SEPC	1	SPP RE
					Great River Energy	GRE	1,3,5,6	MRO
					North Carolina Electric Membership Corporation	NCEMC	3,4,5	SERC

					Rayburn Country Electric Cooperative	RCEC	3	SPP RE
					Buckeye Power, Inc.	BUCK	4	RF
					Southern Maryland Electric Cooperative	SMECO	3	RF
					Wabash Valley Power Association	WVPA	3	SERC

1. Version 5 introduced the BES Cyber System concept, and requirements reference applicability at the *BES Cyber System* level. However, language in the measures shows that, implicitly, many controls are expected to be implemented at the *BES Cyber Asset* or *device* level. The SDT assumes that most auditors expect entities to demonstrate compliance at the device level. Do you agree with the SDT's assumption? If so, how should the SDT address these inconsistencies?

(Refer to the Unofficial Comment Form for more information on this question)

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

Answer	No
Document Name	

Comment

CenterPoint Energy does not agree with the SDT's assumption about the expectation of auditors and believes each entity should have the flexibility to defend compliance decisions based on the requirement language in the CIP Standards. Entities may find some controls easier or more effective to implement and provide evidence at a BES Cyber System level rather than at the BES Cyber Asset or device level, or vice versa depending on the requirement and the current CIP Standards provide this option.

Likes 0	
Dislikes 0	

Response

Scott Downey - Peak Reliability - 1

Answer	No
Document Name	

Comment

For some of the standards, like anti-virus/malware protection, a holistic approach can yield a design that protects assets without being draconian regarding the installation of anti-virus/malware protective software on every individual asset. Peak suggest the SDT consider real-world scenarios for situations and decide, for each standard, which ones can be addressed on an individual-asset basis only, and which ones can be addressed at the BES Cyber System level.

Likes 0	
Dislikes 0	

Response

Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance

Answer	No

Document Name	

Comment

Entergy understands that entities must be able to prove that each device that is part of a BES Cyber System need to be evaluated for compliance, but expect the distinction to be that controls do not have to be implemented at the individual device level provided evidence can prove the they benefit from controls implemented at the BES Cyber System level. For example, depending on the architecture every device may benefit from Intrusion Prevention Systems (IPS) with deep packet inspection for malware prevention, but that does not mean IPS is running on each individual device.

To incorporate virtualization and address the V5TAG transfer issue to clarify the meaning of the term *programmable* in the current definition of *Cyber Assets*, the SDT is proposing changes to the definition that include defining the term in the singular rather than the plural. Updating the definition to include virtual environments allows the definition of other terms based on *Cyber Asset*, such as Electronic Access Control or Monitoring Systems (EACMS) and Protected Cyber Asset (PCA) to also include virtual environments.

The proposed *Cyber Asset* definition is:

An electronic device (physical or virtual) whose operation is controlled by a stored program that can be changed or replaced by the end user, including the hardware, software, and data in the device. A virtual machine is itself a distinct asset from its host(s).

Likes 0	
Dislikes 0	

Response

Steven Rueckert - Western Electricity Coordinating Council - 10

Answer	Yes
Document Name	

Comment

The SDT should consider removing or further clarifying the purpose of including language (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) [see CIP-007-6, Part 4.1]. Additionally, the SDT could consider adding in the Appplicable Systems language, ‘and their associated BES Cyber Systems:’ if the intent of CIP v5 was to leverage a system-centric approach to affording the required controls for all Cyber Assets.

This may require the same change in the purpose statement found in all CIP Reliability Standards:

‘To identify and categorize BES Cyber Systems and their associated BES Cyber Assets…’

The SDT may want to reconsider the following cyber system concept paper –

http://www.nerc.com/docs/standards/sar/Concept_Paper_Categorizing_Cyber_Systems_2009July21.pdf

Likes 0	
Dislikes 0	

Response

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	

It has been BPA's experience that guidance provided to auditors leads them to expect and look for controls to be applied to the Cyber Asset. Also, they seem skeptical of implementations where a given device performs a portion of the control function and additional components of the security strategy are implemented across multiple devices on the network. Auditors might consider only the device portion of an overall control and evaluate it outside of the network-based defense-in-depth strategy.

One way to address this inconsistency would be to normalize the use of the term "system" across the example measures rather than "device" wherever applicable. The SDT should add Guidance in the Technical Basis sections to clarify that defense in depth strategies are desirable. The Electronic Access Control and Monitoring System (EACMS) paradigm should be revised in line with standard IT Security practice and terminology as performing Authentication, Authorization, and Accounting (AAA). It is also important to explicitly allow for distributed systems to perform this AAA function for a security zone rather than the legacy concept of hardened perimeter.

There may also be a need to revisit the Reliability Standards Audit Worksheets in light of system vs device to provide better guidance to auditors attempting to apply the questions in the RSAW to an entity's evidence.

Likes 0	
Dislikes 0	
Response	

Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	

Dominion agrees with the statement that it appears auditors are expecting entities to show compliance at the device level for CIP v5 standards. However, the standard clearly allows compliance to be demonstrated at the system level. If the applicability of the controls is at the system level, then controls can be at the system level OR at the device level (where each device in the system has appropriate controls). If the applicability of the standards is intended to be at the BCA level, the applicability column clearly state that the expectation is for monitoring to occur at that level. To reinforce the applicability at the system level, the SDT should include specific system examples in the Measures section and similar system examples in the GTB or an Implementation Guidance document.

Likes 0	
Dislikes 0	
Response	

Chris Scanlon - Exelon - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Exelon agrees with the assumption that the current expectation from auditors is to see compliance demonstrated at the BCA or device level. We view this as a concern that should be addressed, and we would welcome more clarity in the guidance on when device level compliance is required versus when protections can be demonstrated at the BES Cyber System level. In the meantime, Exelon does continue to demonstrate compliance down to the BCA and device level, including all individual logical or virtual machines as well as their VM Host machine(s).	
Likes 0	
Dislikes 0	
Response	

Preston Walker - PJM Interconnection, L.L.C. - 2 - SERC,RF	
Answer	Yes
Document Name	
Comment	
It was PJM's experience during our version 5 audit that auditors did expect many controls were implemented at the device level. We found this was expected more for requirements that contained prescriptive language. Objective based controls lend themselves more to implementing controls at the BES Cyber System level. In order to help clarify how to handle the requirements for systems vs individual assets, additional guidance with respect to virtualization for both scenarios may be helpful.	
Likes 0	
Dislikes 0	
Response	

Mike Smith - Consultant - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
I concur with the suggested edits. As long as this new definition is updated and incorporated throughout the CIP standards, we believe this would address any inconsistencies as to device level auditing.	
Likes 0	

Dislikes 0	

Response

Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	

Comment
SRP agrees there are inconsistencies between the language of the requirement and the measures regarding applicability of the requirements at the BES Cyber System level. It has been our experience that in some instances auditors looked at the device level instead of evaluating the controls applied at the system level. SRP utilizes a Defense in Depth security architecture, which applies controls and additional security measures across multiple devices on the network. SRP suggests the SDT add discussion of this strategy in the guidelines and technical basis section.

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	

Comment
Yes – SMUD Agrees. Virtualization is a proven secure method for sharing physical resources, and should be incorporated as an acceptable technology for network, firewall, compute (virtual machines), and storage. The acceptance for each of the areas should be outlined such that auditors and utility companies fully understand the acceptable configurations. At a minimum, the “device level” term should be changed to “operating system” as it is inclusive for processes, data, authentication, configuration, and traffic forwarding. This “operating system” could serve as the basis for all fully virtualized functions including virtual machines, virtual routers, virtual firewalls, etc. For systems that provide services with a shared “operating system”, such as a router with multiple isolated routing tables (VRF), guidelines should summarize the constraints.

Likes 0	
Dislikes 0	

Response

Nicholas Lauriat - Network and Security Technologies - 1

Answer	Yes
Document Name	

Comment

N&ST believes that most Responsible Entities have reconciled to the notion that CIP requirements should be applied on a per- Cyber Asset basis, notwithstanding the fact many requirements are formally applicable to BES Cyber Systems that may comprise multiple Cyber Assets. N&ST also believes the SDT is correct in its belief that most, if not all, auditors expect to see evidence of device-level compliance. If the SDT is convinced this should be codified by revising the Standards, N&ST suggests adding language that clarifies requirements applicable to BES Cyber Systems must be applied to each Cyber Asset comprising a given BES Cyber System.

Likes 0	
Dislikes 0	

Response

Michael Shaw - Lower Colorado River Authority - 1,5,6

Answer	Yes
Document Name	

Comment

To incorporate virtualization and address the V5TAG transfer issue to clarify the meaning of the term *programmable* in the current definition of *Cyber Assets*, the SDT is proposing changes to the definition that include defining the term in the singular rather than the plural. Updating the definition to include virtual environments allows the definition of other terms based on *Cyber Asset*, such as Electronic Access Control or Monitoring Systems (EACMS) and Protected Cyber Asset (PCA) to also include virtual environments.

The proposed *Cyber Asset* definition is:

Redlined

ProgrammableAn electronic devices (physical or virtual) whose operation is controlled by a stored program that can be changed or replaced by the end user, including the hardware, software, and data in those devices the device. A virtual machine is itself a distinct asset from its host(s).

Clean

An electronic device (physical or virtual) whose operation is controlled by a stored program that can be changed or replaced by the end user, including the hardware, software, and data in the device. A virtual machine is itself a distinct asset from its host(s).

Likes 0	

Dislikes 0	

Response

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	Yes
Document Name	

Comment
CIP v5 was conceived and described to industry as a "systems-based" approach, and this conceptual framework should be promoted as much as possible. As such, Seattle City Light believes that new or revised requirements should be structured and written at the BES Cyber System level as much as possible, and new measures and VSL should be developed to reinforce the system-based approach. In some cases there may need to be new parallel VSLs for both systems and devices, but in the long run, the device-focused approach should be phased out over time.

Likes 0	
Dislikes 0	

Response

sean erickson - Western Area Power Administration - 1,6	
Answer	Yes
Document Name	

Comment
Where virtual machines behave like physical machines (run an OS such as Windows), it makes sense to request the same sort of evidence as for a physical machine that is also one component of a BES Cyber System. With regard to hypervisors due consideration should be given to their specialized nature to avoid treating them like just another OS, although change control and cybersecurity still apply.

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
Add the clear definitions for Hyper Visor (as a required asset) and Virtual Server (as a required asset) and then don't be concerned with the commodity abilities to add/remove processor, memory, disk, etc. Require that Virtual Servers remain constant in an environment regardless of what physical

hypervisor asset they are running at any given time. This will ensure consistency and allow for clear asset level tracking. Scaling is a normal part of operating in a virtual environment and needs to account for virtual scaling. With respect to horizontal scaling, an entity would need to have at least one consistent virtual asset that is listed on the BES Asset List with a stated program for how and when horizontal instance is created/destroyed to account for spikes in demand. The entity would need to clearly show how they protect (via a program) for CIP007 requirements as instances are created. The burden would be on each entity to prove their model of protection (which is the model other security compliance standards such as PCI take).

Likes 0	
Dislikes 0	

Response

Stephanie Burns - International Transmission Company Holdings Corporation - 2 - MRO,SPP RE,RF

Answer	Yes
Document Name	

Comment

ITC understands that today security is assigned at the device level and technologies have surpassed the language used in the CIP standards. Regardless, ITC recommends revising the CIP-005, CIP-007, and CIP-010 standards that reflect BES Cyber Systems to address virtualization.

We agree that controls should be applied at the device level, however, there should be specific language instead of vague and ambiguous language regarding virtualization. For instance, if a hypervisor is installed on a physical server device it should be stated that the guest OS's are all part of the same cyber asset classification. To add further clarity, if the hypervisor and physical server host BCAs then all devices should be BCAs.

The standard should offer exceptions for other methods of virtual and physical separation such as virtual firewalls, virtual switch instances, and other technologies that offer security between virtualized networks or hosts. Vendors such as CheckPoint offer VSec (a technology used to spin up virtual firewalls) both at hypervisor and host levels. Other vendors such as Cisco offer ACI technology on their Nexus 9000 switching platforms. These allow for a single layer 2 network to have enterprise security groups which isolate devices and hosts from each other.

Likes 0	
Dislikes 0	

Response

Aaron Austin - AEP - 3,5

Answer	Yes
Document Name	

Comment

AEP has observed that Regional Entity compliance staff expect evidence at the Cyber Asset level even where the applicability to the standard is at the "Cyber System" level. Regarding the definition of Cyber Asset, AEP believes the best approach is to modify the definition of Cyber Asset to make it general enough to encompass virtual machines or virtual Cyber Assets. Additional recommendation would be to evaulate inconsistencies of Applicable Systems and Measures columns.

Likes 0	
Dislikes 0	

Response

Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC

Answer	Yes
Document Name	

Comment

This is an ongoing problem that extends beyond virtualization. The SDT should consider using the Applicable Systems column to address distinctions between BES Cyber System application of requirements and BES Cyber Asset application on an explicit and per requirement basis.

Is there a recommendation include in the auditors audit guide about the ways the control should be implemented? (at the *BES Cyber Asset* or *device* level) If it's the case this guide needs to be updated.

To incorporate virtualization and address the V5TAG transfer issue to clarify the meaning of the term *programmable* in the current definition of *Cyber Assets*, the SDT is proposing changes to the definition that include defining the term in the singular rather than the plural. Updating the definition to include virtual environments allows the definition of other terms based on *Cyber Asset*, such as Electronic Access Control or Monitoring Systems (EACMS) and Protected Cyber Asset (PCA) to also include virtual environments.

An electronic device (physical or virtual) whose operation is controlled by a stored program that can be changed or replaced by the end user, including the hardware, software, and data in the device. A virtual machine is itself a distinct asset from its host(s).

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

We agree that auditors look for asset level evidence for certain requirements and that the application of this expectation is consistent with the way the Standards are written. For instance, one asset may provide AV protection for an entire system; auditors will check that asset for compliance.

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	

Ideally, the host should be treated as the high watermark of any of the devices (should be able to operate in a mixed mode, as long as demonstratable that none of the other devices have the potential to impact a higher risk impact virtual machine). NRG recommends that the language should be rewritten to accommodate the different nuances that virtual technology presents. Especially concerning the differences between a physical desktop (device level), a standalone virtual desktop (device level), and virtual linked-clone pools (system level) which contain a virtual base/parent image and their linked clones (cloned children images). The requirement is written such that the auditors are bound to look at the system level, but all of the standards have to be applied at the device level. Ultimately the choice should be up to the entity to define how they want to set up their Virtual Environment as long as all of the security controls are in place.

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 Dominion and ISO-NE	
Answer	Yes
Document Name	
Comment	

This is an ongoing problem that extends beyond virtualization. The SDT should consider using the Applicable Systems column to address distinctions between BES Cyber System application of requirements and BES Cyber Asset application on an explicit and per requirement basis.

Is there a recommendation include in the auditors audit guide about the ways the control should be implemented? (at the *BES Cyber Asset* or *device* level) If it's the case this guide needs to be updated.

To incorporate virtualization and address the V5TAG transfer issue to clarify the meaning of the term *programmable* in the current definition of *Cyber Assets*, the SDT is proposing changes to the definition that include defining the term in the singular rather than the plural. Updating the definition to include virtual environments allows the definition of other terms based on *Cyber Asset*, such as Electronic Access Control or Monitoring Systems (EACMS) and Protected Cyber Asset (PCA) to also include virtual environments.

The proposed *Cyber Asset* definition is:

Redlined

ProgrammableAn electronic devices (physical or virtual) whose operation is controlled by a stored program that can be changed or replaced by the end user, including the hardware, software, and data in those devices the device. A virtual machine is itself a distinct asset from its host(s).

Clean

An electronic device (physical or virtual) whose operation is controlled by a stored program that can be changed or replaced by the end user, including the hardware, software, and data in the device. A virtual machine is itself a distinct asset from its host(s).

Likes 0	
Dislikes 0	

Response

Lee Maurer - Oncor Electric Delivery - 1

Answer	Yes
Document Name	

Comment

We agree with the assumption. This may be the expectation of an auditor. However, more education and guidance may be required for auditors to fully understand the technology being used by industry and how to appropriately audit it.

The requirements do allow protections to be performed at a BCS level. There are some requirements where it is easier to apply a control at a BCS level. This would include malware protection at the BCS level, patch assessment at the BCS level, and event logging at a BCS level. Conversely, there are some requirements where it is easier to demonstrate compliance at the Cyber Asset level. For us, that includes baseline of assets.

When addressing compliance with virtual systems, it will be important to have the controls allowed at the host or template level as long as the entity is capable of showing how the control is inherited by a guest.

Likes 0	
Dislikes 0	

Response

Harold Sherrill - Sempra - San Diego Gas and Electric - NA - Not Applicable - WECC

Answer	Yes
Document Name	

Comment

The BES Cyber System needs to be more defined. Utilities can declare BES Cyber Systems pretty much how they see fit. This means the SDT must enforce compliance at the device level since the ‘system’ concept is still inconsistent. Provide better examples of what a ‘system’ is and how it can be audited. CIP-007 and CIP-010 require verification of things like ports open, software versions, and logging that can only be checked at the asset level, not the System Level.

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 with the assumption of the SDT that auditors have been expecting entities to demonstrate compliance at the device level. We recommend that greater efforts be made so that a measure will support/reinforce the level of control set forth in the requirement. Secondly, we feel that more coordination between a standard drafting team and auditors may be beneficial. In some instances, a standard could be audited differently than what an SDT had intended. Perhaps auditor representation, or SDT members that have audit experience may be beneficial to have on an SDT as well.	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
The present definition of BES Cyber System is very broad, as it is a grouping of BES Cyber Assets to perform one or more reliability tasks. As a result, Responsible Entities have been observed to implement this definition in many ways, from the one-to-one mapping of BES Cyber Assets into BES Cyber Systems to the other extreme of grouping all BES Cyber Assets at one impact level into a single BES Cyber System. This wide range of implementation has made evidence sampling at the BES Cyber System level impossible, forcing audits to focus on BES Cyber Assets rather than on BES Cyber Systems. Also, the term “reliability tasks” has not been defined, and this appears to contribute to the variety of groupings of BES Cyber Assets into BES Cyber Systems. If the concept of the BES Cyber System is to become truly useful, the definition must be modified such that the BES Cyber System becomes a small grouping of BES Cyber Assets that performs a specific function. It may be beneficial to identify a list of functions performed at each type of physical asset, Control Center, substation, and generator. A starting point for such a list can be found in the NERC CIPC document, “Security Guideline for the Electricity Sector: Identifying Critical Cyber Assets,” dated June 17, 2010. While obsolete for the current Standards, this document provided an extensive list of the types of functions performed at each physical asset.	
Likes 0	
Dislikes 0	
Response	

Sheranee Nedd - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
Recommendation to make the virtual machine subject to the same requirements as a physical asset but allow deployment to be done in a virtual environment. PSEG also supports Edison Electric Institute's comments.	
Likes 1	PSEG - PSEG Fossil LLC, 5, Kucey Tim
Dislikes 0	
Response	
David Francis - Midcontinent ISO, Inc. - 2 - MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG	
Answer	Yes
Document Name	
Comment	
We agree with the assumption. This may be the expectation of an auditor. However, more education and guidance may be required for auditors to fully understand the technology being used by industry and how to appropriately audit it. The requirements do allow protections to be performed at a BCS level. There are some requirements where it is easier to apply a control at a BCS level. This would include malware protection at the BCS level, patch assessment at the BCS level, and event logging at a BCS level. Conversely, there are some requirements where it is easier to demonstrate compliance at the Cyber Asset level. For us, that includes baseline of assets. When addressing compliance with virtual systems, it will be important to have the controls allowed at the host or template level as long as the entity is capable of showing how the control is inherited by a guest.	
Likes 0	
Dislikes 0	
Response	
Sarah Gasienica - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	

Answer	Yes
Document Name	
Comment	

Requirements and controls should be still enforced at a BES Cyber System level, but evidence should be provided at a device level. In virtualization and Software Defined Data Centers infrastructure is typically policy driven, meaning IT Engineers specify the ways systems should work via configuration files that apply to all systems within that container. Virtualization in particular adopted this methodolgy very early on in deployment. Therefore, applying rulesets at a system level (i.e.: All Hypervisors must require vendor-signed installation packages) makes sense -- we would want all nodes of the cluster to operate the same. However, evidence should be gathered at the device level (i.e.: provide evidence that hypervisor Cluster01-Node5 only allows vendor-signed installation packages). NIPSCO OT has already taken this stance and it seems to be the best way to manage and maintain compliance.

Likes 0	
Dislikes 0	
Response	

Nathan Mitchell - American Public Power Association - 3,4

Answer	Yes
Document Name	
Comment	

This is an ongoing problem that extends beyond virtualization. The SDT could consider using the Applicable Systems column to address distinctions between BES Cyber System application of requirements and BES Cyber Asset application on an explicit and per requirement basis.

Likes 0	
Dislikes 0	
Response	

Brandon Cain - Southern Company - Southern Company Services, Inc. - NA - Not Applicable - SERC

Answer	Yes
Document Name	
Comment	

Southern Company agrees with the SDT assumption. Version 5 introduced the BES Cyber System concept; however, for most of the high and medium impact requirements, auditors expect Responsible Entities to demonstrate compliance at the device level rather than the system as a whole. To address this issue, the SDT could add system-level implementation examples to the Guidelines and Technical Basis along with new system-level evidence examples to the measures of the requirements. Southern agrees that the current standards have a "everything is a Cyber Asset and all requirements apply to all devices" framework which can present numerous issues when applied to the seemingly endless variety of programmable electronic devices in the entire Bulk Electric System. The "per device capability" phrasing helps but often requires research and documentation to prove the negative in its own right.

The current CIP V5 standards allow for the implementation and documentation for virtualization. However because some features of virtualization are not clear, additional guidance should be considered for the implementation of mixed virtual environments, hardware pooling, and temporary virtual machines.

Likes 0	
Dislikes 0	

Response

Joseph Mosher - EDF Renewable Energy - NA - Not Applicable - WECC

Answer	Yes
Document Name	

Comment

This would require extensive changes in how auditors are sampling for audit. It would also require a look into how CIP-002 is currently defined and applied. CIP-002 talks about identifying the BES Cyber Systems, which consist of BES Cyber Assets. This is has been the explanation given to me about why auditors like to see evidence at the Cyber Asset level.

Likes 0	
Dislikes 0	

Response

Warren Cross - AEP - 1,3,4,5 - WECC,Texas RE,SERC,SPP RE,RF, Group Name ACES Standards Collaborators

Answer	Yes
Document Name	

Comment

ACES does believe the current standards are designed at the BES Cyber Asset or device level. The CIP standards were created to protect industrial controls systems that impact the BES within 15 minutes. Virtualized machines are not designed with those cyber systems in mind. How can an auditor audit a virtual system that exists in one minute and is gone the next? The two worlds, assumption and architecture do not mesh well, if at all. We would like to see a completely new set of standards that reflect the intangibles of virtualization, storage and networking without being tied to 5 year old definitions and concepts of NERC CIP.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes

Document Name	
Comment	
Reclamation recommends that definition of cyber asset be modified to include hardware, software, data and services.	
Likes 0	
Dislikes 0	
Response	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
OPG agrees that much of CIP is implemented and audited at the individual asset or device level. However, it is not unreasonable to have both a device level and a system level focus. Indeed, device level inadequacies are often mitigated by system level compensatory measures. SDT should continue to allow flexibility in how some risks are addressed where either level might be appropriate. In addition, it may be useful to consider introducing another level for virtualization host resources to address the systemic risks they introduce, as touched on in later responses.	
Likes 0	
Dislikes 0	
Response	
Lauren Price - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Where it may be a technical incapability to implement required controls on an individual device, the SDT could continue to use the “Per Cyber Asset Capability” language to give entities the flexibility to implement/leverage system-level controls. ATC also agrees with EEI member comments that the SDT could add system-level implementation examples to the Guidelines and Technical Basis along with new system-level evidence examples to the measures of the requirements.	
Likes 0	
Dislikes 0	
Response	

Wesley Maurer - Lower Colorado River Authority - 1,5,6	
Answer	Yes
Document Name	
Comment	
To incorporate virtualization and address the V5TAG transfer issue to clarify the meaning of the term programmable in the current definition of Cyber Assets, the SDT is proposing changes to the definition that include defining the term in the singular rather than the plural. Updating the definition to include virtual environments allows the definition of other terms based on Cyber Asset, such as Electronic Access Control or Monitoring Systems (EACMS) and Protected Cyber Asset (PCA) to also include virtual environments. The proposed Cyber Asset definition is: Redlined ProgrammableAn electronic devices (physical or virtual) whose operation is controlled by a stored program that can be changed or replaced by the end user, including the hardware, software, and data in those devices the device. A virtual machine is itself a distinct asset from its host(s). Clean An electronic device (physical or virtual) whose operation is controlled by a stored program that can be changed or replaced by the end user, including the hardware, software, and data in the device. A virtual machine is itself a distinct asset from its host(s).	
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 language should be rewritten to accommodate the different nuances virtual technology presents. Especially concerning the differences between a physical desktop (device level), a standalone virtual desktop (device level), and virtual linked-clone pools (system level) which contain a virtual base/parent image and their linked clones (cloned children images). The requirement is written such that the auditors are bound to look at the System Level, but all of the standards have to be applied at the device level. Ultimately the choice should be up to the entity to define how they want to set up their Virtual Environment as long as all of the security controls are in place.	
Likes 1	Berkshire Hathaway Energy - MidAmerican Energy Co., 1, Harbour Terry
Dislikes 0	
Response	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	

Version 5 introduced the BES Cyber System concept; however, for most of the high and medium impact requirements, auditors expect Responsible Entities to demonstrate compliance at the device level. To address this issue, the SDT could add system-level implementation examples to the Guidelines and Technical Basis along with new system-level evidence examples to the measures of the requirements.

Likes 3	Berkshire Hathaway Energy - MidAmerican Energy Co., 1, Harbour Terry; Great Plains Energy - Kansas City Power and Light Co., 1,3,5,6, Webb Douglas; Darnez Gresham, N/A, Gresham Darnez
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	Yes
Document Name	

Comment

The concept of the BES Cyber System, to be useful, must be developed further. There needs to be concessions given for protection of a system when the particular requirement can't or isn't implemented on each individual cyber asset. PacifiCorp would support this development in the CIP standards, however does not believe that it is necessary in order to implement language in the CIP standards that support virtualization.

Likes 2	Berkshire Hathaway Energy - MidAmerican Energy Co., 1, Harbour Terry; Darnez Gresham, N/A, Gresham Darnez
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

Kansas City Power and Light supports Edison Electric Institute's Comments.

Likes 0	
Dislikes 0	

Response

Andrew Gallo - Austin Energy - 1,3,4,5,6

Answer	Yes
Document Name	

Comment
Austin Energy (AE) agrees the SDT ***assumes*** most auditors *expect* entities to demonstrate compliance at the device level. However, AE is troubled by the fact we are making *assumptions* about any NERC Standard. To address the inconsistency, NERC should revise the CIP Standards to say what is intended rather than relying on assumptions.

Likes 0	
Dislikes 0	

Response

Patricia Robertson - BC Hydro and Power Authority - 1,3,5, Group Name BC Hydro

Answer	Yes
Document Name	

Comment
Clarify the language of the standard requirements to explicitly indicate where evidence is expected to be provided on a per device/BES Cyber Asset basis as opposed to a BES Cyber System basis or where either or is acceptable and the conditions under which it is acceptable. This is currently left to the auditing entity to communicate and express their audit approach and can lead to confusion and misinterpretation of standard requirement implementation on behalf of entities.

Likes 0	
Dislikes 0	

Response

Jeffrey Watkins - Berkshire Hathaway - NV Energy - 5 - WECC

Answer	Yes
Document Name	

Comment
Version 5 introduced the BES Cyber System concept; however, for most of the high and medium impact requirements, auditors expect Responsible Entities to demonstrate compliance at the device level. To address this issue, the SDT could add system-level implementation examples to the Guidelines and Technical Basis along with new system-level evidence examples to the measures of the requirements.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	
Comment	

AZPS agrees with the SDT's assumption that most auditors expect entities to demonstrate compliance at the device level and that it can introduce inconsistencies in the treatment of physical or virtual assets. However, AZPS respectfully submits that there are additional areas of potential inconsistency that would need to be evaluated and addressed (where determined necessary). AZPS identifies the following areas of inconsistencies for the SDT's consideration:

- Potential for inconsistent language between the Requirement and associated Measure;
- Potential for inconsistency in audit approaches between regions and/or regional audit staff and the audit documentation utilized during a registered entity's audit, e.g., interpretation of RSAW "blue notes," use of sampling tools and methods, etc.; and
- Potential for inconsistency between the language of the Requirement and associated Measure and the audit approaches, as discussed above.

All of these areas of inconsistencies must be considered by the SDT as the addition of virtualized devices has the potential to significantly complicate both compliance and audit approaches and, without clarification regarding these, inconsistencies could introduce complexity, ambiguity, and inefficiency. For example, where a requirement is applicable to a virtualized system, will each component of that system be evaluated or will the system be evaluated at the system or "common" platform level. Additionally, where such systems communicate with external networks or devices, there will need to be a common understanding of how compliance will be evaluated as controls may be "common" under certain configurations and, therefore, applied at the management plane for distribution across all data planes. For these reasons, AZPS recommends that the SDT evaluate each of these potential inconsistencies as it moves through the standards drafting process to minimize the potential for ambiguity and inconsistency by and between both registered and regional entities relative to the demonstration of compliance and the methods and documentation for compliance monitoring.

All of these areas of inconsistencies must be addressed by the SDT to ensure that both registered and regional entities have consistent understanding of the demonstration of compliance and the methods and documentation for compliance monitoring.

Likes 0	
Dislikes 0	
Response	

Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Deborah VanDeventer - Edison International - Southern California Edison Company - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5,6	
Answer	
Document Name	
Comment	
LCRA Transmission, Segment 1, has no opinion at this time.	
Likes 0	

Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE agrees implementation of the CIP Requirements are at the BES Cyber Asset or device level. The BES Cyber System concept is just 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*." There are no inconsistencies to address, a BES Cyber System is a logical grouping, and you cannot apply the CIP Standards to a logical grouping without knowing what the BES Cyber Assets are.	
Likes 0	
Dislikes 0	
Response	

2. The SDT proposes that each virtual machine and hypervisor are separate Cyber Assets. Do you agree with this position? Please provide a rationale to support your position.

(Refer to the Unofficial Comment Form for more information on this question)

Joseph Mosher - EDF Renewable Energy - NA - Not Applicable - WECC

Answer	No
Document Name	

Comment

The answer to this question is no since a hypervisor is defined as software that allocates resources to VMs. Therefore, a hypervisor should not be a Cyber Asset. The hardware running the hypervisor software should be labeled as a Cyber Asset. This distinction should be clear for all future requirements. Virtualized hardware (VM), and its associated OS, should be classified as Cyber Assets.

Likes 0	
Dislikes 0	

Response

Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance

Answer	No
Document Name	

Comment

The hypervisor’s host machine and the virtual machine are the separate Cyber Assets. The hypervisor is computer software or firmware that creates or runs the virtual machine, but does not have its own OS or system to enforce CIP controls, similar to a SCADA application running on a server. With regards to protecting the hypervisors, controls should be implemented on the host machine.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

The new definition does not address a Cyber Asset with virtualized storage which should be treated as separate Cyber Assets. The definition offers no guidance for identifying virtual Cyber Assets. A methodology is required for example, start with the function performed, then identifies each component –

Virtual Machine, storage, host and hypervisor using a high water mark. The proposed definition uses the term “[A virtual] electronic device”. A virtual Cyber Asset is not an electronic device, or a device at all. A function, for example providing control of a BES element, could be completed by a software program that runs on a vitual operating system (OS). This virtual OS is its self software, the operation of which is controlled by a hardware hypervisor. The vitual system does not function on its own, the identification of components of the system must be addressed by the standard. Managing each component can be done separately.

The definition does not address how to handle a hyper converged environment where building blocks can include storage, network compute and memory resources.

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	No
Document Name	

Comment

NRG disagrees with this proposed definition because it would cause any removable storage device to qualify as a programmable electronic device (“stored operating system” could make the definition more clear).

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	No
Document Name	

Comment

Texas RE does not agree with the SDT’s proposal to treat each virtual machine and hypervisor as separate Cyber Assets. The hypervisor (parent) is the device or software which runs the virtual machine (child). The virtual machine (VM) cannot operate without the hypervisor. This shared relationship means that neither can be separate Cyber Assets. For example, if a VM has been identified as a BES Cyber Asset (BCA); the hypervisor that runs the VM is also a BCA; which also applies to PACS, EACMS, and PCA’s

Treating the VM and hypervisor as separate Cyber Assets can cause mixed-trust virtual environments; the hypervisor runs CIP and corporate VM’s. CIP controls are only being applied to the CIP VM and not the hypervisor; even though the hypervisor “*if rendered unavailable, degraded, or misused*” can impact the CIP and corporate VM’s.

Likes 0	

Dislikes 0	

Response

Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	

Comment
AZPS agrees that each virtual machine and hypervisor are separate Cyber Assets. To ensure clarity, AZPS asserts that virtualized assets, if represented by physical hardware, would meet the current definition of Cyber Asset. Thus, simply virtualizing these assets does not change their criticality or role in the operation of the BES and, as such, these virtualized assets should still meet the definition of Cyber Asset. Moreover, hypervisors running on hardware that manage the resources for virtualized Cyber Assets would also meet the definition of Cyber Assets. Without these physical Cyber Assets, the virtualized Cyber Assets cease to exist. Because these virtualized assets can be identified, classified, and evaluated as Cyber Assets, AZPS strongly recommends that the SDT consider opportunities to modify the existing CIP requirements to expand or clarify that their applicability extends to virtual AND physical Cyber Assets. AZPS understands that there may be some requirements that will not directly apply, e.g., CIP-007-6 R1, Part 1.2's physical port protection requirements would not be applicable to virtualized Cyber Assets. Nonetheless, because these virtualized assets meet the definition of Cyber Asset, they have similar capabilities to meet the majority of the current requirements language. Thus, review and revision to the existing requirements would allow the requirements applicable to all Cyber Assets (based on capability) to be consolidated, which would reduce the potential for confusion and ambiguity given the physical and virtualized nature of virtualized devices and increase the likelihood for the application of consistent approaches by both Regional and Registered Entities.

Likes 0	
Dislikes 0	

Response

Jeffrey Watkins - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	Yes
Document Name	

Comment
NV Energy agrees that each hypervisor and virtual machine are separate Cyber Assets.

Likes 0	
Dislikes 0	

Response

Andrew Gallo - Austin Energy - 1,3,4,5,6	
Answer	Yes

Document Name	
Comment	

Based on modifications to the definition of Cyber Asset, each host and virtual machine can be separately managed and, therefore, should be distinct Cyber Assets. However, AE finds the use of the term "host" problematic when used in connection with a virtual machine. Host is very general and typically refers to servers and systems. AE would recommend using the following definition:

An electronic device (physical or virtual) with its operation controlled by a stored program which the end user can change or replace and includes the hardware, software and data. A virtual machine is itself a distinct asset from its hypervisor-host.

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	

Kansas City Power and Light supports Edison Electric Institute's Comments.

Likes 0	
Dislikes 0	
Response	

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	Yes
Document Name	
Comment	

The controls and risks apply individually to each virtual machine as well as the host (and hypervisor if considered the host).

Likes 2	Berkshire Hathaway Energy - MidAmerican Energy Co., 1, Harbour Terry; Darnez Gresham, N/A, Gresham Darnez
Dislikes 0	
Response	

Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	Yes
Document Name	
Comment	

EEI agrees that a virtual machine is distinct from a hypervisor. The guest machine or virtual machine is what the hypervisor manages/controls on a host machine. Host machines are another distinct component in the virtualization environment; however, we have found that the host (or VM host) and hypervisor may be used interchangeably or the hypervisor term may include the host machine. It would be helpful for the SDT to clearly define these terms so that all Responsible Entities, the ERO, and other stakeholders are using the same meaning for each term. A common lexicon that can be applied to all virtual or logical technologies will be required to enable all stakeholders to understand the concepts being presented by the SDT.

Likes 3	Berkshire Hathaway Energy - MidAmerican Energy Co., 1, Harbour Terry; Great Plains Energy - Kansas City Power and Light Co., 1,3,5,6, Webb Douglas; Darnez Gresham, N/A, Gresham Darnez
Dislikes 0	

Response

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

Answer	Yes
Document Name	
Comment	

This clarifies, the definition of the term *programmable*. See note above about the flexibility of what is a virtual machine.

The entities should be allowed to define how they setup their virtual environments. We agree with the first sentence and how it is defined. The second sentence should be modified to allow the entities to determine whether the Hypervisor and its children are a BES Cyber Asset or multiple BES Cyber Assets.

Likes 0	
Dislikes 0	

Response

Lauren Price - American Transmission Company, LLC - 1

Answer	Yes
Document Name	
Comment	

While this distinction may help to alleviate confusion, virtualization is a complex subject where incorrect or interchangeable use of these technical terms could lead to misinterpretation. ATC recommends that the SDT consider providing additional clarity around these terms through guidance and examples without officially them. ATC recommends that the SDT resist the temptation to reinvent/redefine these terms as historically this approach had the

unintended consequences of creating ‘new terms’ that are too prescriptive, do not scale to ever-changing technology, and/or contradict or otherwise render commonly acceptable technological terms moot.

Likes 0	
Dislikes 0	

Response

David Ramkalawan - Ontario Power Generation Inc. - 5

Answer	Yes
Document Name	

Comment

- Agree that “virtual machines” should be treated as separate cyber assets because applying the CIP requirements to “host devices” without recognizing that “virtual devices” are, in actuality, being managed as individual logical devices is fundamentally counterproductive and introduces many artificial, confusing, and unnecessary dilemmas.
- However, special consideration likely should be given to “host devices” as they represent a new systemic risk to potentially many hosted, dependant BCSs.
- Furthermore, the real risk of virtual machine “escape” attacks (ref: https://en.wikipedia.org/wiki/Virtual_machine_escape) is difficult to address but should be acknowledged. Virtualization discussions presented so far have not mentioned this low probability but very high impact risk. A successful such attack would put at risk all virtual assets in the host environment at once by taking control of the virtualization manager (or CMS). In light of this new, elevated risk, should it be acceptable, for instance, to host “non-CIP” virtual machines on a host shared with CIP virtual machines? It might be advisable, for instance, to deem “non-CIP” virtual assets as PCA equivalents unless some agreed upon mitigating measures are met to better protect the host devices and manager. An example of such a measure might be having the CMS non-virtualized and protected by non-virtual firewalls (i.e. The CMS would not be self-hosted). This is similar to separation of management and data planes addressed in question 7, however either variation might not be sufficient to mitigate these virtual machine escape attacks.
- As a minor matter of terminology, the “hypervisor” is more akin to an operating system and not the actual physical host hardware. As such, use of terms such as “host device” or “host cyber asset” would be more appropriate in the question wording than “hypervisor”.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

Reclamation supports the view of the SDT. The security required for a hypervisor is not necessarily the same as the security required for virtual machines because they are separate cyber assets.

Likes 0	
Dislikes 0	

Response

Warren Cross - AEP - 1,3,4,5 - WECC,Texas RE,SERC,SPP RE,RF, Group Name ACES Standards Collaborators

Answer	Yes
Document Name	

Comment

Yes, if they can be tracked and monitored by a naming convention. Each name of the virtual machine or hypervisor is an instance. If you were to rationale out that a function being performed is a Cyber Asset, the list would be impossible to manage.

Likes 0	
Dislikes 0	

Response

Brandon Cain - Southern Company - Southern Company Services, Inc. - NA - Not Applicable - SERC

Answer	Yes
Document Name	

Comment

Southern Company agrees each virtual machine and hypervisor are separate Cyber Assets. The purpose of the hypervisor is to manage one or more virtual machines. Virtual machines provide the same functionality of a physical computer or a Cyber Asset. Since many of the CIP requirements are at the device level, we view each instance of an OS as its own Cyber Asset and we agree it is not simply a disk image data file or application.

Likes 0	
Dislikes 0	

Response

Nathan Mitchell - American Public Power Association - 3,4

Answer	Yes
Document Name	

Comment
The SDT should consider the hypervisor and overlying virtual machines as separate Cyber Assets to enable consistent and distinct protections to be applied in each case.

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
The virtual machine represents a separate and unique attack surface from the underlying hypervisor and therefore needs to be protected as a distinct asset. Treating the hypervisor and guest virtual machines as a single device confuses physical and virtual domains and doesn't make sense from a practical standpoint. For example, management of the ports/services of the hypervisor with numerous virtual operating systems running on the same physical hardware becomes very difficult.

Likes 0	
Dislikes 0	

Response

Sarah Gasienica - NiSource - Northern Indiana Public Service Co. - 1,3,5,6

Answer	Yes
Document Name	

Comment
It is impossible to secure a guest VM and the physical hypervisor using the same technology in a requirement. For example, we would have BIOS firmware to maintain on the hypervisor. We do not have that in a virtual machine. Likewise, there are security updates for Windows guest Operating Systems that is updated much more frequently than the hypervisor -- however a vulnerability in the guest operating system does not impact the host hypervisor, and therefore it is critical to treat the two as separate entities. NIPSCO OT has always considered the hypervisor and the guest VMs as separate entities even under CIP Version 3.

Likes 0	
Dislikes 0	

Response

David Francis - Midcontinent ISO, Inc. - 2 - MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG	
Answer	Yes
Document Name	
Comment	
Based on the modifications provided to the definition of Cyber Asset, each host and guest can be separately managed objects and therefore should be treated as distinct Cyber Assets.	
Likes 0	
Dislikes 0	
Response	
Sheranee Nedd - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
PSEG supports Edison Electric Institute's comments.	
Likes 1	PSEG - PSEG Fossil LLC, 5, Kucey Tim
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 recommends that the drafting team consider whether a definition of "system" may be necessary. Depending on the type of language that is used in revising the standard language, a consistent and industry wide definition of the term "system" could remove some ambiguity which may exist.	
Likes 0	
Dislikes 0	
Response	
Harold Sherrill - Sempra - San Diego Gas and Electric - NA - Not Applicable - WECC	

Answer	Yes
Document Name	
Comment	
VMs and Hypervisors have separate Security Controls. In addition, the processors that manage the storage arrays must also be considered separate Cyber Assets as well. So you effectively have three cyber asset considerations with regards to virtualization: Virtual machine, Hypervisor, and Storage processors.	
Likes 0	
Dislikes 0	
Response	
Scott Downey - Peak Reliability - 1	
Answer	Yes
Document Name	
Comment	
There are very few protective measures that can be taken at the hardware or virtualization host layer that don't ignore the individual components of the multitude of operating system environments residing on the physical asset. This gets even more complex as modern standards, such as containerized applications, become prevalent - something the SDT will need to address very soon or risk the standards becoming obsolete to current technology.	
Likes 0	
Dislikes 0	
Response	
Lee Maurer - Oncor Electric Delivery - 1	
Answer	Yes
Document Name	
Comment	
Based on the modifications provided to the definition of Cyber Asset, each host and guest can be separately managed objects and therefore should be distinct Cyber Assets.	
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 Dominion and ISO-NE	
Answer	Yes
Document Name	
Comment	
The SDT should consider the hypervisor and overlying virtual machines as separate Cyber Assets to enable consistent and distinct protections to be applied in each case.	
Likes 0	
Dislikes 0	
Response	
RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
SCE&G treats a virtual machine and a hypervisor as separate devices. Each device has to be configured, applied patching, etc.	
Likes 0	
Dislikes 0	
Response	
Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	Yes
Document Name	
Comment	
The SDT should consider the hypervisor and overlying virtual machines as separate Cyber Assets to enable consistent and distinct protections to be applied in each case.	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 3,5	

Answer	Yes
Document Name	
Comment	

AEP recommends the lead-in sentence be reworded as follows, “The SDT proposes that each virtual machine and host are separate Cyber Assets.” The hypervisor is a piece of software running on the host and serves as an abstraction layer between the virtual machines and their physical host. Accounting for physical hosts and virtual machines separately is appropriate as they are often managed and supported as separate entities.

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	

You must consider both the hypervisor and each virtual machine as separate assets as each has a defined purpose and operation separately.

Likes 0	
Dislikes 0	
Response	

sean erickson - Western Area Power Administration - 1,6

Answer	Yes
Document Name	
Comment	

For some common virtualization platforms (VMWare, XenServer), there appears to be clear separation between the host OS and guest OS’s. This is evidenced by the ability to update the hypervisor OS and VM OS’s independently of each other. However, this does not preclude a design existing where there is much tighter integration between the Host OS and Guest OS’s which blurs any separation. Also any system in which VM’s are dynamically created and destroyed based on workload (e.g. dynamic provision) could complicate treating each VM as a distinct asset as opposed to an instance of an application.

Likes 0	
Dislikes 0	
Response	

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	Yes
Document Name	
Comment	
This proposal seems reasonable, although a systems-based approach may eliminate the need for such differentiation.	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	Yes
Document Name	
Comment	
N&ST believes this position is consistent with a widely (multi-industry) accepted view of virtualization that considers each so-called “guest OS” to be separate and distinct from the underlying hypervisor and its host OS. N&ST believes the draft NIST Special Publication, “NIST Definition of Microservices, Application Containers and System Virtual Machines,” SP800-180 (DRAFT) also supports the SDT position.	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Hypervisors offer complete dataplane (network and operating sytem-level) separation from their hosted virtual machines. The hypervisor and virtual machine each run an independent operating system, and all process and memory allocations are contained within their respective operating systems.	
Likes 0	

Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
CenterPoint Energy considers a hypervisor distinct with an independent operating system, software, user access list, network address, security configuration, etc from its guests.	
Likes 0	
Dislikes 0	
Response	
Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
The virtual machine and hypervisor are managed as separate devices and act as separate devices and should be treated as such.	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Consultant - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Any device that communicates should be considered a separate cyber asset. For example, the host physical machine that has an installed hypervisor would have ethernet interfaces for the hypervisor as well as interfaces for the virtualized devices. The virtual machines could be connected to a virtual switch which is connected to the physical Ethernet interface of the host/hypervisor machine. Therefore, any device that communicates and performs a dedicated function should be considered a separate cyber asset.	
Likes 0	

Dislikes 0	
Response	
Preston Walker - PJM Interconnection, L.L.C. - 2 - SERC,RF	
Answer	Yes
Document Name	
Comment	
Each VM and each hypervisor exist as separate network-connected devices, so this approach makes sense.	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Yes, Exelon agrees that when implementing a virtualized environment for CIP, the VM Host machine(s) as well as each individual VM guest should be considered as distinct Cyber Assets. We believe the term “VM Host machine(s)” should be utilized instead of “hypervisor” to identify what in a virtualization environment requires CIP Protection in addition to the individual VM’s.	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Please reference the response provided for #3.	
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 definition of Cyber Asset must include virtual machines (see caveat in question 3 regarding “data inside the device”). BPA believes that both “virtual machine” and “hypervisor” are well-understood terms with formal definitions (NIST SP 800-125, SP 800-125A {Draft}, SP 800-125B) and broad IT Industry acceptance, thus do not need further definition in the NERC Glossary. BPA agrees that each Hypervisor and Virtual Machine is a distinct Cyber Asset. Controls and strategies for securing virtual machines across a variety of industries have been published by agencies such as NIST and SANS.

The key issue the SDT appears to address in this revised definition is clarifying the scope or boundaries of a given virtual cyber asset in order to apply requirements and controls to each. Clarifying the definition is only necessary to address gaps in current requirements language that allow for miss-applying the requirement. BPA believes Industry understands and can securely apply the technical controls.

Likes 0	
Dislikes 0	

Response

Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	

On a network subnet, a virtual machine is logically an independant Cyber Asset (node) and should be afforded the appropriate CIP controls based on its Applicable System catagorization.

Likes 0	
Dislikes 0	

Response

Deborah VanDeventer - Edison International - Southern California Edison Company - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Wesley Maurer - Lower Colorado River Authority - 1,5,6	
Answer	Yes
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	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - International Transmission Company Holdings Corporation - 2 - MRO,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5,6	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Shaw - Lower Colorado River Authority - 1,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

3. Do you agree that the proposed Cyber Asset definition clarifies the term *programmable*? Please provide a rationale to support your position.

(Refer to the Unofficial Comment Form for more information on this question)

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

Answer	No
Document Name	

Comment

BPA agrees that the SDT's proposed definition of *programmable* encompasses a device subject to hardware and software changes by the end user.

However, BPA disagrees that the definition should apply to the data stored in the device.

- Data inside the device is peripheral and irrelevant to the operation of the device.
- The use of *data* in the current definition of *Cyber Asset* does not match Section 215 of the Energy Policy Act of 2005 that reads: "…programmable electronic devices and communication networks including hardware, software and data **that are essential to the reliable operation of the bulk power system**."
- Best practice IT Security across a broad spectrum of industries typically separates the mechanisms of protecting a *system* (better known as *Information Assurance,* Source: NIST SP 800-50, CNSSI-4009) from the mechanisms of protecting *data* transiting or resident on that system (the latter being *Information Security,* Source: NIST SP 800-59; SP 800-53; SP800-53A; SP 800-60; CNSSI-4009; FIPS 199; 44 U.S.C., Sec. 3542).
- The introduction of the concepts of *management plane* and *data plane* which are referenced in question 8 is a useful addition to the NERC CIP discussion because it enables appropriate controls to specifically protect systems or data.

Likes 1	Massachusetts Municipal Wholesale Electric Company, 5, Gordon David
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion

Answer	No
Document Name	

Comment
Dominion does not recommend a change to the current definition of Cyber Assets. If a change to the definition is made, Dominion recommends using the more generic term “logical” instead of “virtual”, as outlined below. The term “logical” would encompass any virtual environment including dual-bootable OS machines. Additionally, the phrase, “*including the hardware, software, and data in the device* “ is misplaced and should be moved. Finally, Dominion proposes that the term “machine” should be replaced by “device” for consistency: Recommended language change: *“An electronic device (physical or virtual logical), including the hardware, software, and data in the device, whose operation is controlled by a stored program that can be changed or replaced by the end user, including the hardware, software, and data in the device. A virtual logical machine device is itself a distinct asset from its host(s).”*

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1,3,5,6	
Answer	No
Document Name	

Comment
Exelon does not agree that the proposed update to the Cyber Asset definition sufficiently clarifies the meaning of “programmable.” The addition of the language “a stored program that can be changed or replaced by the end user” can be interpreted to extend the scope of the CIP requirements down to all field-updateable devices. This includes chipsets that are configurable but not programmable. If changing the device requires physical removal of a chip or any other disassembly or destruction of the device to change or update the device, then the device should be categorized as “not programmable”. The CIP-002-5: BES Cyber Assets Lessons Learned published by the NERC CIPV5 Transition Program provides examples of what the study participants used to address “programmable” during the implementation of the CIPV5 standards. Specifically, page 3 states: “study participants set the scope to be evaluated as those devices that have a microprocessor and can accept firmware, software or logic. Additionally, the study participants considered devices that had a physical or wireless port or a web interface that can be used to “flash” firmware to be Cyber Assets and then evaluated them to determine whether they meet the BES Cyber Asset definition.” Since the term “Cyber Asset” is foundational to the entire suite of CIP Standards, Exelon is concerned with the removal of the word “programmable” and changes to the Cyber Asset definition unnecessarily prompting an entire reassessment of our Cyber Assets. Exelon has an internal definition of “programmable” that is consistent with the BES Cyber Asset Lessons Learned and encourages the CIP SDT to use a similar approach. If the CIP SDT determines to make adjustments to the Cyber Asset term, any updates to clarify “programmable” should make use of example statements that are consistent with the published Lessons Learned and not replace the word “programmable” within the Cyber Asset definition. Additionally, Exelon would support the addition of a statement to the Cyber Asset definition that clarifies that “A virtual machine is itself a distinct Cyber Asset from its host(s).” Exelon does not believe that it is necessary to add the parenthetical reference “(physical or virtual)” to the Cyber Asset definition.

Likes 0	

Dislikes 0	
Response	
Preston Walker - PJM Interconnection, L.L.C. - 2 - SERC,RF	
Answer	No
Document Name	
Comment	
PJM suggests removing “by the end user.” A stored program that can be replaced or updated “by the end user” does not take into account the principle of least privilege. End users should not have the ability to update software, but rather to only perform system functions relevant to their roles. For example, a server is a programmable device, but the operating system software and firmware cannot be updated by end users – only by system administrators.	
Likes 0	
Dislikes 0	
Response	
Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
SRP requests additional clarification of *stored program*. The phrase “including the hardware, software, and data in the device” is unnecessary. Replacing the final sentence of the proposed definition with, “A virtual device is a Cyber Asset” would add clarity. SRP also requests clarification on dip switches and jumpers. Under the proposed definition would it be acceptable to exclude devices that are configured using dip switches and/or jumpers as cyber assets?	
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 Cyber Asset definition does not clarify the term programmable and is not clear where "data in the device" is concerned. In a virtual environment, the data accessible to a virtual machine (VM) is still "in" the hypervisor, but not accessible to it. Data stored on a storage area network (SAN) may not be accessible to the administrator of the SAN, but only authorized users of the SAN. CenterPoint Energy believes the clause "including hardware, software, and data in the device" does not add value and clarity to the Cyber Asset definition and should be removed.

As an alternative, CenterPoint Energy recommends addressing data that is either a) accessible by an authorized user of an asset; or b) data that is impacted by the availability of an asset, but not accessible to an authorized user of that asset. The latter case could be data stored in a VM or container that can be made unavailable by actions of the hypervisor administrator, but is not accessible or modifiable by the administrator. Data that is not accessible to users of a device cannot be modified by programmable instructions, and therefore might be excluded from the definition.

Likes 0	
Dislikes 0	

Response

Aaron Austin - AEP - 3,5

Answer	No
Document Name	

Comment

Modifications to the definition of such a key term can have far-reaching and potentially unforeseen consequences. Modifications to the definition of “Cyber Asset” could impact all aspects of an entity’s CIP compliance program. AEP suggests the following wording for the definition of Cyber Asset: “An electronic device (whether physical or virtual, including […]) whose function is controlled by an end user created stored program. A virtual machine is itself a distinct asset from its host(s).”

Likes 0	
Dislikes 0	

Response

Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC

Answer	No
Document Name	

Comment

Programmability sould be seen as independent of who perform the action.

Do you consider program configuration and scripting (scripts) as part if this definition?

We think that program configuration and scripts be part of the term parameterized.

We found a definition for Script: A computer script is a list of commands that are executed by a certain program or scripting engine.

We suggested to modify the definition of programable for :

*An electronic device (physical or virtual) whose operation is controlled by a stored program that can be changed, replaced **or parameterized** by the end user, including the hardware, software, and data in the device. A virtual machine is itself a distinct asset from its host(s).*

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 phrase ***controlled by a stored program*** is problematic and will lead to no more clarity than the use of the word programmable.

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	No
Document Name	

Comment

NRG disagrees with this proposed definition because it would cause any removable storage device to qualify as a programmable electronic device (“stored operating system” could make the definition more clear).

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 Dominion and ISO-NE

Answer	No
Document Name	

Comment

Prefer leaving the use of the term “programmable” this definition as is. Entities may have an internal definition in their existing CIP compliance program. Changing this foundational concept has multiple far-reaching impacts. Modifying the Cyber Asset definition to address scripts and firmware is unnecessary since they are already covered in CIP-010. Guidance could be added to CIP-002 on possible definitions of the term “programmable”.

In virtualized environments, the physical infrastructure can be shared between BES Cyber Systems and other non-CIP Cyber Assets while maintaining isolated virtualized environments for each.

Likes 0	
Dislikes 0	

Response

Scott Downey - Peak Reliability - 1

Answer	No
Document Name	

Comment

Creating a definition specific to the CIP standard does not benefit the SDT or the industry. Standards-based language should be used for these kinds of terms, not newly created terms with questionable interpretations. For example, why use the terms "Cyber Asset" and "programmable"? Why not use the dictionary definition of a "Computer" as "an electronic device for storing and processing data, typically in binary form, according to instructions given to it in a variable program", followed by giving specific examples of what the SDT considers to be a "Computer" in scope of the 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 does not agree that the proposed definition of Cyber Asset helps to clarify the term *programmable*. We believe that there is still the possibility for a difference of opinion between an entity and a regulator as to what an end user is capable of. We recommend the drafting team consider the following as a definition for *programmable*:

“A programmable device has a communication interface through which it’s stored program or configuration may be accessed, verified, modified, or replaced.”

Likes 0	
Dislikes 0	

Response
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4, Group Name FirstEnergy Corporation
Answer	No
Document Name	
Comment
FirstEnergy does not support any modifications to the Cyber Asset definition because it is foundational to the existing implementation of the CIP Standards. Any change will create a significant compliance exercise that requires burdensome compliance paperwork review and updates with no benefit to the reliability of the BES. Instead of modifying definitions, the SDT should seek to add requirements, guidance, and measures to enable the secure use of virtualization in the CIP environment.
Likes 0	
Dislikes 0	
Response
Anthony Jablonski - ReliabilityFirst - 10
Answer	No
Document Name	
Comment
While the change does help clarify the term “programmable,” other issues have been introduced. In addition, the phrase “that can be changed or replaced by the end user” is both ambiguous and ill-advised from a security perspective. The phrase is ambiguous in that it can be construed as broadly as a laptop PC that has been locked down by its administrators so that the end user cannot modify the programming, only the data. However, even if the definition is changed to something like “a stored program that can be changed or replaced only by direct intervention in the hardware,” this will still leave many devices out of scope. It can be argued that these devices are some of the most risky devices in a Responsible Entity’s inventory, as any programs on these devices cannot be patched even when vulnerabilities are found. As an example, see “https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/”. Changing the definition of Cyber Asset such that these devices are not included in the required CIP protections, but will be out of scope for the CIP Standards (and thus completely invisible to audit teams) should not be considered acceptable.
Likes 0	
Dislikes 0	
Response

Sheranee Nedd - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	No
Document Name	
Comment	
The scope of the revised definition proposed seems more broad than the previous definition. Caution must be exercised to ensure that additional unintended devices, for example 'smart' instruments that use HART or similar protocols, are not inadvertently defined as Cyber Assets by a change to the term's current definition intended only to address virtualization. PSEG also supports Edison Electric Institute's and NPCC's comments.	
Likes 1	PSEG - PSEG Fossil LLC, 5, Kucey Tim
Dislikes 0	
Response	
Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	No
Document Name	
Comment	
This definition does not take the distinction between configurable and programmable as was discussed under the V5 project into account. This new definition would seek to include devices that are configurable (i.e. via dip-switches) as changes to these predefined configurations/inputs would result in a change to a stored program by an end-user. Devices that have embedded programming that cannot be changed by end users, except through pre-defined configurations/inputs should be excluded.	
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	
Suggest provide guidance or clarification to include software / firmware in definition of "stored program".	
Likes 0	

Dislikes 0	
Response	
Nathan Mitchell - American Public Power Association - 3,4	
Answer	No
Document Name	
Comment	
Prefer leaving the use of the term “programable” in the definition as is. Entities may have an internal definition in their existing CIP compliance program. Changing this foundational concept has multiple far-reaching impacts. Modifying the Cyber Asset definition to address scripts and irmware is unnecessary since they are already covered in CIP-010. Guidance could be added to CIP-002 on possible defintinos of the term “programable”.	
Likes 0	
Dislikes 0	
Response	
Brandon Cain - Southern Company - Southern Company Services, Inc. - NA - Not Applicable - SERC	
Answer	No
Document Name	
Comment	
Southern Company does not agree with the proposed changes to the Cyber Asset definition. The current Cyber Asset definition is an integral part of the the CIP Standards. Modifications to the Cyber Asset definition would require a review of the current compliance documentation for thousands of devices. NERC has provided implementation guidance on defining BES Cyber Assets that Southern finds sufficient regarding the term programmable. The SDT should add guidance, and measures to enable the secure use of virtualization in the CIP environment.	
Likes 0	
Dislikes 0	
Response	
Warren Cross - AEP - 1,3,4,5 - WECC,Texas RE,SERC,SPP RE,RF, Group Name ACES Standards Collaborators	
Answer	No
Document Name	
Comment	

I don’t think it is clear as to how that included virtualization. Is a virtualized storage device, programmable? Trying to fit virtualization concepts into Cyber Assets that are tangible is problematic. I would recommend using a NIST Virtualization Guidance and have two set of standards. That perform functions in different way, terminology and capabilities.	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	
Reclamation recommends that definition include programmable electronic devices, including the hardware, software, and data that is essential to the reliable operation of the bulk electric system.	
Likes 0	
Dislikes 0	
Response	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
EEI does not support any modifications to the Cyber Asset definition because it is foundational to the existing implementation of the CIP Standards. Any change will create a significant compliance exercise that requires burdensome compliance paperwork review and updates with no benefit to the reliability of the BES. Instead of modifying definitions, the SDT should seek to add requirements, guidance, and measures to enable the secure use of virtualization in the CIP environment.	
Likes 3	Berkshire Hathaway Energy - MidAmerican Energy Co., 1, Harbour Terry; Great Plains Energy - Kansas City Power and Light Co., 1,3,5,6, Webb Douglas; Darnez Gresham, N/A, Gresham Darnez
Dislikes 0	
Response	
Deborah VanDeventer - Edison International - Southern California Edison Company - 1,3,5,6 - WECC	
Answer	No

Document Name	
Comment	
SCE does not support modifications to the Cyber Asset definition because of its impact to the current CIP standard implementations. Modifications may create potential compliance review and updates with no significant benefit.	
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	
Kansas City Power and Light supports Edison Electric Institute's Comments.	
Likes 0	
Dislikes 0	
Response	
Jeffrey Watkins - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	No
Document Name	
Comment	
NV Energy does not believe that the proposed definition clarifies the term programmable. A possible alternate definition could be: An electronic device (physical or virtual) that is controlled by a stored program and has a locally or remotely accessible input interface such as a management port or a web interface that would allow the introduction of firmware, software, or a logic update. NV Energy does have some concerns with the changing of the Cyber Asset definition. Because this definition is the foundation to the existing CIP Standards any change will create a significant compliance exercise that requires burdensome compliance paperwork review and updates with no benefit to the reliability of the BES. Instead of modifying definitions, the SDT should seek to add requirements, guidance, and measures to enable the secure use of virtualization in the CIP environment.	
Likes 0	
Dislikes 0	
Response	

Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	No
Document Name	
Comment	

AZPS respectfully asserts that the proposed definition introduces new areas and potential for ambiguity and confusion relative to the term "programmable." In particular, AZPS identified the following questions:

- Where is/can the "stored program" stored?
- Can it be stored on a separate Cyber Asset for the control of a virtualized or different asset?
- Who is the "end user" and how is "changed or replaced by the end user" defined?
- Does such change or replacement have to be performed directly by the "end user" or can it be performed by a third party through a contractual service obligation?
- Does the phrase require that an "end user" have the actual technical or other capability to make such a change or replacement before the asset would qualify as a Cyber Asset?
- If an "end user" has no one on staff that can change the stored program and no service provider, is the asset not considered a Cyber Asset?

Given the potential confusion associated with these questions, AZPS offers the following definition of Cyber Asset:

"A physical or virtual electronic device containing operating system(s), software, and/or firmware which programming and configuration can be modified.

Physical electronic devices include the hardware, software, and data in the device.

A virtual electronic device includes its virtual hardware, software, and data, and is distinct and separate from its physical host(s)."

Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	

Answer	Yes
Document Name	
Comment	
The SDT should consider removing the language "by the end user." The security objective should be to afford controls to a Cyber Asset irrigardless of who can change or replace it.	
Likes 0	
Dislikes 1	Massachusetts Municipal Wholesale Electric Company, 5, Gordon David
Response	
Mike Smith - Consultant - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
I also believe that the terminology as to “stored program” offers flexibility in that this can be software or programmable hardware (e.g., as in a field-programmable gate array).	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Removal of the word Programmable narrows the new wording and the definition to software. The term ‘end user’ should be defined to avoid confusion.	
Likes 0	
Dislikes 0	
Response	

Nicholas Lauriat - Network and Security Technologies - 1	
Answer	Yes
Document Name	
Comment	
N&ST believes the qualifying criterion, "...stored program that can be changed or replaced…" is helpful.	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	Yes
Document Name	
Comment	
A definition in the singular ordinarly is more precise and easier to parse than one in plural. In this case the difference appears relatively minor, with the exception that the added sentence, about a virtual machine, adds clarity about these cases.	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	Yes
Document Name	
Comment	
It seems clear from the definition that what is being talked about is re-programmability—the ability for a devices function to be changed, which obviously has cybersecurity implications that a hard-coded, un-alterable device does not. Whether a device is virtual doesn't seem to alter they fact that it may be re-programmable.	
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	
The updated definition accounts for the ability to change hardware, software, and data for an asset. This provides for firmware, data, and other software that can change or update the functionality of the device and hence is programmable. This differs from a fixed device that is purpose built to perform one action and cannot change hardware, software, or data to change the functionality.	
Likes 0	
Dislikes 0	
Response	
Lee Maurer - Oncor Electric Delivery - 1	
Answer	Yes
Document Name	
Comment	
The definition is an improvement in that it addresses the meaning of programmable and allows for the use of virtual systems instead of just physical systems.	
Likes 0	
Dislikes 0	
Response	
Harold Sherrill - Sempra - San Diego Gas and Electric - NA - Not Applicable - WECC	
Answer	Yes
Document Name	
Comment	
We suggest "computing" rather than "electronic". Please give a definition of “end user” that includes administrators. However, I think it is beneficial to retain “by the end user” because this limits the inclusion of additional devices that might not apply because they are not truly programmable as in the ability to be provided with coded instruction for performance of an automatic task either serially or through Ethernet. I disagree with this alternative. I think the 4th alternate example is the best suggestion with the added language regarding the virtual machine.	
Likes 0	
Dislikes 0	

Response	
Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Clarification is needed that user-modifiable configuration settings are not considered part of the stored program. Also, replace the term “asset” with “device.”	
Likes 0	
Dislikes 0	
Response	
David Francis - Midcontinent ISO, Inc. - 2 - MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG	
Answer	Yes
Document Name	
Comment	
The definition is an improvement in that it addresses the meaning of “programmable” and allows for the use of virtual systems instead of just physical systems.	
Likes 0	
Dislikes 0	
Response	
Sarah Gasienica - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
This new definition is significantly clearer and leaves must less room for interpretation. This aligns closely with how NIPSCO OT has deployed virtualization, treating every virtual machine as it's own BES Cyber Asset. **However** I would caution that the SDT somehow accounts for things such as the firmware on a hard disk. Firmware on a disk controls the operations of the drive, which especially in enterprise-grade hardware is certainly modifiable. I do believe it is the intent of the SDT that hard drives, peripherals, etc of the asset are all logically grouped together, providing they're managed together. For example, most of our servers get hard drive firmware as part of the server firmware package. The server as a whole is placed at a certain firmware version, which includes hard drives. I would suggest that if a Storage Area Network was used to store the data for a device the	

Storage Area Network device should be maintained separately from the collective BCAs. Hard Drives, IO cards, etc should all be considered part of the same BES Cyber Asset. While this new definition is much clearer, some additional scope restrictions would further reduce confusion.	
Likes 0	
Dislikes 0	
Response	
Joseph Mosher - EDF Renewable Energy - NA - Not Applicable - WECC	
Answer	Yes
Document Name	
Comment	
The proposed definition is much clearer and removed most of the ambiguity around programmable.	
Likes 0	
Dislikes 0	
Response	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Yes, this definition better describes the essence of cyber assets and their malleable nature versus devices whose functionality is permanently set. There is yet some concern that devices that may appear “permanently set” or “non-programmable” might actually consist of common programmable computer architectures “under the hood” and that this might be something of a loophole. If an irresponsible vendor of such a system elects not to disclose the internals of a device and refuses to release updates of any type, then the device could harbor CIP related concerns, elevated for lack of updates, and yet still not qualify as a cyber asset under the proposed definition. This concern might be partially addressed by dropping the words “*by the end user*”.	
Likes 0	
Dislikes 0	
Response	
Lauren Price - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	

While the Cyber Asset definition is foundational to the existing implementation of the CIP Standards, in its current form it does not go far enough to adequately capture the devices that should be under the purview of the standards. ATC supports the revised definition and recommends the SDT consider replacing the word “program” with the word “executable code” for added clarity. The use of the word “program” might may have the unintended consequences of bringing in digital logic based devices.

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

Yes the standards need to allow for mixed trust devices as long you can logically separate them. The CIP standards need to be modified to support this because currently they do not address this. Not all companies have the resources to have multiple hypervisors for both CIP and Non-CIP.

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	Yes
Document Name	

Comment

PacifiCorp believes that the language does provide some clarity to the term *programmable*, but does not substantially alter the definition. While we believe that we should have a definition for *programmable*, we do not believe that developing one now is required to develop requirements necessary to support virtualization. PacifiCorp suggests a dedicated effort directed at clarifying the language in CIP-002 so that application of the CIP standards becomes more consistent across the industry.

Likes 0	
Dislikes 0	

Response

Andrew Gallo - Austin Energy - 1,3,4,5,6

Answer	Yes

Document Name	
Comment	
The revised definition addresses the meaning of "programmable" and allows for using virtual systems instead of just physical systems.	
Likes 0	
Dislikes 0	
Response	
Michael Shaw - Lower Colorado River Authority - 1,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - International Transmission Company Holdings Corporation - 2 - MRO,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wesley Maurer - Lower Colorado River Authority - 1,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE recommends the following: "*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	

4. In virtualized environments, the physical infrastructure can be shared between BES Cyber Systems and other non-CIP Cyber Assets while maintaining isolated virtualized environments for each.

Such configurations are not addressed explicitly in CIP-005-5. Are modifications required to address the issue? Please provide your rationale.

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

Answer	No
Document Name	

Comment

The current CIP-005-5 standards do not sufficiently address the logical isolation and separation using VLANs. If you can acknowledge and allow entities to do this, it would be highly beneficial to them and to the auditors. VLAN's can be separated and standards can be applied to allow this separation.

Likes 0	
Dislikes 0	

Response

Sarah Gasienica - NiSource - Northern Indiana Public Service Co. - 1,3,5,6

Answer	No
Document Name	

Comment

Standard 5 requirements are clear enough to enable an entity to architect the infrastructure as needed and to segment for subnet isolation.

Likes 0	
Dislikes 0	

Response

Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance

Answer	No
Document Name	

Comment

Agree with the below rationale for question #5.

Concerning virtual networks, network devices can have multiple logical networks configured (e.g. virtual local area networks (VLANs)). Physical or virtual devices perform "logical isolation" when configured such that some network interfaces are available inside an ESP, and other interfaces are outside an

ESP and the two networks cannot communicate with each other inside of the device. This would not prevent the VLANs configured inside the device from communicating through an EAP.	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	
The premise of the question, “In virtualized environments, the physical infrastructure can be shared between BES Cyber Systems and other non-CIP Cyber Assets while maintaining isolated virtualized environments for each,” is not correct. See “https://cmaurice.fr/pdf/ndss17_maurice.pdf”.	
Likes 0	
Dislikes 0	
Response	
RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	
Answer	No
Document Name	
Comment	
No modifications necessary.We do not use.	
Likes 0	
Dislikes 0	
Response	
Daniel Grinkevich - Con Ed - Consolidated Edison Co. of New York - 1,3,5,6	
Answer	No
Document Name	
Comment	

CIP-005-5 does not need to explicitly address virtualization. The Standard is adequate as written, and allows for the use of virtualized systems within an ESP boundary. Mixed-used virtualization which crosses ESP boundaries is an insecure practice, because any vulnerability in hosted systems can expose networks and host that share the same hypervisor.

We are concerned about scope creep into non-BCA CIP assets, e.g. EACMS. Virtualized EACMS should not inherit the same protections required of BCS.

Likes 0	
Dislikes 0	

Response

Aaron Austin - AEP - 3,5

Answer	No
Document Name	

Comment

AEP recommends the SDT modify the guidelines and technical basis of CIP-005 or other standards to include additional language supporting the hosting of multiple impact ratings on the same Cyber Asset. The impact ratings of BCS comprised, in part or in whole, of virtual Cyber Assets can be independent of the impact rating of the physical Cyber Asset host. Cyber Assets hosting virtual Cyber Assets are assigned the impact rating of the highest impact BCS or highest impact rating EACMS, PACS, or PCA it hosts. A "non-CIP Cyber Asset" hosted on a CIP Cyber Asset would not have an impact rating imparted on it. Responsible Entities should be expected to demonstrate segmentation between virutal Cyber Assets of differing impact ratings. Further, AEP recommends the SDT develop reference architectures accounting for potential use cases.

Likes 0	
Dislikes 0	

Response

Mike Smith - Consultant - NA - Not Applicable - NA - Not Applicable

Answer	No
Document Name	

Comment

I checked “no” on the assumption that the new definition of “cyber asset” would extend to all other existing standards reliant on the definition of “cyber asset”.

Likes 0	
Dislikes 0	

Response

Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Yes. Assuming that virtualization is permitted for BES Cyber Systems, which AZPS supports, to the extent possible, AZPS recommends revising and/or clarifying through revisions to defined terms that the existing CIP Reliability Standards (such as CIP-005) are applicable to virtualized devices. Additionally, AZPS recommends that the SDT clearly address the following: • Whether or not non-CIP Cyber Assets are permitted to operate on physical infrastructure used by virtualized CIP Cyber Assets; • Whether CIP Cyber Assets of different impact ratings are permitted to operate the physical infrastructure used by virtualized CIP Cyber Assets; • How a Registered Entity should extend CIP-005-5 controls through lower level elements of a virtualization stack, such as a hypervisor or other shared virtualization services; • Whether, if BCS(s) of different CIP-002 impact ratings reside on the same physical/shared virtualization environment, all BCS would be subject to a “high-water mark” requirement based on the highest impact BCS utilizing the shared environment.	
Likes 0	
Dislikes 0	
Response	
Jeffrey Watkins - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	Yes
Document Name	
Comment	
NV Energy feels that additional language in CIP-005 would be helpful to provide guideance as to what methods are considered to be adequate to overcome reisks and provide secure isolation or separation of the environments.	
Likes 0	
Dislikes 0	
Response	
Patricia Robertson - BC Hydro and Power Authority - 1,3,5, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
The current standard language is not sufficient to clearly differentiate between the boundary of what is in scope for CIP protections and what is not regarding virtualization. Additional explicit language and examples would be beneficial for entities in this regard.	

Likes 0	
Dislikes 0	
Response	
Andrew Gallo - Austin Energy - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
To encourage consistent implementation, modifications would help ensure implementation of proper controls and architecture to reduce risk to BES Cyber Systems.	
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	
Kansas City Power and Light supports Edison Electric Institute’s Comments.	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
While it is a practice that PacifiCorp would likely not employ, modifications to CIP-005 (as well as possibly CIP-002, CIP-007, and CIP-010) would be necessary to support mixed-trust environments.	

Likes 2	Berkshire Hathaway Energy - MidAmerican Energy Co., 1, Harbour Terry; Darnez Gresham, N/A, Gresham Darnez
Dislikes 0	

Response

Deborah VanDeventer - Edison International - Southern California Edison Company - 1,3,5,6 - WECC

Answer	Yes
Document Name	

Comment

SCE believes that clarification is needed on the classification of the shared asset. For example, will non BES-assets come in scope due to common physical infrastructure? SCE recommends that virtualization implementations used for CIP Cyber Assets should not share physical infrastructure with non-CIP Cyber Assets.

Likes 0	
Dislikes 0	

Response

Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	Yes
Document Name	

Comment

If the intent of the SDT is to allow sharing of physical infrastructure between CIP and non-CIP Cyber Assets through virtualization, then new requirements would need to be added to ensure adequate isolation methods are implemented. For example, virtual technologies cannot deny access by default as required by CIP-005-5, Requirement R1, Part 1.3. Currently, virtualization is used for CIP Cyber Assets, but these implementations do not share physical infrastructure with non-CIP Cyber Assets.

Likes 3	Berkshire Hathaway Energy - MidAmerican Energy Co., 1, Harbour Terry; Great Plains Energy - Kansas City Power and Light Co., 1,3,5,6, Webb Douglas; Darnez Gresham, N/A, Gresham Darnez
Dislikes 0	

Response

Lauren Price - American Transmission Company, LLC - 1

Answer	Yes
Document Name	

Comment

ATC recommends the SDT consider potential unintended consequences and construct the requirement in a manner so as to preclude regional interpretations of high watermarking to result in rendering the added flexibility moot. Additionally, the requirement must address what constitutes an EAP where and ESP dissects physical infrastructure Additionally, ATC support EEI's comments that new requirements would need to be added to ensure adequate isolation methods are implemented. For example, virtual technologies cannot deny access by default as required by CIP-005-5, Requirement R1, Part 1.3. Currently, virtualization is used for CIP Cyber Assets, but these implementations do not share physical infrastructure with non-CIP Cyber Assets.

Likes 0	
Dislikes 0	

Response

David Ramkalawan - Ontario Power Generation Inc. - 5

Answer	Yes
Document Name	

Comment

There is the concern, as raised in response 2, of "escape attacks", which it might be appropriate to acknowledge or address in part or in full in CIP-005. As discussed in response 2, it may be prudent to require more stringent risk mitigation approaches before allowing mixing of CIP and non-CIP Cyber Assets on a shared host resource or else all otherwise non-CIP virtual assets would be held to the PCA requirements.

It would perhaps be advisable to explicitly state that all virtualization host devices which host CIP virtual BCAs would in turn be classified as BCAs. This could tie in with the idea of a third level to complement the device and BCS levels as discussed in response 1 and 2.

Finally, in the case of software defined network "switches" that reside completely in the virtualization platform as an instantiated component of that platform, it is currently unclear if that would be regarded as a separate virtual cyber asset, as would be the case with a virtual machine or physical switch. In many cases these virtual networking components aren't managed in a way that's analogous to their physical counterparts (no user accounts, passwords, patching, etc.) because they are managed entirely in the "management plane". Do they need be treated as a distinct virtual asset?

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

Reclamation recommends adding virtualization to the current CIP-005-5 as it relates to the OSI Model.

Likes 0	

Dislikes 0	

Response

Warren Cross - AEP - 1,3,4,5 - WECC,Texas RE,SERC,SPP RE,RF, Group Name ACES Standards Collaborators

Answer	Yes
Document Name	

Comment

Yes they need to be addressed through a virtualization standard and not forced into the current CIP concept.

Likes 0	
Dislikes 0	

Response

Joseph Mosher - EDF Renewable Energy - NA - Not Applicable - WECC

Answer	Yes
Document Name	

Comment

We would need language that states we can use infrastructure to support protected and non-protected areas. Based on current CIP-005 language, it seems that we cannot use protected hardware/infrastructure to service a larger environment (i.e., regulated and non-regulated). We do not believe that the same rigor should be required of the supporting infrastructure. There should be a tiered approach where the Cyber Assets running the critical services receive the most attention.

Likes 0	
Dislikes 0	

Response

Brandon Cain - Southern Company - Southern Company Services, Inc. - NA - Not Applicable - SERC

Answer	Yes
Document Name	

Comment

Southern Company agrees modifications to CIP-005-5 are needed to address sharing physical infrastructure between BES Cyber Systems and non-CIP Cyber Assets in virtual environments. Additional requirements could be considered to ensure isolation methods are implemented when virtual environments are shared. Current approaches are to avoid mixing CIP and non-CIP environments until further clarity can be provided through the Standards development process.

Likes 0	
Dislikes 0	
Response	
Nathan Mitchell - American Public Power Association - 3,4	
Answer	Yes
Document Name	
Comment	
From the CIP compliance standpoint, one of the reasons to isolate virtualized environments, whether physical or virtual, is to allow for different impact level for each environment. It is unclear at this time, the SDT's intent in allowing mixed mode configurations. As currently written, CIP-005-5 requires all components contained in a virtual system to be protected at the impact level of the highest single component of the system. CIP-005-5 would need to be revised to allow for mixed impact levels within a single virtual host.	
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	
The ESP definition is defined as a logical border but there is currently no construct by which to apply layer 2 network controls for logical isolation to support this type of configuration. All controls are applied at Layer 3 for an ESP at the EAP.	
Likes 0	
Dislikes 0	
Response	
David Francis - Midcontinent ISO, Inc. - 2 - MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG	
Answer	Yes
Document Name	
Comment	

To ensure consistency of implementation, modifications would help ensure that proper controls and architecture are implemented to reduce risk to BES Cyber Systems.

Likes 0	
Dislikes 0	

Response

Sheranee Nedd - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs

Answer	Yes
Document Name	

Comment

From the CIP compliance standpoint, one of the reasons to isolate the virtualized environments, whether physical or virtual, is to allow for different impact level for each environment. It is unclear at this time, the SDT's intent in allowing mixed mode configurations.

PSEG supports Edison Electric Institute's comments.

Likes 1	PSEG - PSEG Fossil LLC, 5, Kucey Tim
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 the current CIP standards do not explicitly address this issue. We believe that more guidance is necessary to improve understanding and clearly state the what is expected of industry stakeholders.

Duke Energy would also like to highlight the topic of storage, and recommend that the drafting team consider discussing its importance relative to virtualization. Virtualization cannot be done without some type of storage. More guidance around this topic, and what should be considered by an entity when addressing this issue is needed.

Likes 0	
Dislikes 0	

Response

Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Current CIP-005 does not describe how to handle these boundaries or if any additional protection / configuration is required. The current CIP-005 is based on physical connections and a physical inspection. This does not work well at all with virtual systems. If a virtual host spans multiple networks, the standards must address how to treat each component of the virtual system. There must be some framework for grouping of systems on a host such that guest systems of a different security level are not mixed with high security systems.	
Likes 0	
Dislikes 0	
Response	
Harold Sherrill - Sempra - San Diego Gas and Electric - NA - Not Applicable - WECC	
Answer	Yes
Document Name	
Comment	
Clarify security control requirements when CIP and non-CIP resources are in a shared environment.	
Likes 0	
Dislikes 0	
Response	
Scott Downey - Peak Reliability - 1	
Answer	Yes
Document Name	
Comment	
See response 2 above. Logical technologies are becoming the standards at all layers of the OSI model except the physical and data link layers; virtual routers, switches and firewalls are commonly used tools. The specific criteria the SDT expects entities to abide by when it comes to partitioning the physical and logical layers of CIP and non-CIP protected assets is a line that needs to be clearly addressed.	
Likes 0	
Dislikes 0	
Response	

Lee Maurer - Oncor Electric Delivery - 1	
Answer	Yes
Document Name	
Comment	
To ensure consistency of implementation, modifications would help ensure that proper controls and architecture are implemented to reduce risk to BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion and ISO-NE	
Answer	Yes
Document Name	
Comment	
From the CIP compliance standpoint, one of the reasons to isolate virtualized environments, whether physical or virtual, is to allow for different impact level for each environment. It is unclear at this time, the SDT's intent in allowing mixed mode configurations. As currently written, CIP-005-5 requires all components contained in a virtual system to be protected at the impact level of the highest single component of the system. CIP-005-5 would need to be revised to allow for mixed impact levels within a single virtual host. Concerning virtual networks, network devices can have multiple logical networks configured (e.g. virtual local area networks (VLANs)). Physical or virtual devices perform "logical isolation" when configured such that some network interfaces are available inside an ESP, and other interfaces are outside an ESP and the two networks cannot communicate with each other inside of the device. This would not prevent the VLANs configured inside the device from communicating through an EAP.	
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	

NRG recommends that the standards need to allow for mixed trust devices as long you can logically separate them. The CIP standards need to be modified to support this because currently they do not address this. Not all companies have the resources to have multiple hypervisors for both CIP and Non-CIP. (The Hypervisor would need to be operated as the high water-mark).

Likes 0	
Dislikes 0	

Response

Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC

Answer	Yes
Document Name	

Comment

From the CIP compliance standpoint, one of the reasons to isolate virtualized environments, whether physical or virtual, is to allow for different impact level for each environment. It is unclear at this time, the SDT's intent in allowing mixed mode configurations. As currently written, CIP-005-5 requires all components contained in a virtual system to be protected at the impact level of the highest single component of the system. CIP-005-5 would need to be revised to allow for mixed impact levels within a single virtual host.

Concerning virtual networks, network devices can have multiple logical networks configured (e.g. virtual local area networks (VLANs)). Physical or virtual devices perform "logical isolation" when configured such that some network interfaces are available inside an ESP, and other interfaces are outside an ESP and the two networks cannot communicate with each other inside of the device.

Likes 0	
Dislikes 0	

Response

Stephanie Burns - International Transmission Company Holdings Corporation - 2 - MRO,SPP RE,RF

Answer	Yes
Document Name	

Comment

The standard must address new technologies which would allow security groups and other means of virtual separation within the virtualized environment. This includes virtual firewalls, switch instances, and other mechanisms which can be used to secure virtual hosts from each other.

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	
Absolutely! In order to account for the sharing of physical virtualization infrastructure for NERC CIP and no-NERC CIP assets the requirements need to be updated to account for virtual LANs, Virtual Firewalls, and the protection of the base hypervisor and physical infrastructure. It is possible to manage this in a secure and auditable fashion but the current standards do not account for how to collect and verify the correct level of separation and security controls.	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	Yes
Document Name	
Comment	
Auditors have evolved over time significantly in what they consider mixed trust, making it hard for entities to be inline with a moving target. The standards should clearly define by a deterministic process or via specific examples what the limits are on sharing infrastructure between CIP and non-CIP systems. It may be better to prescribe security controls that must exist when sharing, rather than forbidding the sharing due to the existing of technologies which leverage shared technology while providing significant isolation.	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	Yes
Document Name	
Comment	
Seattle suggests that the concept of ESP needs to be made even more "logical" in nature, removing all vestige of a physical nature. To achieve this end, it might help to assign the revised concept a new name that does not implicitly imply anything physical (as does the term "perimeter"). Perhaps "electronic security isolation" or ESI?	

Seattle further wishes to see virtualization concepts to expanded to address cloud-based systems. We are highly frustrated, for example, that NERC itself appears since early 2015 to have employed cloud storage for sensitive E-ISAC information including CIP incident reports from registered entities (see slide 6 of ES-ISAC Update in: http://www.nerc.com/gov/bot/botsotc/board%20of%20trustees%20%20standards%20oversight%20and%20tech1/sotc_presentations_february_2015.pdf) and yet has been unable to provide audit guidance as to whether the cloud systems with the FedRAMP protections would satisfy the security requirements of CIP-004 and CIP-011. We encrouage the SDT to address cloud matters if possible.

Likes 0	
Dislikes 0	

Response

Nicholas Lauriat - Network and Security Technologies - 1

Answer	Yes
Document Name	

Comment

Absent any definitive requirement statements in CIP-005-5 about virtualization and the use of “mixed trust” configurations, Regional Entity auditors have, largely be default, become the arbiters in any dispute over whether or not a given “mixed trust” implementation is in compliance.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

Parameters of an ESP within a virtual environment require clarification.

Likes 0	
Dislikes 0	

Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
CenterPoint Energy agrees with EEI's comments. If the intent of the SDT is to allow sharing of physical infrastructure between CIP and non-CIP Cyber Assets through virtualization, then language should be added addressing isolation methods.	
Likes 0	
Dislikes 0	
Response	
Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
SRP does feel this needs to be addressed in CIP-005-5; however, it is unclear what the modifications would look like at this time. More information is needed and the SDT should perform an evaluation of the impact these modifications will have on the standards. SRP also requests clarification regarding hypervisors. Would a hypervisor be considered a BES Cyber Asset?	
Likes 0	
Dislikes 0	
Response	
Preston Walker - PJM Interconnection, L.L.C. - 2 - SERC,RF	
Answer	Yes
Document Name	
Comment	
This should be clarified in the standards, since without explicit direction on this issue, it is left to the interpretation. The SDT should be mindful to provide these clarifications at the objective level in order to prevent becoming too prescriptive and to help future proof the standards.	
Likes 0	
Dislikes 0	

Response	
Chris Scanlon - Exelon - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Yes, in order for CIP and non-CIP environments to share a physical infrastructure via a virtualized environment, additional language in CIP-005 would be helpful to provide guidance for what methods are considered to be adequate to overcome risks and provide secure isolation or separation of the environments. Having said that, Exelon does not currently envision undertaking the risk inherent in utilizing a “mixed” virtualized environment to host CIP and non-CIP VM’s, unless the entire “mixed” environment is afforded NERC CIP protections. In other words, we would not want to trust implementing security only at the software level to isolate virtualized CIP and non-CIP components.	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
The ability for logical separation between BCSs and non-CIP Cyber Assets should be addressed. This includes the ability of a network switch to perform the logical separation as well as virtual environments.	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
It is BPA’s position that CIP-005-5 would benefit from being modified to a security objective-oriented standard rather than a requirements-based standard. The security objective in this case would be isolation of CIP-applicable Cyber Assets from Cyber Assets that are out of scope of CIP controls.	

The mechanisms of that protection are primarily Boundary Protection and Control of Network Ports, Protocols, and Services (SANS 20 Critical Security Controls).

CIP v5 narrowly focuses on routable protocols and Layer 3 controls and does not address the other layers of the OSI model. For example, under CIP-005-5 Layer 2 protocols are not addressed and can convey malware as well as allow information exfiltration and cyber-attacks even if no routable IP communications are present. Controls for these protocols should not be limited to or defined by Layer 3/4 ACLs on a firewall or router as the only or even the best means of achieving in-bound and out-bound access control. Entities need the opportunity to provide technical controls at whatever conceptual layer is appropriate to meet the security objective.

BPA recommends expanding CIP-005 language to include security zones with the ESP construct. When framed in terms of Boundary Protection, a security zone is more inclusive and granular because it is not limited to routable protocols at the OSI Model's Layer 3. A security zone construct does not force any particular interpretation or control onto serial or other non-routable means of transporting data or accessing the management plane of any systems. Security zones apply to physical and logical separation equally. An example of logical isolation provided by other than ACLs would be when a hypervisor provides isolation between Guest VMs or between Virtualized Network Functions. This isolation is implemented in the control plane by means of logic embedded in code base (NIST SP 800-125A – Draft, Section 1.2: Hypervisor Baseline Functions) and not at a conceptual network layer.

Current CIP standards take a broad stroke approach by requiring the protection of all cyber assets within an ESP in a singular manner at the highest impact level of controls. This is not cost effective or flexible enough for individual entities' needs. Security zones provide a scalable means of appropriately protecting Cyber Systems of differing security risks by further isolation within the zone.

Likes 0	
Dislikes 0	

Response

Steven Rueckert - Western Electricity Coordinating Council - 10

Answer	Yes
Document Name	

Comment

The SDT should consider requiring additional controls for the Electronic Security Perimeter including the current access control lists in CIP-005-5, Part 1.3.

Likes 0	
Dislikes 0	

Response

Laura Nelson - IDACORP - Idaho Power Company - 1

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Wesley Maurer - Lower Colorado River Authority - 1,5,6

Answer	
Document Name	

Comment

Abstains from vote. LCRA seeks clarification on types of modifications SDT would implement prior to voting yes or no.

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	
Document Name	

Comment

Modifications are not required to address the issue since, virtual environments should be treated the same as physical environments.

Such configurations can exist; the hypervisor (physical infrastructure) that is shared between BES Cyber Systems and other non-CIP Cyber Assets must be protected at the impact level of the BES Cyber System.

Furthermore, proper isolation (network segmentation, DMZ, virtual firewalls, vlans, etc,) must be implemented to reduce the risk of non-CIP Cyber Assets impacting BES Cyber Systems (e.g. Denial Of Service (DoS) attack).

Likes 0	
Dislikes 0	

Response

Teresa Cantwell - Lower Colorado River Authority - 1,5,6

Answer	

Document Name	
Comment	
LCRA Transmission Services Corporation (TSC) has chosen to abstain from vote. LCRA TSC seeks clarification on types of modifications SDT would implement prior to voting yes or no.	
Likes 0	
Dislikes 0	
Response	
Michael Shaw - Lower Colorado River Authority - 1,5,6	
Answer	
Document Name	
Comment	
Abstains from vote. LCRA TSC seeks clarification on types of modifications SDT would implement prior to voting yes or no. Concerning virtual networks, network devices can have multiple logical networks configured (e.g. virtual local area networks (VLANs)). Physical or virtual devices perform “logical isolation” when configured such that some network interfaces are available inside an ESP, and other interfaces are outside an ESP and the two networks cannot communicate with each other inside of the device. This would not prevent the VLANs configured inside the device from communicating through an EAP.	
Likes 0	
Dislikes 0	
Response	

5. The SDT asserts that VLANs providing logical isolation are not addressed explicitly in CIP-005-5, and controls may be necessary to isolate BES Cyber Systems. Are the current requirements of CIP-005-5 sufficient to address logical isolation using VLANs? Please provide your rationale.

(Refer to the Unofficial Comment Form for more information on this question)

Steven Rueckert - Western Electricity Coordinating Council - 10

Answer	No
Document Name	

Comment

The current Electronic Security Perimeter definition establishes the protective enclave at a network (Layer 3). This is further identified in CIP-005-5, Part 1.3 access control lists. VLANs (layer 2) have not been an acceptable approach to establishing an Electronic Security Perimeter with a layer 2 switch; the switch cannot afford the required controls of Part 1.3. The SDT should clearly identify at what OSI model layer the SDT is asserting an Electronic Security Perimeter can be established and require controls to ensure isolation.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

BPA believes the same modifications necessary to make CIP-005-5 adequate to question 4 would apply to addressing the specific question of 802.1 Q VLANs providing adequate logical isolation in question 5. The security objective should be to provide isolation by means of Boundary Protection as well as Control of Network Ports, Protocols, and Services. Legacy software vulnerabilities that have long since been patched or known exploits that are mitigated through proper configuration should not require the blanket rejection of VLANs as a component of a particular entity's specific security scheme. Newly discovered exploits and vulnerabilities are addressed through CIP-007 testing and patching, CIP-010 baseline configuration, change management, vulnerability scanning and assessment.

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion

Answer	No

Document Name	
Comment	
Please reference the answer provided for #4.	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1,3,5,6	
Answer	No
Document Name	
Comment	
Exelon agrees that the current requirements of CIP-005-5 do not explicitly allow for VLANs providing logical isolation. Exelon has serious concerns that virtual isolation may not be adequately secure, and rewriting the CIP Standards is not the answer. There may not be an acceptable way to revise CIP standards to allow use of VLANs for mixed environments, as the risk for compromise is too high. Virtualization is one configuration mishap away from revoking logical isolations, no matter how well thought out, should the management layer collapse into a single unified network. Employing technology that eliminates the possibility of collapse provides a much more effective mitigation by removing the possibility of any collapse. Firewalls provide an active control environment meeting CIP-005-5 by utilizing a comprehensive security toolset, including rulesets, the deny-all rule, bidirectional controls, scanning for malware, etc. However, a Layer 3 network switch does not have these features, and cannot provide the same level of security. Exelon contends that implementing VLANs using a Layer 3 network switch will not meet current requirements or security needs. While VLANs can be configured to go thru a firewall, the switch itself is still vulnerable to reconfiguration to directly connect separated VLANs. Layers of manual processes to manage the risks are the only alternative, and would be considered weak security as well as additional cost (possibly offsetting any cost-savings from virtualizing). As such, we consider that VLANs are not an appropriate technology to provide adequate security in a CIP environment.	
Likes 0	
Dislikes 0	
Response	
Preston Walker - PJM Interconnection, L.L.C. - 2 - SERC,RF	
Answer	No
Document Name	
Comment	
This should be clarified in the standards, since without explicit direction on this issue, it is left to the interpretation of auditors. PJM suggests that it should be clarified at the objective level and should not be prescriptive, to account for different implementation methods.	

Likes 0	
Dislikes 0	
Response	
Mike Smith - Consultant - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
While traditional network technologies such as VLANs can provide an an easy way to isolate traffic within a network, software-defined networking technology provides a much stronger protection by not forwarding tagged packets in the first place. I assert that methods of isolation are not explicitly addressed within CIP-005-5 and that expanded language should be added to detail additional controls. I also assert that if language such as “physical separation” is used that controls such as software defined networking be recognized as “physical separation.” If a software defined networking Ethernet switch does not have any flow rules programmed into the switch, then there is no physical connectivity (deny by default) with devices attatched to the same switch. Software-defined networking employs a superior approach in that no additional data must be inserted into the header (e.g., VLAN TAG), rather the grouping can be accomplished with flow rules and executed at the packet forwarding devices (SDN Switches) in a highly simplified and automated manner. This ensures the tamper resistant flow of communication, limiting what an adversary could do with a man-in-the-middle attack, e.g., modifying the VLAN tag.	
Likes 0	
Dislikes 0	
Response	
Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
SRP does not feel this is addressed in any of the CIP-005-5 requirements. CIP-005-5 addresses ESPs, which are a layer 3 concept. VLANs are a layer 2 concept. Addressing this in CIP-005-5 would assist with clarifying acceptable isolation. SRP requests clarification regarding why VLANs are a concern. Is using VLANs for isolation a concern because of inadvertent traffic between VLANs (i.e., VLAN hopping)? What about the shared storage from which the hypervisor serves VMs? Is the entire storage array CIP if there is a single CIP VM on it?	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	

Answer	No
Document Name	
Comment	

CenterPoint Energy believes VLANs are a separate topic from "virtualization" as it relates to virtual machines and that the requirements around VMs will be difficult to apply equally to network infrastructure. These requirements, when written, should be separate without an attempt to write one requirement applicable to all virtual technology.

CenterPoint Energy believes the logical protection afforded by a VLAN is well established, having been in broad usage in industry for decades, but has risks not addressed in existing requirements. Entities should be free to maximize hardware utilization through use of VLANs if they choose. The practical examples of VLAN-escape attacks, exploiting default VLANs or the trunk protocol used to manage VLANs, are well known and easily mitigated with switch configuration. The requirements of CIP-005 do not address these mitigations, and the Cyber Vulnerability Assessment may or may not address them. To adopt VLANs securely, CenterPoint Energy recommends creating a new CIP-005 requirement and suggests the following wording: "Implement a process to ensure that a virtual network infrastructure, fully or partially within an Electronic Security Perimeter, is configured to mitigate the risk of VLAN escape attacks."

Furthermore, the terms "connected using a routable protocol within or on an ESP" in the Protected Cyber Asset definition is confusing in relation to virtual machines. CenterPoint Energy recommends clarification to the PCA definition:

1. A hypervisor hosting a BCS virtual machine must be a BCS since it can impact the availability of a BCS within 15 minutes.

2. An asset hosted by a hypervisor in an ESP that is not part of the BCS within the same ESP must be treated as a Protected Cyber Asset.

Likes 0	
Dislikes 0	
Response	

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

Answer	No
Document Name	
Comment	

CIP 005 does not sufficiently address modern network topologies. The use of layer-2 VLANs should be an explicitly acceptable method of segregation for BES Cyber Systems and non-CIP Cyber Assets on a shared physical network infrastructure.

Security measures to protect virtualized workloads can be implemented in an equivalent security posture as a traditional physical workload. Complete datapath isolation can be achieved on routers and firewalls using virtualized routing tables and virtualized operating systems. This virtualized datapath isolation provides a secure foundation for enabling workloads, such as virtual BES Cyber Systems and non-CIP Cyber Assets, to share physical network infrastructure.

Likes 0	
Dislikes 0	

Response

Nicholas Lauriat - Network and Security Technologies - 1

Answer	No
Document Name	

Comment

N&ST agrees with the SDT's view that CIP-005-5 does not address VLANs and how they might be logically segregated. Needless to say, this lack of information is making it difficult for entities to determine whether or not a given VLAN implementation will satisfy Regional Entity auditors.

Likes 0	
Dislikes 0	

Response

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body

Answer	No
Document Name	

Comment

The SDT has made good progress in their white paper identifying many of the concepts and approaches necessary for virtualization, and we support continued development along these lines. We are concerned, however, about relying too heavily on a single model of virtualization to frame the concepts and approaches for new requirements, and urge the SDT to consider more broadly the various implementations and possibilities of virtualized systems in addition to the reference model they have created.

Likes 0	
Dislikes 0	

Response

sean erickson - Western Area Power Administration - 1,6

Answer	No
Document Name	

Comment

If the SDT asserts that VLANs isolation is not sufficient security to protect the ESP from communication beyond the ESP, explicit language forbidding the practice is necessary which would open a can of worms since there will always be emerging security issues too numerous to itemize in regulations. When entities do not use a best-practice, or common-practice approach to security, it is probably not best addressed in CIP regulations, but rather as an evidence-based, educational communique indicating the risk of a certain approach. Any entity that continues to take on such a risk can be later evaluated on their CVA process as to why they are not remediating risks above a certain level.

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 requirements need to be enhanced to specify the expectations for using VLANs within an EAP. VLANs are used extensively now to perform the level of logical exception but these are almost exclusively done at the port level.

Likes 0	
Dislikes 0	

Response

Stephanie Burns - International Transmission Company Holdings Corporation - 2 - MRO,SPP RE,RF

Answer	No
Document Name	

Comment

The standard needs to be revised to take technologies that have been around for a very long time. Such as VLAN tagging and separations and 802.1Q trunking. The standard should say when an 802.1Q trunk consists of VLANs that are both outside the ESP and inside the ESP that the layer 3 route must terminated at an EAP.

Likes 0	
Dislikes 0	

Response

Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC

Answer	No

Document Name	
Comment	

The SDT should add requirements to address all the risk presented in the virtualization risk map file.

The SDT has identified certain risks inherent to virtualization regarding the use of centralized management automation. The SDT is proposing to classify *Centralized Management System* (CMS) explicitly as a type of applicable system for some CIP requirements. In examining management architecture and risk management for virtual environments, the SDT identified an increased risk inherent to the span of control of hypervisor management consoles. Further, the SDT noted that similar risks exist in CMSs used to manage physical devices, and recognized these risks may not be fully addressed in current CIP standards and the *EACMS* definition. The SDT is considering a new definition of this class of system.

The proposed *Centralized Management System* (CMS) definition is:

A centralized system for administration or configuration of BES Cyber Systems, including but not limited to systems management, network management, storage management, or patch management.

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	No
Document Name	
Comment	

NRG recommends that the current CIP-005-5 standards do not sufficiently address the logical isolation and separation using VLANs. If entities could be allowed to do this, it would be beneficial to them and to the auditors. VLAN's can be separated and standards can be applied to allow this separation.

Likes 0	
Dislikes 0	
Response	
Scott Downey - Peak Reliability - 1	
Answer	No
Document Name	
Comment	

VLAN isolation is one of the oldest methods of securing networked systems, particularly when VLANs are then trunked through firewalls for VLAN-to-VLAN management. The SDT hasn't addressed this level of virtualization in an environment.

Likes 0	
Dislikes 0	

Response

Harold Sherrill - Sempra - San Diego Gas and Electric - NA - Not Applicable - WECC

Answer	No
Document Name	

Comment

Clarify security control requirements when CIP and non-CIP resources are in a shared environment.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Current CIP-005 program does not address VLAN at all and it is very difficult to determine what the SDT / NERC requires. There is no framework or guidance on network architecture. The standard does not address where physical separation is required, and where the use of VLAN or other virtual network technology is appropriate or beneficial. The CIP-005 standard does not address communication requirements between systems, or give guidance on separating systems with external communication.

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 believes that the current requirements in CIP-005-5 do not adequately address logical isolation using VLANs. More guidance on this issue would be beneficial to to improve understanding and clearly state the what is expected of industry stakeholders.

Likes 0	
Dislikes 0	

Response

Sheranee Nedd - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs

Answer	No
Document Name	

Comment

The SDT should consider defining a Virtual Security Perimeter (VSP) or modifying the existing ESP term in a way that would apply to cyber assets associated with a hypervisor and dependent virtual machine relationship to address needed controls in such a situation.

Suggest that the SDT provide guidance on the use of the isolation of traffic provided by VLANS as an electronic control.

Likes 1	PSEG - PSEG Fossil LLC, 5, Kucey Tim
Dislikes 0	

Response

Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance

Answer	No
Document Name	

Comment

Entergy agrees with the concept of logical isolation as described above, but has received contrary guidance related to this concept from outside entities. Entergy does not agree that additional controls are required for logical isolation. However, providing clarity on the applicability of existing CIP-005 controls related to logical isolations would benefit all parties.

The SDT has identified certain risks inherent to virtualization regarding the use of centralized management automation. The SDT is proposing to classify *Centralized Management System* (CMS) explicitly as a type of applicable system for some CIP requirements. In examining management architecture and risk management for virtual environments, the SDT identified an increased risk inherent to the span of control of hypervisor management consoles. Further, the SDT noted that similar risks exist in CMSs used to manage physical devices, and recognized these risks may not be fully addressed in current CIP standards and the *EACMS* definition. The SDT is considering a new definition of this class of system.

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	
There is no construct provided to apply layer 2 controls to technologies like VLANs. Adding this construct could allow for future proofing of the use of isolation technology such as VLANs, VXLANs, MPLS, etc.	
Likes 0	
Dislikes 0	
Response	
Nathan Mitchell - American Public Power Association - 3,4	
Answer	No
Document Name	
Comment	
The SDT should consider defining a term such as “Virtual Security Perimeter (VSP)” or modifying the existing ESP term to allow for the isolation fo BES Cyber Assets or BES Cyber Systems using virtual technologies. While CIP-005 is applicable to High and Medium Impact only, therefore, request the SDT to address VLANs for Low Impact in CIP-003. Currently, a VLAN may be part of the electronic security controls (per CIP-003-6 and CIP-003-7) for a low impact BES Cyber System. The determination by the SDT to allow or eliminate these VLANS in CIP-005 may have an unintended corresponding consequences on the interpretation of CIP-003 for low impact. Suggest that the SDT provide guidance on the use of the isolation of traffic provided by VLANS as an electronic control.	
Likes 0	
Dislikes 0	
Response	
Brandon Cain - Southern Company - Southern Company Services, Inc. - NA - Not Applicable - SERC	
Answer	No
Document Name	
Comment	
Southern Company does not agree with the SDT assertion that VLANs providing logical isolation are not addressed in CIP-005-5. The CIP-005 Standard requirements can be applied to VLANs without additional clarification as CIP-005 requires that applicable Cyber Assets must	

reside in a “logical border” and any external routable connectivity through that logical border must be through an identified Electronic Access Point, and that EAP must deny all traffic except for what is explicitly allowed. These objectives can be met with physical or virtual networks and logical isolation.	
Likes 0	
Dislikes 0	
Response	
Joseph Mosher - EDF Renewable Energy - NA - Not Applicable - WECC	
Answer	No
Document Name	
Comment	
CIP-005 language changes should not be limited to VLANs. It should also apply to virtualized routing instances, firewall contexts, and virtual network appliances. You can still control the boundary using virtual mechanisms if you explicitly allow VLANs it implicitly disallows other virtual solutions. You should use more general terms and not use VLANs as the sole mechanism.	
Likes 0	
Dislikes 0	
Response	
Warren Cross - AEP - 1,3,4,5 - WECC,Texas RE,SERC,SPP RE,RF, Group Name ACES Standards Collaborators	
Answer	No
Document Name	
Comment	
No the current standard doesn’t address VLANs or the concepts at all. The requirements, applicability and measures would all have to be modified.	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	

Reclamation recommends defining and adding VLANs, Hypervisor, Virtual Machines, Virtual Networks and Virtal Storage to the NERC Glossary of Terms and identifying which VLAN features are to be included in CIP-005-5.

Likes 0	
Dislikes 0	

Response

David Ramkalawan - Ontario Power Generation Inc. - 5

Answer	No
Document Name	

Comment

VLAN implementation is all ready being used and relied on extensively in CIP environments. CIP-003-7 Model 9 also supports use of virtualization, so it seems VLANs have already been adopted as acceptable.

What is not clear is that CIP-005 does not state that CIP related and non-CIP related though isolated on VLANs can be mixed on a single physical switch. Up to this point we have used seperate switches for CIP related traffic and VLANS have been only used to further subdivide the CIP related traffic. For instance into a SCADA network and a DMZ supporting EACMS and PACS. An explicit statement allowing mixed virtually isolated CIP and non-CIP traffic on shared physical host networking devices, and under what conditions, if any, would give more compliance certainty about VLAN acceptibility in these circumstances.

Also, as a second concern, it might be pruduent to disscuss the issue that it is inherently easier to misconfigure virtual networking and VLANS in such a way that a setup is intended and thought to be secure and compliant with CIP-005 but in fact is not, even though it appears to be "working". Mandating an independent review/verification by a second person/party (fresh set of eyes) or actual security testing during comissioniong or some other verification measure might be an appropriate mitigation for this risk in a virtual environment.

Likes 0	
Dislikes 0	

Response

Lauren Price - American Transmission Company, LLC - 1

Answer	No
Document Name	

Comment

ATC agrees that the regulation is not clear as to when layer 2 or layer 3 VLANs constitute access, or the requirement for an EAP on the device configured to use VLANs. Additionally, ATC supports EEI’s comments in that CIP-005-5 is insufficient because it does not enable the use of VLANs for logical isolation since the requirements cannot be met and the use of VLANs (i.e., layer 3 switch) to logically isolate CIP from non-CIP environments does not provide the same level of security as a layer 2 switch with a firewall.

Likes 0	

Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
If the host (or hypervisor) carries routable protocol communications destined for both inside and outside of the ESP, then it would itself be a conundrum (it should be a BCA or PCA if inside, but cannot be a BCA or PCA if outside). The current language in CIP-005-5 (and CIP-002, CIP-007, and CIP-010) do not support this current configuration and would need to be modified to allow it.	
Likes 2	Berkshire Hathaway Energy - MidAmerican Energy Co., 1, Harbour Terry; Darnez Gresham, N/A, Gresham Darnez
Dislikes 0	
Response	
Patricia Robertson - BC Hydro and Power Authority - 1,3,5, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
There is no clear standard requirement language at present that excludes the usage of VLANs, and it is not clear through inference as to under what conditions VLANs can be used. Recommend the standard requirements provide clear distinctions regarding VLAN usage and requirements for such configurations.	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	No
Document Name	
Comment	

AZPS respectfully submits that VLANs have the ability for appropriate controls, but that, previously, there has been inconsistency about whether VLAN controls are adequate to meet the current ESP-related requirements. AZPS encourages the SDT to review and revise CIP-005-5 such that VLANs and their applied security controls can be utilized as an ESP boundary.

Likes 0	
Dislikes 0	

Response

Jeffrey Watkins - Berkshire Hathaway - NV Energy - 5 - WECC

Answer	No
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Aaron Austin - AEP - 3,5

Answer	Yes
Document Name	

Comment

As implemented, AEP believes VLAN configurations provide sufficient records of and controls for logical network segmentation. And, there is no need for a requirement to dictate a standard of proof.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

The current requirements of CIP-005-5 are clear in their assertion that virtualized systems may reside within an ESP. ESPs should be isolated from other networks. Virtualized systems should not cross ESP boundaries. We do not believe that logical controls are sufficient to define an ESP boundary. VLANs should not be permitted to define ESP boundaries.

We are concerned that the SDT is confusing VLANs and hypervisor based virtual switches.

Likes 0	
Dislikes 0	

Response

RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC

Answer	Yes
Document Name	

Comment

More clarification is needed for the question.

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 Dominion and ISO-NE

Answer	Yes
Document Name	

Comment

The current requirements of CIP-005-5 are clear in their assertion that virtualized systems may reside within an ESP. ESPs should be isolated from other networks. Virtualized systems should not cross ESP boundaries. We do not believe that logical controls are sufficient to define an ESP boundary. VLANs should not be permitted to define ESP boundaries.

The proposed *Centralized Management System* (CMS) definition is:

A centralized system for administration or configuration of BES Cyber Systems, including but not limited to systems management, network management, storage management, or patch management.

The SDT should add requiremnts to address all the risk presented in the virtualization risk map file.

Likes 0	
Dislikes 0	

Response

Lee Maurer - Oncor Electric Delivery - 1	
Answer	Yes
Document Name	
Comment	
The current requirements related to EAPs and inbound and outbound access controls are sufficient. However, guidance would help in showing that the use of VLANs is an adequate means of logical isoloation and physical isolation on dedicated equipment is not required.	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Logical isolation is not the equivalent of security isolation. While VLANs are useful within environments containing different levels of trust to reduce broadcast domains and to isolate different types of traffic, VLANs should not be considered a security mechanism used to separate highly critical traffic from untrusted traffic. As traffic not within CIP scope must be considered as completely untrusted by the CIP audit teams, mixing non-CIP-scope traffic and CIP traffic within the same physical network should not be considered acceptable.	
Likes 0	
Dislikes 0	
Response	
David Francis - Midcontinent ISO, Inc. - 2 - MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG	
Answer	Yes
Document Name	
Comment	
The current requirements related to EAPs and inbound and outbound access controls are sufficient. However, guidance would help in showing that the use of VLANs is an adequate means of logical isoloation. Physical isolation on dedicated equipment is not required.	
Likes 0	

Dislikes 0	
Response	
Sarah Gasienica - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Addressing the routable subnets in CIP005 inherently addresses the VLANs at layer 2.	
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	
Kansas City Power and Light supports Edison Electric Institute’s Comments.	
Likes 0	
Dislikes 0	
Response	
Andrew Gallo - Austin Energy - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
The current requirements related to EAPs and inbound/outbound access controls suffice. However, guidance would help show the use of VLANs is an adequate means of logical isolation and physical isolation on dedicated equipment is not required.	
Likes 0	
Dislikes 0	
Response	

Laura Nelson - IDACORP - Idaho Power Company - 1	
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	
Deborah VanDeventer - Edison International - Southern California Edison Company - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Shaw - Lower Colorado River Authority - 1,5,6	
Answer	
Document Name	
Comment	

Abstains from vote. LCRA TSC seeks clarification on types of modifications SDT would implement prior to voting yes or no.

The SDT has identified certain risks inherent to virtualization regarding the use of centralized management automation. The SDT is proposing to classify *Centralized Management System* (CMS) explicitly as a type of applicable system for some CIP requirements. In examining management architecture and risk management for virtual environments, the SDT identified an increased risk inherent to the span of control of hypervisor management consoles. Further, the SDT noted that similar risks exist in CMSs used to manage physical devices, and recognized these risks may not be fully addressed in current CIP standards and the *EACMS* definition. The SDT is considering a new definition of this class of system.

The proposed *Centralized Management System* (CMS) definition is:

A centralized system for administration or configuration of BES Cyber Systems, including but not limited to systems management, network management, storage management, or patch management.

Likes 0	
Dislikes 0	

Response

Teresa Cantwell - Lower Colorado River Authority - 1,5,6

Answer	
Document Name	

Comment

LCRA TSC has chosen to abstain from vote. LCRA TSC seeks clarification on types of modifications SDT would implement prior to voting yes or no.

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	
Document Name	

Comment

Yes, the current requirements of CIP-005-5 are sufficient to address logical isolation using VLANs, physical or virtual networks.

VLANs can meet the definition of an ESP, which is “*the logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol*.”

Likes 0	
Dislikes 0	

Response

Wesley Maurer - Lower Colorado River Authority - 1,5,6

Answer	
Document Name	

Comment

Abstains from vote. LCRA seeks clarification on types of modifications SDT would implement prior to voting yes or no.

Likes 0	
Dislikes 0	

Response

6. Do you agree with the proposed definition of CMS? If not, please provide alternative language for the definition and your rationale.

(Refer to the Unofficial Comment Form for more information on this question)

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

Answer	No
Document Name	

Comment

AZPS respectfully submits that the development and creation of additional terms and asset classifications is unnecessary. As discussed above, all cyber assets (physical or virtual) can be classified in existing classification of Cyber Asset if it is modified as recommended in AZPS's response to Question #2. Hence, AZPS does not agree with or support the creation of a new definition for CMS or the use of such a term in the CIP Reliability Standards.

Likes 0	
Dislikes 0	

Response

Jeffrey Watkins - Berkshire Hathaway - NV Energy - 5 - WECC

Answer	No
Document Name	

Comment

This new definition seems broad and is hard to support without a clear idea of how it will be used in requirements and how this will impact existing CIP implementations. The scope of the new requirements also needs to be very clear.

Likes 0	
Dislikes 0	

Response

Patricia Robertson - BC Hydro and Power Authority - 1,3,5, Group Name BC Hydro

Answer	No
Document Name	

Comment

The proposed definition is too general and appears to potentially include compliance management systems that are relational databases used to manage compliance activities pertaining to BES Cyber Systems. This comment is in reference to the usage of 'centralized system for administration', and the additional language of 'including but not limited to….'. Recommend adding further qualifiers to the definition that explicitly mention virtualization

applications of said systems or systems used to manage physical devices, which leaves compliance management systems that are not used in such context, out of scope.

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

No.

KCP&L identifies several points of concern and offers an alternative. The alternative, in concept, is not perfect; we offer it to address our concerns and the inherent risks identified by the SDT.

Concerns

1. **Impact to Applicability of Existing CIP Standards**: A new CMS definition is considerable and far-reaching; it requires a review of applicability in the complete suite of CIP Standards and, where impactful changes are identified, the effected Standard going through the revision process.
2. **Impact on Entities**: A new CMS definition requires entities to review and incorporate the new definition and subsequent revisions to Standards because of the new definition into their documentation, policies and procedures.
3. **Potential Scope Expansion**: The proposed CMS definition's scope may potentially swell to include physical systems.

Alternative

The concept is to move away from a CMS new asset type approach to incorporating management devices into existing EACMS asset types. To integrate this concept into the existing NERC EACMS Glossary definition, we offer:

Electronic Access Control, Monitoring or Management Systems (EACMS):

Cyber Assets that perform electronic:

1. Access control of the Electronic Security Perimeter(s) or BES Cyber Systems;
2. Security incident and event monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems; and,
3. System management functions associated with the Electronic Security Perimeter(s) or BES Cyber Systems.

EACMS include, but are not limited to, Intermediate Systems; firewall management; patching management; virtual system management; access control; security incident and event monitoring; and server and workstation management. Management systems are limited to systems capable of modifying the configuration; applying patches, updates or code changes; remotely starting, shutting down, or restarting the asset—rebooting, its services or processes; or has the capability of altering a Cyber Asset's function within in a BES Cyber System.

In addition to the revised EACMS glossary term, a revision to CIP-007-6, Table R1, adding a new subpart under the R1 Table could address when there are instances Out-of-band networks required for Cyber Asset management. The new subpart to Table R1, Ports and Services, would apply to High

Impact and Medium Impact EACMS used for management devices to connect to things like iLOs, virtual switches, firewalls, network devices, and devices that require a port on a network that is separated physically or logically from normal production traffic.	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
In practice, how does the definition of a CMS differ from that of an EACMS? How would the risks be mitigitated differently? Without any clear intent of how the SDT plans to implement a new defition, PacifiCorp cannot support the creation of one.	
Likes 2	Berkshire Hathaway Energy - MidAmerican Energy Co., 1, Harbour Terry; Darnez Gresham, N/A, Gresham Darnez
Dislikes 0	
Response	
Deborah VanDeventer - Edison International - Southern California Edison Company - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
Additional clarity is needed to understand how this new term will be applied in the CIP requirements and how this term will impact existing CIP implementations.	
Likes 0	
Dislikes 0	
Response	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	

This new definition seems broad and is hard to support without a clear idea of how it will be used in requirements and how this will impact existing CIP implementations. The scope of the new requirements needs to be very clear. For example, is this term intended to apply only to virtualized environments or will it extend to other management systems? Will this create duplicative classifications, e.g., as an EAMCS and a CMS or as a PCA and a CMS?

Also, CMS is an acronym commonly used for Content Management Systems, which may cause confusion.

Likes 2	Berkshire Hathaway Energy - MidAmerican Energy Co., 1, Harbour Terry; Darnez Gresham, N/A, Gresham Darnez
Dislikes 0	

Response

Wesley Maurer - Lower Colorado River Authority - 1,5,6

Answer	No
Document Name	

Comment

LCRA seeks language specifying that only devices which make configuration changes would be in scope. Network monitoring software can be part of a network management system but if the network monitor does not make configuration changes it should not be considered a Centralized Management System.

Likes 0	
Dislikes 0	

Response

Lauren Price - American Transmission Company, LLC - 1

Answer	No
Document Name	

Comment

In the standard the Intermediate System definition exists, and could be leveraged to meet this objective. Additionally, if a separate definition were to be created, while it refers to BES Cyber Systems, the scope expands as a function of the applicable systems and associated Cyber Assets within the parts of the standard (unintended consequences) Additionally, ATC supports EEI's comments that this new definition seems broad and is hard to support without a clear idea of how it will be used in requirements and how this will impact existing CIP implementations The scope of the new requirements needs to be very clear. For example, is this term intended to apply only to virtualized environments or will it extend to other management systems? Will this create duplicative classifications, e.g., as an EAMCS and a CMS or as a PCA and a CMS? Also, CMS is an acronym commonly used for Content Management Systems, which may cause confusion.

Likes 0	
Dislikes 0	

Response

David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	
Comment	
A reservation regarding the proposed definition is that it does not define a threshold for when a supporting cyber asset becomes a CMS. Is it if it supports a single BCA? Or multiple? Inclusive or exclusive of PCAs, EACMS, PACS? Does it apply if only a single BCS is managed? Or more than one?	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	
Reclamation recommends providing clarification on the proposed definition of CMS. Does the SDT intend for the proposed definition of CMS apply to CIP-010-2?	
Likes 0	
Dislikes 0	
Response	
Joseph Mosher - EDF Renewable Energy - NA - Not Applicable - WECC	
Answer	No
Document Name	
Comment	
We do not think you should differentiate CMS from EACMS. If anything, you should broaden the definition of an EACMS to include other central management and administration systems. Many of these systems perform both functions, which would only increase ambiguity.	
Likes 0	
Dislikes 0	
Response	

Brandon Cain - Southern Company - Southern Company Services, Inc. - NA - Not Applicable - SERC	
Answer	No
Document Name	
Comment	
In the absence of more information on how it would be used, Southern Company does not agree with the proposed definition of Centralized Management System (CMS). Assuming the typical virtualization environment, management consoles may be within the ESP and protected at least as PCA's, including CIP-010 change management for the console and all configured BES Cyber Systems. Alternatively, management consoles classified as an EACMS may be used to support many EACMS outside an ESP, and therefore would complicate the identification, classification, and applicable requirements of various Centralized Management Systems used in different capacities (BCS, EACMS, PCA).	
Likes 0	
Dislikes 0	
Response	
Nathan Mitchell - American Public Power Association - 3,4	
Answer	No
Document Name	
Comment	
CMS's that meet the definition of a BES Cyber Asset would already be identified in the CIP-002 assessment process since they would be Cyber Assets that, if misused, could have a 15 minute impact on the BES. This was not an issue that was identified by FERC. A revisions to the CIP standards caused by this expansion of scope could cause additional delays in the current implementation thereby delaying the security that the standards are meant to insure. We suggest that this term not be included as part of this CIP modification project. If the SDT determines that there is an additional risk associated with the CMS for hypervisor management consoles, this risk should be addressed without pulling in unrelated systems.	
Likes 0	
Dislikes 0	
Response	
Sheranee Nedd - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	No
Document Name	
Comment	

PSEG supports Edison Electric Institute's comments.

Likes 1	PSEG - PSEG Fossil LLC, 5, Kucey Tim
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer	No
Document Name	

Comment

The definition is well crafted, but the term "centralized" may contain some ambiguity in this context. Must the CMS be centralized in one device? In one location? For one function? Suggested revision:

Centralized Management System (CMS): A system for administration or configuration of multiple BES Cyber Assets, including but not limited to systems management, network management, storage management, or patch management.

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 does not agree with the proposed definition of Centralized Management System. As written, the definition is too broad, and could possibly bring in devices not intended by the SDT (i.e. Corporate laptops). The examples identified appear to be appropriate, but the capability aspect alluded to in the definition makes this definition too broad in scope.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment
A CMS should be managed/protected. The definition does not give clear criteria on what is included as a CMS. How is the term “administration” defined and what type of administration is included. If a system provides operational monitoring but cannot change an end point is it included? If a system stores backup configuration files or data is it included? How is the term “configuration” defined? The text in the statement “including but not limited to” should be moved to a guidance section and do not belong in a definition. There is no clear definition of what functions a “systems management system” performs. The types of devices in the examples typically require Interactive Access to Cyber Assets, and as such are already in scope of the standard based on CIP-005 R2. A network communication centric identification is better suited to these types of assets. Also, it’s not clear how to differentiate a CMS from an EACMS. For example, an Active Directory server seems to fit the definitions of both CMS and EACMS. Should it be designated as both, and if not, which designation should take precedence?

Likes 0	
Dislikes 0	

Response

Scott Downey - Peak Reliability - 1	
Answer	No
Document Name	

Comment
The term "CMS" in this instance is too generic. It would be beneficial to include the specific forms of systems management the SDT intends to include in the standard (patch management, application deployment, virtualiztion management, storage management, and so on), and further, the individual included components of a management system should have requirements tailored to the specific function (see response 7 below).

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 Dominion and ISO-NE	
Answer	No
Document Name	

Comment
Centralized management systems that meet the definition of a BES Cyber Asset would already be identified in the CIP-002 assessment process since they would be Cyber Assets that, if misused, could have a 15-minute impact on the BES.

Defining a new term and including it in the applicability columns of the CIP standards may add additional Cyber Assets to the existing CIP scope. This was not an issue that was identified by FERC. The revisions to the CIP standards caused by this expansion of scope could cause additional delays in the current implementation thereby delaying the security that the standards are meant to insure. We suggest that this term not be included as part of this CIP modification project

If the SDT determines that there is an additional risk associated with the CMS for hypervisor management consoles, this risk should be addressed without pulling in unrelated systems.

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	No
Document Name	

Comment

NRG has concerns that the proposed definition is too broad and includes systems that are beyond the virtual Hypervisor issue.

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 definition is too broad as written, making its intent unclear. If the intent of CMS is to cover hypervisor type technologies the definition should include the word virtual or other reference to management of virtual architecture.

Likes 0	
Dislikes 0	

Response

Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC

Answer	No
Document Name	

Comment
Centralized management systems that meet the definition of a BES Cyber Asset would already be identified in the CIP-002 assessment process since they would be Cyber Assets that, if misused, could have a 15-minute impact on the BES. Defining a new term and including it in the applicability columns of the CIP standards may add additional Cyber Assets to the existing CIP scope. This was not an issue that was identified by FERC. The revisions to the CIP standards caused by this expansion of scope could cause additional delays in the current implementation thereby delaying the security that the standards are meant to insure. We suggest that this term not be included as part of this CIP modification project If the SDT determines that there is an additional risk associated with the CMS for hypervisor management consoles, this risk should be addressed without pulling in unrelated systems.

Likes 0	
Dislikes 0	

Response

Aaron Austin - AEP - 3,5	
Answer	No
Document Name	

Comment
AEP does not support the definition as proposed and is not certain that it is appropriate without indication of the requirements the SDT believes such a definition would be applicable. The definition should be exclusive of Cyber Assets included in the scope of the EACMS definition. Without this exclusivity, entities will be forced to account for all possible combinations of cyber system types.

Likes 0	
Dislikes 0	

Response

Teresa Cantwell - Lower Colorado River Authority - 1,5,6	
Answer	No
Document Name	

Comment
LCRA TSC seeks additional clarification as to what devices are or are not considered CMSs.

Likes 0	
Dislikes 0	

Response

Michael Shaw - Lower Colorado River Authority - 1,5,6	
Answer	No
Document Name	
Comment	
LCRA TSC seeks additional clarification as to what devices are or are not considered CMSs.	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	
See comments for Question 7, below.	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	No
Document Name	
Comment	
It is possible to have virturalized CIP infrastructure that is not part of a BES Cyber system and would still need protections. Examples include EACMS infrastructure and intermediate systems. The SDT should consider the risks posed by vitualized EACMS devices in the CMS definition.	
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 CMS definition and the intent to add CIP requirements to the proposed asset category. First, the proposed CMS definition contains open ended wording subject to broad interpretation by auditors beyond the intent of the SDT. The proposed definition will expand the scope of CIP applicable systems. CenterPoint Energy believes the term should address the intended system explicitly in order to limit scope creep.

Centralized management systems could be in place to provide services to multiple systems within a data center, or enterprise-wide, both in and out of scope for NERC CIP. The required regulatory response of entities to comply with requirements to protect CMS, as yet unwritten, may be much broader than the intent of the SDT. In particular, the addition of patch management systems is a concern. If the CIP Standards dictate how entities deploy patches and restrict the ways this can occur, better solutions will be abandoned in exchange for compliant ones. This has already occurred in response to the malware signature deployment testing requirement. Patch management systems have no place in the CMS definition. Similarly, storage management is a huge area, often managed enterprise-wide. SDT is well advised to focus on protection of data per CIP-011 in storage rather than expanding scope of CIP to cover storage systems as well.

Finally, hypervisors are not listed among the examples even though this term is clearly meant to cover them.

As an aside, the acronym CMS is well-known and used in data centers to refer to a Content Management System and the new acronym might cause confusion.

Likes 0	
Dislikes 0	

Response

Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

Patch management is an act, not a system, and should not be included in the definition. Using the term “management” (systems management, network management, etc.) is much too broad, as it pulls in aspects of management that have no impact on the reliability of the BES. More emphasis should be placed on configuration. There should also be more definition around “administration.” SRP proposes revising the definition to, “A tool used for the configuration, turn-up, or deployment of BES Cyber Systems…”

Likes 0	
Dislikes 0	

Response

Preston Walker - PJM Interconnection, L.L.C. - 2 - SERC,RF

Answer	No

Document Name	
Comment	
PJM suggests adjusting the language to align with the structure of the approved EACMS and PACS definitions: *Cyber Assets that perform administration or configuration of BES Cyber Systems., including systems management, network management, storage management,* or *patch management.*	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1,3,5,6	
Answer	No
Document Name	
Comment	
Exelon is concerned with the proposed definition extending what “Centralized Management Systems” would be in scope for the CIP standards. A definition should focus on virtualization so as not to create confusion since not all centralized management systems are virtualized, and not all virtualized systems are for central management. Exelon understands that the CIP SDT has to refrain from using any specific terms that could identify any one vendor product. One approach the CIP SDT could take, if they believe that there needs to be a definition for the management system, is to use “Virtualization Management System” instead of “Centraized Management System” along with the definition in this posting. This would correctly scope the applicability to not include other “Centrlized Management Systems.”	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	No
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	
In examining virtualization, the SDT considered centralized management systems or consoles for these environments. These systems allow for the mass addition, deletion and modification of virtual machines and networks. Access to the control surface of a cyber system is known as the *management plane*. The management plane is where the virtual infrastructure is configured and managed by a limited group of administrators as opposed to the *data plane*. The data plane is where the end user's access to the virtual machine's business function takes place. To meet the security objective of protecting a BES Cyber System from threats in the data plane, the management plane should be isolated from the data plane. These types of controls are referred to as *out of band* management.	
Likes 0	
Dislikes 0	
Response	
Warren Cross - AEP - 1,3,4,5 - WECC,Texas RE,SERC,SPP RE,RF, Group Name ACES Standards Collaborators	
Answer	Yes
Document Name	
Comment	
Not addressed in v5. Industry must have some guidance as to what is defined and in scope.	
Likes 0	
Dislikes 0	
Response	
Sarah Gasienica - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Centralized Management Systems are a huge issue for NIPSCO OT. We have wrapped a number of our CMS' into EACMS which causes a ton of grief for our operability. These suites of systems require special protections but not the same level as an EACMS. I agree with this definition as it identifies areas that are of significant security concern while potentially minimizing impacts to our operability. NIPSCO OT has taken a conservative approach with our management consoles and made all of them EACMS systems. This causes significant costs and difficult operability for my teams. I would encourage further development on this term and encourage that the requirements are placed somewhere between a TCA and an EACMS.	

Likes 0	
Dislikes 0	
Response	
David Francis - Midcontinent ISO, Inc. - 2 - MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG	
Answer	Yes
Document Name	
Comment	
There has long been uncertainty on how to address these types of assets. Please consider a new name of the term since this acronym is already overly used in different contexts. Please clarify that system health and statistic monitoring is not to be included within this definition.	
Likes 0	
Dislikes 0	
Response	
Lee Maurer - Oncor Electric Delivery - 1	
Answer	Yes
Document Name	
Comment	
There has long been uncertainty on how to address these types of assets. Also, please consider a new name of the term since this acronym is already overly used. Please clarify that system health and statistic monitoring is not to be included in this definition.	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	Yes
Document Name	
Comment	
We support the general concept and approach, but are concerned that the concept, being new and unfamiliar to industry and auditors alike, may end up bringing other, non-CIP systems into scope or otherwise impact non-virtualized BES Cyber Systems. To minimize the risk of unintended consequences,	

we suggest that the scope of a CMS be narrowed to apply only to virtual systems at this time. The expansion of the CMS concept to address risks that may be present in managing physical devices is beyond the SAR of this project.

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 SDT's proposed definition of CMS captures most types of systems that support automation with a large span of control and privileged access. A similar span of control risk exists in that EACMS is a type of CMS for electronic access but the term *EACMS* is specific to NERC CIP and used nowhere else in IT Security or Information Assurance in any other industry. This inherently limits the amount of expertise, guidance, and documentation available for solving the root problem of controlling access to CIP-applicable systems.

BPA recommends that the SDT should retire the NERC CIP defined term *Electronic Access Control & Monitoring System* from the NERC Glossary and adopt the industry solution *Authentication, Authorization, and Accounting* System (AAA System). Non-standard jargon should be avoided when adequate terms and concepts exist already. See link: http://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-35/101-aaa-part1.html

Further, BPA recommends that the SDT should clarify in Guidelines and Technical Basis, that:

- AAA *clients* that subscribe to AAA services (e.g. via a protocol such as LDAP, RADIUS or TACACS+) but do not maintain any account information are not AAA Systems in themselves
- 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

Andrew Gallo - Austin Energy - 1,3,4,5,6

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Harold Sherrill - Sempra - San Diego Gas and Electric - NA - Not Applicable - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - International Transmission Company Holdings Corporation - 2 - MRO,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	
sean erickson - Western Area Power Administration - 1,6	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Mike Smith - Consultant - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
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	

7. Do you agree with the SDT's approach to reference the CMS specifically as a type of applicable system in the CIP standards? Please provide your rationale.

(Refer to the Unofficial Comment Form for more information on this question)

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

Answer	No
Document Name	

Comment

See comments to Question (6)

Likes 0	
Dislikes 0	

Response

Nicholas Lauriat - Network and Security Technologies - 1

Answer	No
Document Name	

Comment

N&ST recognizes there are legitimate security concerns associated with systems used to manage and/or configure BES Cyber Systems and associated EACMS and PACS systems (especially, and for example, network firewalls whose interfaces include one or more EAP). However, N&ST is concerned that the SDT's well-intentioned attempt to define "Centralized Management System" could result in significant pushback from industry and endless arguments about what type of system would meet the proposed definition of "CMS." What does "centralized" mean? It is technically feasible (to borrow a phrase) for a firewall administrator to modify the configuration of multiple firewalls using his or her smartphone. Would doing so render his or her smartphone a CMS? N&ST believes that hypervisors used to create, modify, or remove virtual machines that qualify as BES Cyber Assets should themselves be evaluated as potential BES Cyber Assets or other Cyber Assets subject to CIP requirements, and that the Standards should make this clear. However, N&ST believes that security for other types of devices used for management and configuration in CIP environments is adequately addressed by existing requirements (e.g. CIP-005 requirements for Remote Interactive Access). This opinion is based, in part, on the fact many N&ST clients have chosen to locate systems used for the administration and/or configuration of BES Cyber Systems INSIDE defined ESPs, which makes them Protected Cyber Assets and therefore already subject to many CIP requirements.

Likes 0	
Dislikes 0	

Response

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body

Answer	No

Document Name	
Comment	
It is too soon to tell. The concept is fetching but we would want to see more details.	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	No
Document Name	
Comment	
There are so many ways once in the ESP to negatively affect BES systems. Single out CMS for addition scrutiny seems unnecessarily as all other CIP controls already apply. Potentially for devices that can effect multiple systems simultaneous, more attention could be called for in the area of recovery plans.	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 3,5	
Answer	No
Document Name	
Comment	
The SDT should consider reviewing, revising, or replacing existing definitions of supporting cyber system types to achieve its goal of protecting those centralized cyber systems used to manage BCS or other related cyber systems.	
Likes 0	
Dislikes 0	
Response	
Daniel Grinkevich - Con Ed - Consolidated Edison Co. of New York - 1,3,5,6	
Answer	No

Document Name	
Comment	
We do not think this is necessary if virtualized systems managing BES Cyber Systems are required to stay within the boundaries of an 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 Dominion and ISO-NE	
Answer	No
Document Name	
Comment	
The proposed definition of CMS is more general than just those types of CMS associated with command and control of virtual resource environments. This takes the discussion beyond the scope intended for addressing virtualization technology in the context of CIP. If the SDT decides to include CMS applicability, the definition should be refined to include only virtualization or addressed in a new CIP standards modification project. This type of systems are not addressed in the standard and represent risks that need to be addressed.	
Likes 0	
Dislikes 0	
Response	
Scott Downey - Peak Reliability - 1	
Answer	No
Document Name	
Comment	
There are a myriad of ways to manage systems. Trying to add these definitions now, and bringing those systems into the scope of the CIP standards, would be burdensome on entities, and provide very little risk management. For example, patch management systems frequently have methodologies to ensure that the content of the patch management system has not been tampered with (checksum, digital signatures, and so on). Further, entities very well may rely on logical separation of the management of systems from the user access of systems. Trying to create standards around these types of assets would create confusion and complexity, and not inherently improve security. There would also be overlap with existing definitions in the standards, such as EACM, which could also qualify as a CMS. Instead, focus on which types of management systems should be specifically included in the scope of the standards, and write requirements specific to those assets to ensure the integrity of the CMS, instead of applying the general CIP-007 standards to them. Using the previously referenced patch management system example, a standard for an application deployment or patch management system could be that the system must demonstrate methods to ensure the integrity of deployment packages to endpoints (authorization of deployments, validation of deployment content, and that's it).	

Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	No
Document Name	
Comment	
The types of devices in the examples typically require Interactive Access to Cyber Assets, and as such are already in scope of the standard based on CIP-005 R2. A network communication centric identification is better suited to these types of 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	
See our comments in #6 above. We believe the definition is too broad as written.	
Likes 0	
Dislikes 0	
Response	
Sheranee Nedd - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	No
Document Name	
Comment	
PSEG supports Edison Electric Institute’s and NPCC’s comments.	
Likes 1	PSEG - PSEG Fossil LLC, 5, Kucey Tim
Dislikes 0	

Response
Nathan Mitchell - American Public Power Association - 3,4

Answer	No
Document Name	

Comment
The proposed definition of CMS is more general than just those types of CMS associated with command and control of virtual resource environments. This takes the discussion beyond the scope intended for addressing virtualization technology in the context of CIP. If the SDT decides to include CMS applicability, the definition should be refined to include only virtualization or addressed in a new CIP standards modification project.

Likes 0	
Dislikes 0	

Response
Brandon Cain - Southern Company - Southern Company Services, Inc. - NA - Not Applicable - SERC

Answer	No
Document Name	

Comment
Southern Company does not agree with the SDT's approach to reference the CMS specifically as a type of applicable system in the CIP Standards. As stated in Question 6, CIP-010 change management is being administered for the BES Cyber Systems that are administered through these CMS systems. Also additional clarity would be required for how the definition would be used and why it would be an applicable system different than a PCA or other already in-scope Cyber Asset.

Likes 0	
Dislikes 0	

Response
Joseph Mosher - EDF Renewable Energy - NA - Not Applicable - WECC

Answer	No
Document Name	

Comment
We do not think you should differentiate CMS from EACMS. If anything, you should broaden the definition of an EACMS to include other central management and administration systems. Many of these systems perform both functions, which would only increase ambiguity.

Likes 0	

Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	
Reclamation recommends the SDT consider that some tools (such as CMS) are not critical to the operation of the BES.	
Likes 0	
Dislikes 0	
Response	
Lauren Price - American Transmission Company, LLC - 1	
Answer	No
Document Name	
Comment	
ATC agrees with EEI's comments that it is unclear how this new definition will be used and therefore it is also unclear why it would be referenced as a type of applicable system in the CIP standards.	
Likes 0	
Dislikes 0	
Response	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
It is unclear how this new definition will be used and therefore it is also unclear why it would be referenced as a type of applicable system in the CIP standards.	
Likes 3	Berkshire Hathaway Energy - MidAmerican Energy Co., 1, Harbour Terry; Great Plains Energy - Kansas City Power and Light Co., 1,3,5,6, Webb Douglas; Darnez Gresham, N/A, Gresham Darnez

Dislikes 0	
Response	
Deborah VanDeventer - Edison International - Southern California Edison Company - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
Additional clarification is needed on how this new definition will be used and why it would be referenced as a type of applicable system in the CIP standards. Specific examples are needed to clearly describe the context and how these devices will be used in the CIP environment.	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
In practice, how does the definition of a CMS differ from that of an EACMS? How would the risks be mitigitated differently? Without any clear intent of how the SDT plans to implement a new defition, PacifiCorp cannot support the creation of one.	
Likes 2	Berkshire Hathaway Energy - MidAmerican Energy Co., 1, Harbour Terry; Darnez Gresham, N/A, Gresham Darnez
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	
Kansas City Power and Light supports Edison Electric Institute’s Comments.	
Likes 0	

Dislikes 0	
Response	
Patricia Robertson - BC Hydro and Power Authority - 1,3,5, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
See comments to question 6.	
Likes 0	
Dislikes 0	
Response	
Jeffrey Watkins - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	No
Document Name	
Comment	
It is unclear how this new definition will be used and therefore it is also unclear why it would be referenced as a type of applicable system in the CIP standards.	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	No
Document Name	
Comment	
No, as discussed above, AZPS respectfully submits that the development and creation of additional terms and asset classifications is unnecessary. All cyber assets (physical or virtual) can be classified in existing classification of Cyber Asset if it is modified as recommended in AZPS's response to Question #2. Hence, AZPS does not agree with or support the creation of a new definition for CMS or the use of such a term in the CIP Reliability Standards.	
Likes 0	

Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
The proposed CMS should be classified as its own applicable system to ensure controls specific to those Cyber Assets are required.	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
DOminon agrees that this approach could lessen the risk of misidentifying these types of devices as they have a potential impact to BCSs within 15 minutes of their operation.	
Likes 0	
Dislikes 0	
Response	

Chris Scanlon - Exelon - 1,3,5,6	
Answer	Yes
Document Name	
Comment	

Consistent with Exelon's response to question 6 above, we support specific applicability; however, as long as the definition is sufficiently scoped to only be those "Centralized Management Systems" related to the tools to manage the virtualized environments.

Additionally, the informational posting states that the SDT is concerned with risks to the virtualized environment presented by the use of a centralized management system (CMS) to meet CIP requirements. It would be helpful if the CIP SDT would more fully explain what those risks are and the scope of CMS that require protections. The definition as presented could apply to any CMS used for general administration of existing BES Cyber Systems (e.g., configuration management, patching, etc.). We do not believe the SDT has provided a sufficient reason to extend CIP applicability to all CMSs, especially if those systems do not fall within CIP scope now because they do not qualify as BES Cyber Systems and are not associated with their PCAs, EACMS or PACS. The approach used should be clear in limiting the applicability of the CMS to virtualized environments.

Likes 0	
Dislikes 0	
Response	

Preston Walker - PJM Interconnection, L.L.C. - 2 - SERC,RF	
Answer	Yes
Document Name	
Comment	

This will help reduce confusion over the classification of different types of systems and provide explicit direction for registered entities and auditors.

Likes 0	
Dislikes 0	
Response	

Mike Smith - Consultant - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	

A CMS is a vulnerable asset just like any other in a network, often more so as they are generally designed to be run on private, secured networks and are rarely the focus of as much security testing as other systems.

Likes 0	
Dislikes 0	

Response

Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC

Answer	Yes
Document Name	

Comment

SRP agrees with the SDT's approach to reference the CMS specifically as a type of applicable system in the CIP standards, assuming the SDT develops a clear definition for CMS. It provides clarity to the scope of systems that should be afforded protections but do not necessarily fall under the EACMS definition. SRP suggests adding criteria to determine a CMS and limiting the scope to the BES.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

Clarification is necessary to consider EACMS, intermediate systems and other environments outside of the BES Cyber System.

Likes 0	
Dislikes 0	

Response

Michael Shaw - Lower Colorado River Authority - 1,5,6

Answer	Yes

Document Name	
Comment	
In examining virtualization, the SDT considered centralized management systems or consoles for these environments. These systems allow for the mass addition, deletion and modification of virtual machines and networks. Access to the control surface of a cyber system is known as the *management plane*. The management plane is where the virtual infrastructure is configured and managed by a limited group of administrators as opposed to the *data plane*. The data plane is where the end user's access to the virtual machine's business function takes place. To meet the security objective of protecting a BES Cyber System from threats in the data plane, the management plane should be isolated from the data plane. These types of controls are referred to as *out of band* management. The SDT is considering limiting the scope of management plane protection requirements to high and medium impact Control Centers because these environments contain the highest risk.	
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	
It is the correct approach, but specific requirements need to be added to address the protection and management of CMS. They should be managed similar to EACM.	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - International Transmission Company Holdings Corporation - 2 - MRO,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
While ITC agrees with protecting critical systems that can be compromised to affect the systems they manage, more determination needs to be made carefully regarding the controls for the proposed CMS system.	
Likes 0	

Dislikes 0	

Response

Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	Yes
Document Name	

Comment
This type of systems are not addressed in the standard and represent risks that need to be addressed. In examining virtualization, the SDT considered centralized management systems or consoles for these environments. These systems allow for the mass addition, deletion and modification of virtual machines and networks. Access to the control surface of a cyber system is known as the *management plane*. The management plane is where the virtual infrastructure is configured and managed by a limited group of administrators as opposed to the *data plane*. The data plane is where the end user's access to the virtual machine's business function takes place. To meet the security objective of protecting a BES Cyber System from threats in the data plane, the management plane should be isolated from the data plane. These types of controls are referred to as *out of band* management. The SDT is considering limiting the scope of management plane protection requirements to high and medium impact Control Centers because these environments contain the highest risk.

Likes 0	
Dislikes 0	

Response

Lee Maurer - Oncor Electric Delivery - 1	
Answer	Yes
Document Name	

Comment
Due to their potential impact on the assets they manage, it would be appropriate to have controls identified through requirements.

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes

Document Name	
Comment	
This is an area some Responsible Entities have had difficulty with under the current Standards. Explicitly identifying CMS as a separate system type will provide needed clarity that these systems must be protected.	
Likes 0	
Dislikes 0	
Response	
David Francis - Midcontinent ISO, Inc. - 2 - MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG	
Answer	Yes
Document Name	
Comment	
Due to their potential impact on the assets they manage, it would be appropriate to have controls identified through requirements.	
Likes 0	
Dislikes 0	
Response	
Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	Yes
Document Name	
Comment	
Yes. Agree there are systems that may pose a risk to Cyber Assets if compromised that do not meet the strict definition of EACM. In examining virtualization, the SDT considered centralized management systems or consoles for these environments. These systems allow for the mass addition, deletion and modification of virtual machines and networks. Access to the control surface of a cyber system is known as the *management plane*. The management plane is where the virtual infrastructure is configured and managed by a limited group of administrators as opposed to the *data plane*. The data plane is where the end user's access to the virtual machine's business function takes place. To meet the security objective of protecting a BES Cyber System from threats in the data plane, the management plane should be isolated from the data plane. These types of controls are referred to as *out of band* management. The SDT is considering limiting the scope of management plane protection requirements to high and medium impact Control Centers because these environments contain the highest risk.	
Likes 0	
Dislikes 0	

Response	
Sarah Gasienica - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Centralized Management Systems are a huge issue for NIPSCO OT. We have wrapped a number of our CMS' into EACMS which causes a ton of grief for our operability. These suites of systems require special protections but not the same level as an EACMS. I agree with this definition as it identifies areas that are of significant security concern while potentially minimizing impacts to our operability. NIPSCO OT has taken a conservative approach with our management consoles and made all of them EACMS systems. This causes significant costs and difficult operability for my teams. I would encourage further development on this term and encourage that the requirements are placed somewhere between a TCA and an EACMS.	
Likes 0	
Dislikes 0	
Response	
Warren Cross - AEP - 1,3,4,5 - WECC,Texas RE,SERC,SPP RE,RF, Group Name ACES Standards Collaborators	
Answer	Yes
Document Name	
Comment	
My concern, as stated, is that once you start down this road of including new concepts into a v5 CIP set of standards. Where does it end? I would recommend a fresh start and virtualization only definitions, security control, and auditing that are similar to other industries.	
Likes 0	
Dislikes 0	
Response	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Agree that these sytems represent a systemic risk and it is prudent to reconginze as such. There is concern though regarding what additional controls might be placed on a CMS, specifically their applicablitiy and feasbility given the many different types of CMS that might exist.	
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	
We agree with this approach to require the isolation between the data plane and the management plane. The required separation between the two plans will provide greater security and follows the same principal applied to “Seperation of Duties” concept.	
Likes 0	
Dislikes 0	
Response	
Andrew Gallo - Austin Energy - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
Due to their potential impact on the assets they manage, it is appropriate to have controls identified through requirements.	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	
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	
Harold Sherrill - Sempra - San Diego Gas and Electric - NA - Not Applicable - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Wesley Maurer - Lower Colorado River Authority - 1,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	
Document Name	
Comment	
It is BPA's experience that there are inherent risks in centralized management systems' span of control and privileged access to CIP-applicable Cyber Systems. BPA recommends that this be addressed in support of the security objective of protecting BES Cyber Systems from threats in the data plane by isolation of the management plane (out of band management).	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE recommends the SDT consider adjusting the existing EACMS definition, which has been applied (applicable systems) to the CIP Requirements already.	

Likes 0	
Dislikes 0	
Response	

8. Do you agree with the SDT's approach to require the isolation between the data plane and the management plane? Please provide your rationale.

(Refer to the Unofficial Comment Form for more information on this question)

Jeffrey Watkins - Berkshire Hathaway - NV Energy - 5 - WECC

Answer	No
Document Name	

Comment

The data plane already receives what's considered the highest level or protection in the CIP standards. There would be little gained by separating the data and management planes.

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

Kansas City Power and Light supports Edison Electric Institute's Comments.

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment

The data plan already receives what's considered the highest level of protection in the CIP standards (likely a High Impact ESP). Little would be gained by elevating the protections of the management plane.

Likes 0	

Dislikes 0	
Response	
Deborah VanDeventer - Edison International - Southern California Edison Company - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
Further clarification is needed on the data plane and management terms, and the context in which they will be used.	
Likes 0	
Dislikes 0	
Response	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
The SDT's intent with these new terms is unclear, including how they will be used.	
Likes 3	Berkshire Hathaway Energy - MidAmerican Energy Co., 1, Harbour Terry; Great Plains Energy - Kansas City Power and Light Co., 1,3,5,6, Webb Douglas; Darnez Gresham, N/A, Gresham Darnez
Dislikes 0	
Response	
Wesley Maurer - Lower Colorado River Authority - 1,5,6	
Answer	No
Document Name	
Comment	
LCRA requests a definition of isolation and will then consider and vote accordingly.	
Likes 0	
Dislikes 0	
Response	

Joseph Mosher - EDF Renewable Energy - NA - Not Applicable - WECC	
Answer	No
Document Name	
Comment	
This is good practice. However, this may not always possible with some hardware. So, you should include “per Cyber Asset capability” and possibly allow for TFEs if this is required.	
Likes 0	
Dislikes 0	
Response	
Brandon Cain - Southern Company - Southern Company Services, Inc. - NA - Not Applicable - SERC	
Answer	No
Document Name	
Comment	
Southern Company agrees with the SDT’s approach to require the isolation between the data plane and the management plane, but it is unclear at what level the SDT is asking the question. The data plane and the management plane are isolated by the nature of the configuration of the virtual system and the role authorizations which are provided for each. If the SDT is concerned with network level connectivity and that network access to administrative environments should only occur over separate physical networks or connections, then caution is required as not all systems or Cyber Assets can support physical out of band management. Even if limited to only Control Centers (as in Question 9), not every Cyber Asset in a Control Center can be administered out of band. This goes back to the issue in Question 1 where every requirement is expected to be applied to every device.	
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 in principle, but we cannot agree entirely at this time without more information as to the direction of this approach. More information is needed as to what the SDT means by “isolation” at the physical and virtual level.	
Likes 0	

Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	No
Document Name	
Comment	
This decision should be up to the entity. In-band management may be appropriate in a small environment. Some vendors also require in-band management in their reference architecture. The definition of a CMS includes systems such as patch management servers. Typically these communicate in-band to systems using built-in operating system mechanisms. If included this would involve creating a separate management plane for all systems, and additional work to segregate data and management planes. This architecture may not be supported by EMS vendors. Other devices have only a single network port and the data and management planes cannot be segregated. In some cases management systems are created specifically for high-risk systems. These management systems are treated at the same level and are used in band to manage a small number of devices.	
Likes 0	
Dislikes 0	
Response	
Scott Downey - Peak Reliability - 1	
Answer	No
Document Name	
Comment	
Out of band management is only one way to isolate the management of systems from user access. Dedicated management VLANs and perimeter and host firewall rules are effective at this, for example, and don't require out of band management to be an effective method of securing the administrative functions of a system.	
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 Dominion and ISO-NE	
Answer	No
Document Name	
Comment	

The isolation of the two planes would only make sense in a mixed trust environment. These additional controls should be determined based on the increased risk to the BES due to the management of multiple BES Cyber Systems from a single source. The addition of the controls should not be based solely on the existence of the management plane. If the Entity chooses to not high watermark then the Entity must isolate. This isolation should not be required in all situations.

Virtualization brings new risks. I think this is one of them. These new risks need to be analysed and addressed.

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	No
Document Name	

Comment

NRG disagrees. The management plane should be addressed at the high water-mark. The management plane needs controls but, it doesn't necessarily have to be isolated from the data plane (this would mean that an entity would have to create a separate network). It should be sufficient that the management plane has controls which protect it from the data plane.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

We are concerned that the language would not allow for single plane management if the virtual system resides wholly within an ESP. Also there does not appear to be a distinction between EACMS and BES Cyber System.

We are also concerned that this approach would require entities to build a separate architecture to manage the data plane and management plane.

Likes 0	
Dislikes 0	

Response

Stephanie Burns - International Transmission Company Holdings Corporation - 2 - MRO,SPP RE,RF	
Answer	No
Document Name	
Comment	
The language is too ambiguous to understand the requirements. Out of band management comes with many connotations when it comes to deployment methods. More specificity needs to be provided in the proposed requirement. For example, should console servers be deployed to provide out of band management? Would VLAN separation of management interfaces vs. non-managed interfaces be sufficient? All this is unclear in the proposed language.	
Likes 0	
Dislikes 0	
Response	

Teresa Cantwell - Lower Colorado River Authority - 1,5,6	
Answer	No
Document Name	
Comment	
LCRA TSC requests a definition of isolation and will then consider and vote accordingly.	
Likes 0	
Dislikes 0	
Response	

Michael Shaw - Lower Colorado River Authority - 1,5,6	
Answer	No
Document Name	
Comment	
LCRA TSC requests a definition of isolation and will then consider and vote accordingly.	
Likes 0	
Dislikes 0	
Response	

Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	

N&ST believes that proper separation of end-user and administrative capabilities is important in any information processing context. However, N&ST recommends against trying to develop new data / management plane isolation requirements in virtual environments unless the SDT can (a) reach consensus on a clear definition of what “isolation” means and (b) can identify specific examples, to be included in requirement statements, of approaches to achieving “isolation” that would satisfy the requirement(s).

Likes 0	
Dislikes 0	
Response	

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	

CenterPoint Energy does not support the addition of a new conceptual framework for provision of security controls on a *management plane* and *data plane*. These concepts are new to NERC CIP, with potential for confusion and mis-interpretation by auditors and registered entities, as well as unforeseen special cases that do not fit the binary concept as presented.

Existing security controls applied to hypervisors and VMs are sufficient without the need for a new conceptual framework, through use of the definitions for Cyber Asset, BCS, and PCA including hypervisors, as previously commented. The management and data plane concepts would be useful to publish in guidance, rather than to requirement language. CenterPoint Energy suggests language in the guidance to explain the distinction between access controls to data that is accessible to authorized users of a system versus data isolated in a VM or container with authorized users of its own inaccessible to users of the host.

Likes 0	
Dislikes 0	
Response	

Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	

While out of band management is a good practice, it should not be a requirement. There are other ways to segregate traffic. CIP does not require this for physical systems. If this is not requested for physical systems, then it should not be required for virtual systems. Additionally, the requirement should not be as specific as this may limit future technology. Stating “the data plane should be protected from the management plane” would be an alternative. Having specific ways to do this could be listed in the Guidelines and Technical Basis section.

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion

Answer	No
Document Name	

Comment

The description contained in the document was not clear enough to know the intent of the SDT. Without understanding the potential use of the approach outlined by the SDT, Dominion cannot support such a proposal.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

AZPS believes that the modification of the definition of Cyber Asset, coupled with the existing CIP requirements, affords sufficient differentiation between these planes and, therefore, as requirements become applicable, sufficient isolation – even where the co-mingling of CIP and non-CIP Cyber Assets on the same physical infrastructure – is present.

Likes 0	
Dislikes 0	

Response

Andrew Gallo - Austin Energy - 1,3,4,5,6

Answer	Yes
Document Name	

Comment
Due to their potential impact on the assets they manage, it makes sense to require isolation between the data plane and the management plane. AE requests more guidance on this issue. It is allowable for the management plane and data plan to coexist in the same environment so long as the environment is watermarked to the highest level of either plane.

Likes 0	
Dislikes 0	

Response

David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	

Comment
Clarification is needed if logical isolation is sufficient or if physical isolation is intended here. Either seems prudent however physical might be cost prohibitive for smaller virtualization setups. Perhaps there should be some manner of threshold for when this becomes necessary, for instance when the number of virtual cyber assets is some multiple greater than he underlying phyiscal hosts. One factor that separation of the management and data plane does not address is the additional systemic risk posed by the physical hosts themselves, even with a segregated management plane. For instance, in the most simple case without physical reduancy to illustrate the point, if 10 physical cyber assets are converted to virtual machines on a single physical host, the cyber assets are still "leveraged up" 10:1 to a physical failure or to a direct cyber attack that quite possibly bypasses the management plane. This is a systemic risk not addressed by the data / management plane speration proposal.

Likes 0	
Dislikes 0	

Response

Wendy Center - U.S. Bureau of Reclamation - 1,5	
Answer	Yes
Document Name	

Comment
Reclamation supports the SDT’s approach to the isolation between the data plane and the management plane.

Likes 0	
Dislikes 0	

Response

Warren Cross - AEP - 1,3,4,5 - WECC,Texas RE,SERC,SPP RE,RF, Group Name ACES Standards Collaborators	
Answer	Yes
Document Name	
Comment	
Low impact facilities should not be in scope for virtualization.	
Likes 0	
Dislikes 0	
Response	
Nathan Mitchell - American Public Power Association - 3,4	
Answer	Yes
Document Name	
Comment	
The isolation of the two planes would only make sense if the Cyber Assets in those planes were allowed to different required security controls apart from the associated impact level. These additional controls should be determined based on the increased risk to the BES due to the management of multiple BES Cyber Systems from a single source. The addition of the contols should not be based solely on the existance of the management plane.	
Likes 0	
Dislikes 0	
Response	
Sarah Gasienica - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Yes. NIPSCO OT completed work to separate the management plane of the virtual environment in January 2017. This is a common IT best practice and should certainly be encouraged.	
Likes 0	
Dislikes 0	
Response	

Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	Yes
Document Name	
Comment	
Yes. Conforms with the principle of least privilege.	
Likes 0	
Dislikes 0	
Response	
David Francis - Midcontinent ISO, Inc. - 2 - MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG	
Answer	Yes
Document Name	
Comment	
Due to their potential impact on the assets they manage, it would be appropriate to require isolation. We request more information on this. It is allowable for the management plane and data plan to coexist in the same environment as long as that environment is watermarked to the highest level of either.	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Isolation between the data traffic and the control traffic will improve security, albeit at the cost of added complexity. This tradeoff is probably worthwhile in larger Control Centers, but may not be feasible at the low impact level at this time.	
Likes 0	
Dislikes 0	
Response	

Harold Sherrill - Sempra - San Diego Gas and Electric - NA - Not Applicable - WECC	
Answer	Yes
Document Name	
Comment	
This is appropriate especially if you consider this to be a form of iLo or some other Out of band management (OOBM) function. OOBM functions that touch BES Cyber Assets should have a separate network in the PSP in order to properly secure it.	
Likes 0	
Dislikes 0	
Response	
Lee Maurer - Oncor Electric Delivery - 1	
Answer	Yes
Document Name	
Comment	
Due to their potential impact on the assets they manage, it would be appropriate to require isolation. We request more information on this. It is allowable for the management plane and data plan to coexist in the same environment as long as environment is watermarked to the highest level of either.	
Likes 0	
Dislikes 0	
Response	
RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
SCE&G would like for it to be separated. As an organization, we're currently performing isolation between the data plane and the management plane.	
Likes 0	
Dislikes 0	
Response	
Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC	

Answer	Yes
Document Name	
Comment	
Virtualization brings new risks. I think this is one of them. These new risks need to be analysed and addressed.	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 3,5	
Answer	Yes
Document Name	
Comment	
AEP agrees with that it is appropriate to require isolation between the data plane and management plane. AEP recommends the SDT identify procedural controls related access request and access management practices rather than technical controls which may not be readily demonstrable.	
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	
This is a standard approach to security separation to limit scope and impact	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	Yes
Document Name	

Comment
As indicated in our comment 5, above, we are concerned that some of the concepts and approaches being presented may not reflect the full range and diversity of virtual systems. Please carefully word any requirements to avoid tying obligations to one particular virtualization concept or approach.

Likes 0	
Dislikes 0	

Response

Mike Smith - Consultant - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	

Comment
The risk inherent with the management plane is elevated because of the potential impact of a malicious or non-malicious change to the device. The approach to separate the management and data planes is fundamentally sound. The issue that must be addressed, however, is the implementation used to separate these two planes. For example, utilization of logical separation via VLANs creates an easy and simplistic method for the separation. However, this is not necessarily the most secure method of separation. Likewise, the use of VLANs with a two byte tag to the header is not secure; this tag can be modified by an adversary through various techniques. When looking at the current state of technology and discussing physical separation, what does this imply? For example, if two devices that should be physically separated were to be connected to a SDN switch (e.g., SEL-2740S) there is no 'physical' connectivity between the devices. The switch has no capability to route/forward traffic between these two devices until an appropriate instruction (e.g., Match/Action rule in the case of OpenFlow) is sent to the switch. With SDN technology and SDN Ethernet switches, virtual separation equals physical separation. Language should be clear and concise enough to define a separation between the management and data planes where adversarial techniques cannot cause routing or access of communication between these two planes. Specifically, the language stating OOB (Out of Band) and other technology that allows for the equivalent of OOB. SDN offers the capability to isolate flows within the packet forwarding device (Ethernet switch). In this case, it is not necessary to populate the header or payload of the Ethernet frames with switching isolation data. The SDN switch should have a secure encrypted command channel to the switch's controller to prevent a man-in-the-middle (MiM) type of attack that would allow it to receive instructions from an illegitimate assigned controller. This type of solution allows the use of the same physical network infrastructure and the policy and flow rules of the SDN to create the separation in a highly secure manor.

Likes 0	
Dislikes 0	

Response

Preston Walker - PJM Interconnection, L.L.C. - 2 - SERC,RF	
Answer	Yes
Document Name	

Comment

With the addition of a “where technically feasible” PJM agrees with the SDT’s approach.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

Exelon would like to see this addressed in the Guidance and Technical Basis section. Additional guidance can help by providing examples of data plane vs. management plane and how they could be adequately isolated. We interpret this isolation to include limiting the ability of any data plane to expand permissions into the underlying management plane. This is a standard security control within virtualized system management. There are also vulnerabilities that would constantly challenge this isolation – which could position a compliant solution one day as non-compliant the next.

Intermediate systems and other assets that are not completely located within an ESP benefit from data plane/management plane isolation. However, the systems that are entirely contained within an ESP may not benefit from the isolation at the cost of additional logical and physical complexity to provide that isolation. Any additional guidance should clearly address only the case where a virtualized environment is not completely contained within an ESP, and not imply isolation requirements for systems already contained entirely within an ESP (and protected accordingly).

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

BPA agrees with the SDT’s proposal to require isolation between Data Plane and Management Plane for centralized management systems when system capability allows and risk justifies it. BPA cautions the SDT against overly rigid prescriptions for providing isolation. Combinations of other controls may afford the same or better protection in a particular circumstance. When the use of automated tools can improve security and manageability, it is important to avoid discouraging automation with overly burdensome compliance requirements.

Likes 0	
Dislikes 0	

Response

Patricia Robertson - BC Hydro and Power Authority - 1,3,5, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lauren Price - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sheranee Nedd - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	

Likes 1	PSEG - PSEG Fossil LLC, 5, Kucey Tim
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
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	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

9. Do you agree with limiting the applicability to high and medium impact Control Centers? Please provide your rationale.

(Refer to the Unofficial Comment Form for more information on this question)

Chris Scanlon - Exelon - 1,3,5,6	
Answer	No
Document Name	
Comment	

Exelon generally agrees that the greater risk exists at high and medium Control Centers. However, what is the potential applicability to other medium impact assets where virtualization might be considered? We also suggest addressing how virtualization might allow for the aggregation of multiple Low Impact Systems to the point where there is a much greater potential impact to the BES than from each individual Low Impact device or System.

(Reference this Vulnerability - https://www.theregister.co.uk/2017/03/31/researchers_steal_data_from_shared_cache_of_two_cloud_vms/)

Likes 0	
Dislikes 0	
Response	

Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	No
Document Name	
Comment	

Tri-State would like the SDT to provide more information regarding the use of virtualization on EACMs and PACS. As written, the SDT is only covering assets within the ESP, however, virtualization is also being used for EACMs and PACS systems. We anticipate there will be some requirements to incorporate this type of utilization. Could the SDT please speak to this?

Likes 0	
Dislikes 0	
Response	

Mike Smith - Consultant - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	

SDN's high degree of repeatability drives economic viability in smaller installations. Given that even low-priority installations may be an attack target, it would seem wise to secure them as well.

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

Control centers are certainly important and are the minimum level to include. I would argue that Medium impact sites that utilize virtualization also need to be included as they have isolated impact that is significant. Hence, this should be applied to all High and Medium impact sites and their associated PCAs and EACMs.

Likes 0	
Dislikes 0	

Response

Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC

Answer	No
Document Name	

Comment

The impact level already determines that there are three risk levels, High, Medium and Low. The existence of “external routable connectivity” is an additional qualifier. It seems that the SDT’s plan is to use “Control Center” as another qualifier. It is understood that a Control Center is at a higher risk because of its span of control. This increased risk has already been addressed in the application of the CIP-002-5.1 criteria.

Likes 0	
Dislikes 0	

Response

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

Answer	No

Document Name	
Comment	
No comment on this question.	
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 Dominion and ISO-NE	
Answer	No
Document Name	
Comment	
The impact level already determines that there are three risk levels, High, Medium and Low. The existence of “external routable connectivity” is an additional qualifier. It seems that the SDT’s plan is to use “Control Center” as another qualifier. It is understood that a Control Center is at a higher risk because of its span of control. This increased risk has already been addressed in the application of the CIP-002-5.1 criteria.	
Likes 0	
Dislikes 0	
Response	
Harold Sherrill - Sempra - San Diego Gas and Electric - NA - Not Applicable - WECC	
Answer	No
Document Name	
Comment	
It should also include all high and medium BES Cyber Systems with ERC, not just at control centers.	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	No
Document Name	

Comment
Definitions and frameworks are required to give guidance to all levels of systems. A VLAN management system that manages network devices at many transmission stations should also be in scope of the protection.

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
See our comments to question 8. We agree in principle, but need more information on direction headed before we agree with the approach at this time.

Likes 0	
Dislikes 0	

Response

Nathan Mitchell - American Public Power Association - 3,4	
Answer	No
Document Name	

Comment
The impact level already determines that there are three risk levels, High , medium and low. The existance of “external routable connectivity” is an additional qualifier. It seems that the SDT’s plan is to use “Contol Center” as another qualifier. It is understood that, a Control Center is at higher risk because of its span of control. This increased risk has already been addressed in the application of the CIP-002-5.1 critera.

Likes 0	
Dislikes 0	

Response

Joseph Mosher - EDF Renewable Energy - NA - Not Applicable - WECC	
Answer	No
Document Name	

Comment	
We do not think that this should be required as it is not possible in all situations.	
Likes 0	
Dislikes 0	
Response	
Wesley Maurer - Lower Colorado River Authority - 1,5,6	
Answer	No
Document Name	
Comment	
LCRA feels that applicability should be limited to High Impact Control Centers.	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	No
Document Name	
Comment	
AZPS recommends the SDT provide the industry with clarity on this topic by not limiting the application of virtualization or requirements applicable to virtualized assets to a given BCS type. This will ensure that both the security and reliability objectives of the reliability standards are met and that points of confusion, potential for human error, etc. with respect to virtualization are reduced. AZPS is concerned that the limitation of applicability could introduce complexity, confusion, and ambiguity into the applicability of the requirements to virtualized assets especially where there is co-mingling of CIP and non-CIP assets that have been assigned different impact ratings. For example, if there is a management system that is virtualized across generating units which range from medium impact to non-CIP or low impact or that is virtualized physical locations, the requirements that are applicable to the shared portions of the Cyber Assets may become unclear for both Registered and Regional Entities.	
Likes 0	
Dislikes 0	
Response	

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
BPA agrees with limiting applicability only to those facilities such as High and Medium Control Centers with the highest level of risk is reasonable, and there may be exceptions to those as well. Combinations of other controls may afford the same or better protection in a particular circumstance.	
Likes 0	
Dislikes 0	
Response	

Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
The applicability should be based on risk to the stability of the BES and not an arbitrary classification.	
Likes 0	
Dislikes 0	
Response	

Preston Walker - PJM Interconnection, L.L.C. - 2 - SERC,RF	
Answer	Yes
Document Name	
Comment	
Yes. Low impact BESCS have limited controls already. Not sure how this would fit into their requirements.	
Likes 0	
Dislikes 0	
Response	

Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes

Document Name	
Comment	
Expanding the applicability to medium impact BCS would cause an undue burden on entities and could affect reliability.	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
High and medium impact Control Centers pose the greatest risk to the BES.	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
The impact of the realized threat would not justify the cost in a low impact environment.	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	Yes

Document Name	
Comment	
If isolation standards are put in place, they should be quite limited in scope. Specifically, to where they have had actual, proven effectiveness, and where implementation is not prohibitive in cost and effort when compared to the security gained.	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 3,5	
Answer	Yes
Document Name	
Comment	
AEP agrees that limiting applicability to high and/or medium impact Control Centers is appropriate due to their associated risk. AEP is unclear if the SDT is suggesting that this guidance limit applicability only to BCS or other related Cyber Systems such as EACMS or PACS as they are just as likely to be virtualized.	
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	
NRG does not have any comments on this.	
Likes 0	
Dislikes 0	
Response	
Lee Maurer - Oncor Electric Delivery - 1	
Answer	Yes

Document Name	
Comment	
This should not be applied to low impact due to the lesser risk they present to the BES.	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
See the answer to (8) above.	
Likes 0	
Dislikes 0	
Response	
Sheranee Nedd - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
PSEG supports Edison Electric Institute’s comments.	
Likes 1	PSEG - PSEG Fossil LLC, 5, Kucey Tim
Dislikes 0	
Response	
David Francis - Midcontinent ISO, Inc. - 2 - MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG	
Answer	Yes
Document Name	
Comment	

*It should not be required to apply these m*easures to low impact assets due to the lesser risk they present to the BES.

Likes 0	
Dislikes 0	

Response

Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance

Answer	Yes
Document Name	

Comment

Yes. Agree with risk assessment.

Likes 0	
Dislikes 0	

Response

Sarah Gasienica - NiSource - Northern Indiana Public Service Co. - 1,3,5,6

Answer	Yes
Document Name	

Comment

Yes. The cost of separating management plane traffic is often difficult with equipment rolled out to low impact sites. The risk is typically very minor and the costs are typically significant. The return on investment is just not present and the risks do not justify this need.

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

There is significantly more risk at control centers because of the type of connectivity and number of devices they have that are capable of Multi-Tenancy and out of band management. Enforcing this control at substations would be impractical in many configurations.

Likes 0	
Dislikes 0	

Response

Brandon Cain - Southern Company - Southern Company Services, Inc. - NA - Not Applicable - SERC

Answer	Yes
Document Name	

Comment

Southern Company agrees with limiting the applicability to High and Medium Control Centers. These assets pose the highest risk to the BES and are in the locations with the primary need for virtualization technologies. However, see the issue on Question 8 as location or facility type alone does not mean the technical capability of all Cyber Assets within it are at a certain level.

Likes 0	
Dislikes 0	

Response

Warren Cross - AEP - 1,3,4,5 - WECC,Texas RE,SERC,SPP RE,RF, Group Name ACES Standards Collaborators

Answer	Yes
Document Name	

Comment

Low impact facilities should not be in scope for virtualization. Smaller entities are having a hard enough time adjusting to the current v5 requirements. If a Low impact facility wants to move into a virtual work then that is their option. NERC had been so opposed to virtualization for so long, it will take some time for new comers to the technology to become proficient in supporting it.

Thank you for your time and consideration to comment.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	
Comment	
Reclamation supports limiting the applicability to only high and medium impact Control Centers.	
Likes 0	
Dislikes 0	
Response	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
This seems prudent espeically given this initiative is in the early stages. Adding controls to Low systems might better be kept until after experience with controls on high and medium systems is more developed. However, consideration should be given to situatios where Low Impact BCAs are managed with the same CMS as used for High and Medium BCAs such that controls intended for high and medium related CMS do not unduely carry over as requirements on the managed low impact cyber assets in such cases.	
Likes 0	
Dislikes 0	
Response	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
High and medium impact Control Centers pose the greatest risk to the BES.	
Likes 3	Berkshire Hathaway Energy - MidAmerican Energy Co., 1, Harbour Terry; Great Plains Energy - Kansas City Power and Light Co., 1,3,5,6, Webb Douglas; Darnez Gresham, N/A, Gresham Darnez
Dislikes 0	
Response	

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
These areas carry the greatest level of risk (and are certainly the most likely to see virtualization in use).	
Likes 2	Berkshire Hathaway Energy - MidAmerican Energy Co., 1, Harbour Terry; Darnez Gresham, N/A, Gresham Darnez
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	
Kansas City Power and Light supports Edison Electric Institute’s Comments.	
Likes 0	
Dislikes 0	
Response	

Andrew Gallo - Austin Energy - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
Limiting the applicability to high and medium impact BCSs at Control Centers makes sense due to the lesser risk posed by low impact BCS.	
Likes 0	
Dislikes 0	
Response	

Jeffrey Watkins - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	Yes

Document Name	
Comment	
High and medium impact Control Centers pose the greatest risk to the BES. Medium facilities such as a substation facility will most likely only effect one facility vs. the many facilities managed by a Control Center.	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Shaw - Lower Colorado River Authority - 1,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5,6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - International Transmission Company Holdings Corporation - 2 - MRO,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lauren Price - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Deborah VanDeventer - Edison International - Southern California Edison Company - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Robertson - BC Hydro and Power Authority - 1,3,5, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	