Comment Report

Project Name:	2016-02 Modifications to CIP Standards | Virtualization and Future Technologies: Case for Change White Paper
Comment Period Start Date:	5/30/2019
Comment Period End Date:	6/28/2019
Associated Ballots:	

There were 30 sets of responses, including comments from approximately 84 different people from approximately 61 companies representing 10 of the Industry Segments as shown in the table on the following pages.

Questions

1. Do you agree with the case for change based on the virtualization issues discussed in the white paper? Please provide comments.

2. Do you agree with the proposed path forward as discussed in the white paper? Please provide comments.

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim	1,3,4	RF	FirstEnergy Corporation	Aaron Ghdooshim	FirstEnergy - FirstEnergy Corporation	4	RF
					Aubrey Short	FirstEnergy - FirstEnergy Corporation	1	RF
					Theresa Ciancio	FirstEnergy - FirstEnergy Corporation	3	RF
					Robert Loy	FirstEnergy - FirstEnergy Solutions	5	RF
					Ann Ivanc	FirstEnergy - FirstEnergy Solutions	6	RF
Tennessee Valley Authority	Brian Millard	1,3,5,6	SERC	Tennessee Valley Authority	Kurtz, Bryan G.	Tennessee Valley Authority	1	SERC
					Grant, Ian S.	Tennessee Valley Authority	3	SERC
					Thomas, M. Lee	Tennessee Valley Authority	5	SERC
					Parsons, Marjorie S.	Tennessee Valley Authority	6	SERC
Public Utility District No. 1 of Chelan County	Davis Jelusich	1,3,5,6		Public Utility District No. 1 of Chelan County	Joyce Gundry	Public Utility District No. 1 of Chelan County	3	WECC
					Jeff Kimbell	Public Utility District No. 1 of Chelan County	1	WECC
					Meaghan Connell	Public Utility District No. 1 of Chelan County	5	WECC
					Davis Jelusich	Public Utility District No. 1	6	WECC

						of Chelan County		
ACES Power Marketing	Jodirah Green	1,3,4,5,6	MRO,NA - Not Applicable,RF,SERC,Texas RE,WECC	ACES Standard Collaborations	Bob Solomon	Hoosier Energy Rural Electric Cooperative, Inc.	1	SERC
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Ginger Mercier	Prairie Power , Inc.	1,3	SERC
					Jennifer Bray	Arizona Electric Power Cooperative	1	WECC
					Bill Hutchison	Southern Illinois Power Cooperative	1	SERC
					Patrick Woods	East Kentucky Power Cooperative	1,3	SERC
Duke Energy	Katherine Street	1,3,5,6	FRCC,RF,SERC	Duke Energy	Laura Lee	Duke Energy	1	SERC
					Dale Goodwine	Duke Energy	5	SERC
					Greg Cecil	Duke Energy	6	RF
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	RSC no Dominion	Guy V. Zito	Northeast Power Coordinating Council	10	NPCC
					Randy MacDonald	New Brunswick Power	2	NPCC
					Glen Smith	Entergy Services	4	NPCC
					Brian Robinson	Utility Services	5	NPCC
					Alan Adamson	New York State Reliability Council	7	NPCC
					David Burke	Orange & Rockland Utilities	3	NPCC

Michele Tondalo	UI	1	NPCC
Helen Lainis	IESO	2	NPCC
Michael Jones	National Grid	3	NPCC
Sean Cavote	PSEG	4	NPCC
Kathleen Goodman	ISO-NE	2	NPCC
David Kiguel	Independent	NA - Not Applicable	NPCC
Silvia Mitchell	NextEra Energy - Florida Power and Light Co.	6	NPCC
Paul Malozewski	Hydro One Networks, Inc.	3	NPCC
Gregory Campoli	New York Independent System Operator	2	NPCC
Caroline Dupuis	Hydro Quebec	1	NPCC
Chantal Mazza	Hydro Quebec	2	NPCC
Laura McLeod	NB Power Corporation	5	NPCC
Nick Kowalczyk	Orange and Rockland	1	NPCC
John Hastings	National Grid	1	NPCC
Joel Charlebois	AESI - Acumen Engineered Solutions International Inc.	5	NPCC
Quintin Lee	Eversource Energy	1	NPCC
Mike Cooke	Ontario Power Generation, Inc.	4	NPCC
Salvatore Spagnolo	New York Power Authority	1	NPCC

					Shivaz Chopra	New York Power Authority	5	NPCC
					Michael Forte	Con Ed - Consolidated Edison	4	NPCC
					Dermot Smyth	Con Ed - Consolidated Edison Co. of New York	1	NPCC
					Peter Yost	Con Ed - Consolidated Edison Co. of New York	3	NPCC
					Ashmeet Kaur	Con Ed - Consolidated Edison	5	NPCC
Lower Colorado River Authority	Teresa Cantwell	1,5		LCRA Compliance	Michael Shaw	LCRA	6	Texas RE
					Dixie Wells	LCRA	5	Texas RE
					Teresa Cantwell	LCRA	1	Texas RE

1. Do you agree with the case for change based on the virtualization issues discussed in the white paper? Please provide comments.

Shirley Mayadewi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	No
Document Name	

Comment

We disagree with the case for change based on the virtualization issues.

In our view, except the Cyber Asset definition doesn't clearly include virtual machine, all the cases that are listed in the white paper can be addressed by the current Version CIP standards without significate changes.

The following are our assessments and suggestions for each case in the white paper:

1. Identification of Virtual Cyber Assets

We agree the current Cyber Asset definition doesn't include virtual machines explicitly. Given that any requirements apply to virtual cyber assets should as well as apply to physical cyber assets for the logical consistency, we suggest to modify the Cyber Asset definition to include virtual cyber asset rather than creating a new term "Virtual Cyber Asset", otherwise, the applicable system will become more complicated such as Virtual BCA, Physical BCA , Virtual EACMS and Physical EACMS, etc. We suggest modifying Cyber Asset definition as follows:

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

In addition, we suggest the hypervisor host should be identified as follows:

- the hypervisor host that contains one or more BCAs must be identified as a highest impact level BCA since it meets BCA criteria (deleting a BCA causes 15 minutes adverse impact).
- the hypervisor host that contains one or more EACMS must be identified as an highest impact level EACMS
- the hypervisor host that contains one or more PACS must be identified as an highest impact level PACS
- the hypervisor host that contains one or more BCAs, PCAs and EACMS must be identified as an highest impact level BCAs (high water-marking)

2. Distributed Firewalls vs. Perimeter Models

We haven't seen any challenges for applying current CIP requirements to this case. After VM falls within modified Cyber Asset definition, the Perimeter Model would apply to VM. If SDT thinks the ESP is not enough for the defense in depth and wants to add another layer network access control at an individual asset level (zero trust Model), it would become an expansion of CIP-005 requirements, which has nothing to do with virtualization. If it is allowable for individual VM to have high-level policy based network access control (zero trust Model) without designating perimeter level ESPs, the individual physical cyber asset should be allowable to do so as well (e.g., using local host firewall). In this case, CIP-005 R1.1 will be still applicable and CIP-005 R1.2 needs to be modified as follows for allowing device level network access control as an alternative measure:

"All External Routable Connectivity must be through an identified Electronic Access Point (EAP) or have network access control on each individual applicable Cyber Asset."

Even though virtualization environments can force network access control at more granular levels including by user, process, or certificate and are not limited to only a source/destination IP address of a routable protocol, entities cannot get around the routable connectivity for the virtual networking. Regardless of virtual or physical network environments, routable protocols will be involved since only routable protocols allow devices to communicate between two different networks by forwarding packets between the two networks. Non-routable protocols only use a "device" address, and do not allow messages to be sent from one network to another, thus allowing communications to take place only on a single network. Note that Layer 3 protocols such as IP are often encapsulated in Layer 2 protocols such as Frame Relay, ATM ("Asynchronous Transfer Mode"), and MPLS ("Multiprotocol Label Switching") for delivery of packets to distant networks. When such mechanisms are employed in Layer 2, the IP routable protocol is still in use. Therefore, the routable connectivity and ESP that have been used in current CIP standards are still correct and effective for addressing network access controls in a physical or virtual networking environment. Defining a new term ESZ is unnecessary since it cause more confusing and more unnecessary topology changes unless the project goal is for the defense in depth.

3. Virtualized Firewall Interfaces ('Firewall on a Stick')

We haven't seen any challenges for applying current CIP requirements to this case. This switch with a firewall module can be addressed as follows using the current CIP requirements:

- For the layer 2 switch, If the switch is identified as a BCA, all (virtual and physical) devices are connected to the switch must be within an ESP
- For the layer 3 switch, the virtual firewall or the physical firewall module can be identified as a separate ECAMS containing EAP.
    - If the switch meets BCA criteria, it should be identified as a BCA, otherwise as an EACMS, where all non-BCA devices that are connected to the switch can be segregated by the above firewall.

    Given that the switch with a firewall module is not prohibited by the current CIP requirements, we don't think the new asset classifications such as ESZ and SCI are needed.

    - 4. Virtual Storage Challenges

We haven't seen any challenges for applying current CIP requirements to SAN. Also we disagree the SAN is only related to the CIP-011 information protection since SAN is normally used by a CIP Cyber Asset for the real time operations. Given that virtual or physical SAN like a local hard drive is used for the real time operations of a (virtual or physical) Cyber Asset; it must be treated as part of the Cyber Asset. For instance, if the Cyber Asset is a BCA, the SAN device must be identified as BCA and all BCA requirements would apply. If entities don't want high-water marking the whole SAN as a BCA when the SAN is used in a mixed-trust environment, they should separate the non-BCA SAN for BCA SAN.

5. Management Plane Isolation

We haven't seen any challenges for applying current CIP requirements to management plane. We disagree a shared cyber infrastructure classification is needed. The management plane device should be identified as part of CIP Cyber Asset it manages as follows:

- If the management plane device is used for creating, modifying, or deleting a virtual BCA, it meets BCA criteria (misuse causes 15 minutes adverse impact) and must be identified as a BCA.
- If the management plane device is used for creating, modifying, or deleting a virtual EACMS or PACS, it should be identified as an EACMS or PACS device. For clarifying this identification, we suggest modifying EACMS and PACS definitions to include the management devices as follows:

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

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

The concept of Figure 8 examples is wrong since BCA cannot be identified as an EACMS from the identification methodology perspective. In addition, if the management plane doesn’t meet BCA criteria, it would be a remote client and has to pass through an Intermedia System or identify the management plane itself as an Intermedia System.

6. Privileged Introspection

We haven’t seen any challenges for applying current CIP requirements to privileged introspection. After resolving the identification of Cyber Asset and management plane (see above), the current CIP-007 R3 already written at a security objective level and can work with privileged introspection seamlessly.

7. Remediation VLANs

We haven’t seen any challenges for dealing with remediation VLAN using current CIP requirements. As we described in Section 3), if the virtual firewall or the physical firewall module is identified as a separate ECAMS containing EAP, regardless of whether the switch is identified as a BCA or not, the remediation VLAN that is connected to the switch can be segregated from ESP since the remediation VLAN is not required to be within ESP by the current requirements if the remediation VLAN doesn’t contain any BCAs.

8. Multi-Site Data Center Extensions (Super ESP)

We haven’t seen any challenges for applying current CIP requirements to a super ESP. For the current CIP requirements, if a super ESP is designated across multiple geographic locations, all Cyber Assets within the ESP must be identified as BCAs or PCAs. If a primary control center to a backup control center across town or across the state, the Cyber Assets between two locations within a super ESP may be impossible to be managed as PCAs since some switches and routers may be owned by third parties. In this case, super ESP is not allowed by the current requirements and it is reasonable. Given that Protocol tunneling can explicitly bypass security restrictions and poses a serious challenge to network security, SDT shouldn’t modify the current CIP-005 requirements to allow use tunneling protocols between Control Centers within a super ESP without identifying in-between switches and routers as PCAs for protection.

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer	No
Document Name	2016-02 Virtualization Review - RF Reveiw.docx

Comment

Note - please see attached word version as well as it has pitures which do not show up in this rich text box.

While the whitepaper provides some insightful thoughts on why change may be required, it is trying to create a solution for a problem that does not exist. This paper seems more of a proposal for allowing mixed-mode or mixed-trust environments as opposed to a need for change to accommodate virtualization. The term “shared infrastructure,” in the last paragraph in the Introduction section on page iv seems to hint towards a case for mixed-mode or mixed-trust environments. The term “shared infrastructure,” is not further documented or mentioned throughout the paper nor are it’s benefits communicated in the “Chapter 1: Virtualization Benefits” section. In addition to the concept of shared infrastructure, Figure 1 seems to leave out some critical layers of the conversion including the Hypervisor and network layers which is what logically and sometimes physically manages and connects the layers together as described in my proposed updated figure shown below.

Additionally, all of the benefits specifically listed in the “Chapter 1: Benefits of Virtualization,” section can already be used in the current CIP Standards just not used in a mixed-mode or mixed-trust environments. If all systems are high watermarked within the “shared infrastructure,” along with the proposed techniques and concepts being brought into scope, there would be minimal to no need for change.

Most entities audited to date in the RF footprint understand how a Guest VM should be categorized, with no changes to the current Standards or Requirements. As stated in the Guidelines and Technical Basis for CIP-005 – Electronic Security Perimeters (ESP) are required as a primary defense layer for those BES Cyber Systems (BCS) that may not have inherent cyber security functionality (such as relays, RTUs, or other physical Cyber Assets that would remain unprotected in some of the scenarios presented). In addition, the ESP provides clarity to determine what systems or Cyber Assets are in scope and what requirements they must meet. This does not preclude the use of a Zero Trust Model, but places the burden of compliance (and explanation at audit) on the Responsible Entity wanting to implement said model. Not only is there a burden of compliance, but also an additional burden of implementation and compliance with zero trust model technology on network, server, and security engineers and administrators.

For well over 10 years, most Microsoft, Linux, and Unix based operating systems have the ability to enforce zero trust models through built-in firewalls and application layer firewalls such as but not limited to:

- Microsoft Windows Firewall
- Ipchains
- ipfirewall
- iptables
- Netfiler
- nftables
- Anti-Virus/Anti-Malware vendor tools.

In many instances, these firewall services are disabled due to the complexity of:

- Troubleshooting network or application issues
- Changes in application network behavior from upgrades or patches
- Maintaining the additional amount of host based rulesets individually or through centralized management that would need to be assess per BES Cyber Systems and Cyber Asset.

-
- Whether zero-trust model tools as the ones described above, introspective versions done through a middle-ware layer in virtualization hypervisors, or 3rd generation switches/firewalls are used, these tools will not be a set-and-forget implementation. They will require regular tuning and maintenance, monitored closely through change management and require more documented elements to track and show for baselines and change management. Zero-trust models regardless of virtualization will greatly improve security and would be highly encouraged to do so, but it will require a high degree of monitoring, review, and constant tuning.
-
- Whether a zero-trust model and introspection tools are enforced or not, the underlying hardware supporting both the hypervisor and Guest VM are required for the operation of the Guest VMs, therefore it must be high water marked to the level of highest Applicable System impacted by the loss of associated physical hardware. This argument is the same for the hypervisor – without which the Guest VM cannot function or operate. Ultimately, minor changes to definitions to assist Responsible Entities in identifying and categorizing virtual devices would be beneficial, but not to the degree called for in the white paper and further cautions against mixed-mode and mixed-trust environments.

Many of the techniques and concepts described in the whitepaper are already allowable even though they are not specifically called out in the current standards or guidance. Many of the techniques and concepts could be used as above and beyond compensating controls for Technical Feasibility Exceptions (TFE)s and for Patch Mitigations. Noting these techniques and concepts as requirements for virtualization could preclude them from the use as TFEs and Patch Mitigations.

While virtualization is not specifically defined in the Standards, there is sufficient understanding between the Responsible Entities and CIP Auditors to set expectations and employ professional judgement to support the security of the BES at this time. Admittedly, virtualization will require minor changes in the current definitions to assist Responsible Entities with identifying Cyber Assets and their associated hypervisors and physical hardware, but not to the level outlined in the white paper.

Finally, RF noted that the white paper authors seemed to find extreme examples to include without noting more common layouts and examples that many Responsible Entities have already implemented. A suggestion would be to modify the current white paper to balance the examples presented with examples that Responsible Entities already have in place for further review and discussion.

Likes 0	
Dislikes 0	

Response

Trevor Tidwell - PNM Resources - 1,3 - WECC,Texas RE	
Answer	No
Document Name	

Comment

As the question is overly broad, we will be providing comments broken down for the individual issues.

Identification of Virtual Cyber Asset – YES

PNM Resources agrees that there is a need to allow the Cyber Asset model to apply to virtual machines. There is also a need to identify the shared infrastructure the virtual machines need to function. Furthermore, the standards need to address when a machine has multiple CIP roles. For example, BES Cyber Asset that has only local accounts could also be considered an EACMS. If it has only local accounts is it not also preforming electronic access control? Or does the device high watermark to BCA? The current implementation guidance is not clear on this.

In addition to virtual machines the SDT needs to consider that technology is changing. Virtual machines are a decades old concept, but the standards are far behind at addressing. Today virtual applications or process virtual machines are also a reality. Depending on the implementation the virtual machine hosting the virtual application may be created from a template when the user calls on the application. The virtual machine is then destroyed when the application is closed. This mayfly virtual machine would have a hard time with the current CIP requirements. Yet this is a concept that virtualization allows and yet the white paper doesn't address it.

Distributed Firewalls vs Perimeter Models – NO to the current reason

It is unclear as to why virtualization is driving this change. The white paper states, "This perimeter model is a prescriptive topology, and for many scenarios is still a valid way to perform network security. What may be prescribed, however, for a small network of similar cyber assets may not be ideal for a large network of virtualized BES Cyber Assets." It doesn't consider that it may not be ideal for even a large network of cyber assets. Virtualization may have a use case where the standard needs to allow for the distributed model, but the actual impetus for this is the current standard is overly prescriptive. It doesn't allow for a defense in depth approach. Ideally entities would be using both the perimeter model and each host also protected with its own firewall. The white paper should make it clear that the current standard is preventing a more robust security approach that could apply to non-virtual systems. This is not a virtualization challenge in the NERC CIP Standards, but a challenge of overly prescriptive standards.

Zero Trust Models – NO to the current reason

The white paper does not make much of a case for change when it comes to the Zero Trust Model. Yes, the problem is that if a person gets past the community gate (EAP) and fence (ESP), then they could get into the house (Cyber Asset). This is not a problem with just virtual cyber assets, but physical cyber assets. It is unclear if a Zero Trust Model is required for only virtual cyber assets when physical cyber assets have the same problem. Gated communities exist to provide a second layer of protection. The white paper doesn't make it clear if this is an either-or proposition or if both will be allowed.

Virtualized Firewall Interfaces (‘Firewall on a Stick’) – NO to the current reason

Most of the problems such as the EAP conundrum in the Virtual Firewall Interfaces section are already covered in the Distributed Firewall vs Perimeter Models and Zero Trust Models and addressed by our comments in those sections. The more unique issue brought up in this section is regarding the question if the Network Switch is a BCS, EACMS or both. This concept is one that we have already discussed in our comments regarding Identification of Virtual Cyber Assets. This scenario highlights again that the standards are not clear regarding multi-role devices. Multi-role issues are not unique to virtualization. This is not a virtualization challenge in the NERC CIP Standards, but a potential gap in the current standards that impacts non-virtualized systems as well.

Virtual Storage Challenges – NO to the current reason

The white paper discusses challenges to virtual storage. The example of a Storage Area Network (SAN) or Network Attached Storage (NAS) array could very easily apply to a Redundant Array of Independent Disks (RAID). All entities should be utilizing a RAID on their BES Cyber Assets, so it is unclear why this challenge only comes up with virtual systems. It is unclear what this statement from the whitepaper means, “Additionally, there is no significant benefit to pulling drives from an array to sanitize or destroy them if there is another way to manage this media.” Is this saying that there is problem with CIP-011 when it comes to any disk array like a RAID. If so, does this mean that CIP-011 with regard to disposal or reuse should not apply to individual drives in an array? This is not a virtualization challenge in the NERC CIP Standards, but a challenge of overly prescriptive standards that impacts non-virtualized systems as well.

This topic also discusses de-duplication. This is not just an issue of virtualization. Many backup systems also employ de-duplication since many systems have similar information as described in the white paper. What happens to de-duplicated backups if all the BCAs are retired in a system upgrade, but some systems that share the de-duplicated data remain? Is the backup storage media still containing BCI or not? De-duplication is not just an issue of virtualization. This is not a virtualization challenge in the NERC CIP Standards, but a challenge of overly prescriptive standards that impacts non-virtualized systems as well.

Management Plane Isolation – NO to the current reason

The white paper discusses controlling access to the management plan of virtualized systems because they are logical constructs. However, this is not exclusively a virtualization issue. Many modern Cyber Assets that are servers or appliances have a baseboard management controller. This is the management plane of a physical server. If management plan isolation is an issue, then it an issue under the current standards for existing physical cyber assets. This is not a virtualization challenge in the NERC CIP Standards, but a potential gap in the current standards that impacts non-virtualized systems as well.

Privileged Introspection - NO to the current reason

While privileged introspection is a concept that does not have a physical corollary like some of the other concepts mention in Chapter 2, the paper fails to clearly identify the problem. The problem with “helper VMs” is that they have access to the entire kernel memory of the VMs they are monitoring. This kernel memory is “information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat

to the BES Cyber System." So, the "helper VM" contains BCSI. CIP-011 already requires procedures to protecting and securing handling BCSI including its storage, transit, and use. The "helper VM" is thus a designated storage location of BES Cyber System Information per CIP-004-5 R4.1.3., R4.4, and R5.3. This concept of a storage location isn't even in CIP-011-2, so the objective could be clarified in CIP-011-2 that storage locations of BES Cyber System Information needs to be identified. This is not a virtualization challenge in the NERC CIP Standards, but a potential gap in the current standards that impacts non-virtualized systems as well.

Remediation VLANs – NO to the current reason

The problem brought up in the white paper regarding adding a Cyber Asset under CIP-010 R3.3 is not unique to virtual systems. Virtual images can be physically moved from a non-production environment to the production environment using Removal Media just as a physical device is moved from non-production environment to the production environment. The concept of a remediation VLAN is misconstrued in the white paper. A limited VLAN with restricted network visibility can be setup for physical Cyber Assets so they can be assessed for vulnerabilities, update itself, and apply security controls to become compliant. The issue of the VLAN being inside the ESP or a separate ESP is the same. The remediation part only comes in when a machine becomes non-compliant and it is moved to the remediation VLAN. Any network switch utilizing Network Access Control can accomplish this. This is not only possible with virtualization. This is not a virtualization challenge in the NERC CIP Standards, but a challenge of overly prescriptive standards that impacts non-virtualized systems as well.

Multi-Site Data Center Extensions (Super ESP) - YES

While the problem of Super ESP is introduced with a virtualization use case the reality is that the problem is anytime an entity stretches the layer 2 LAN across a WAN. At least the white paper in the last sentence of the section recognizes that the problem is not with virtualization, but prescriptive CIP standards that do not allow security measure that could achieve the security objective to be located somewhere.

Summary

PNM Resources does not see the challenges as being issues brought about by virtualization. Instead the problem is prescriptive standards that do not allow for other means to accomplish security objectives. Virtualization just happens to be the current technology that has revealed the prescriptive approach to cyber security is broken. It is to slow to change and the actual case for change is prescriptive standards don't allow for future methods to be easily applied and remain compliant. The standards drafting process is too slow to keep adjusting every time best practices for cyber security change. The white paper is "Virtualization and Future Technologies" yet future technologies is only referred to once in the document. The issue isn't even virtualization. The problem is the standards have prescribed best practices as a particular point in time. However, technology of how tasks are done is changing and with it is the technology of how to secure it. What isn't changing as much are the objectives of security which is discussed more in response to question #2.

Likes 0	
Dislikes 0	
Response	
Leanna Lamatrice - AEP - 3,5	
Answer	Yes

Document Name	
Comment	
AEP supports the efforts of the SDT to change or add definitions and requirements related to the application of virtualization technology to an objective level; making the language describe “what” is required not “how” it is to be implemented. The danger is that the requirement language may be too broad thereby adding to the compliance burden and making compliance assessment more difficult or; too specific such that it excludes viable security solutions. AEP requests the SDT take the time necessary to find that “just right” language that creates the desirable outcomes and avoids unintended consequences.	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
TVA concurs that the current model does not cover virtual cyber asset requirements.	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 1,5	
Answer	Yes

Document Name	
Comment	
Reclamation supports modifications to the CIP standards to future-proof the standards and allow for changing technologies. The proposed approach will benefit industry by allowing entities to achieve compliance while protecting their BES Cyber Systems regardless of the composition of the BCS. Reclamation supports a less prescriptive and more objective-based security framework that allows entities to define their systems at the level that makes sense for a situation. Reclamation recommends the SDT clarify the usage of “(compute, network, storage)” on page 3 of the white paper. Reclamation also recommends a more thorough quality review of the white paper to correct typographical errors throughout the document.	
Likes 0	
Dislikes 0	
Response	
Alex Ybarra - Public Utility District No. 2 of Grant County, Washington - 1,4,5,6	
Answer	Yes
Document Name	
Comment	
No Comments	
Likes 0	
Dislikes 0	
Response	
Davis Jelusich - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Public Utility District No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
CHPD agrees with the case and appreciates the thorough explanation provided by the SDT.	
Likes 0	
Dislikes 0	
Response	
Line Dufour - Hydro-Qu?bec Production - NA - Not Applicable - NPCC	

Answer	Yes
Document Name	
Comment	
No comments.	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Idaho Power agrees there is a need for virtualization. The current CIP standards don't translate well to current uses of several valuable technologies that include those that rely on virtualization.	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Network and Security Technologies - 1 - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
N&ST considers it reasonable to calll attention to virtualization's potential benefits, but only up to a point, and we consider the WP's negative comments about many current CIP implementations (e.g., Fig. 4 "Perimeter Based Model" is characterized as "Not aligned with current security best practices") to be needlessly pejorative. Moreover the WP: - makes several assertions that N&ST considers inaccurate, such as the suggestion that multi-site ESPs and the current Standards are incompatible, - pays fairly little attention to the issue of how compliance with current or modified CIP Standards could be demonstrated, and - does not directly address the question N&ST believes entities have found most nettlesome, which is whether it is allowable for CIP and non-CIP VMs, managed by a single hypervisor, to coexist on a shared hardware platform and, if so, what conditions would have to be satisfied.	

These concerns notwithstanding, N&ST agrees with the WP's main premise, which is that the Standards, along with several current definitions such as "Cyber Asset," should be updated to accommodate entity implementations that are partially or even entirely based on virtual systems. N&ST also strongly supports the goal that any and all revisions should be developed in a manner that fully supports "backward compatibility" and does not compel entities with no major technology updates on their planning calendars to revise their existing set of CIP policies, plans, and procedures.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

No additional comments.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

EEI member companies generally agree that the SDT has provided a clear and concise case for change based on the virtualization issues identified within their white paper. We recognize that steps need to be taken to provide a path forward for those entities that see reliability and security benefits in virtualization technologies while not disrupting the compliance programs of others. EEI appreciates the direction described in the white paper and support the SDT's current, more moderate approach, which we believe will better ensure broader industry acceptance of the changes being proposed. However, more work is needed to identify the security risks associated with virtualization and address methods to mitigate those risks to ensure continued BES reliability and security. We also note that while cloud computing is not directly addressed in the white paper, the document should be clear that the SDT's approach is not seeking to enable the use of off-premise third party cloud platforms for BES system operations (e.g., Supervisory Control and Data Acquisition (SCADA)).

EEI member companies would also like to take this opportunity to commend NERC and the SDT on the proposed direct described in the white paper while also encouraging NERC's long term objective of transforming the NERC CIP Reliability Standards into a body of standards that more closely conform to the results-based standards concept that currently drives all other NERC Reliability Standards. Still, EEI believes that the drafting team has selected the right path for this current effort.

Likes 0	
Dislikes 0	

Response

Barry Lawson - National Rural Electric Cooperative Association - 3,4	
Answer	Yes
Document Name	

Comment
In the white paper, and Q9 in the Q&A document, it's unclear whether the SDT is treating a Storage Area Nework (SAN) as a separate BES Cyber Asset (BCA) or only as a BES Cyber System Information (BCSI) storage location. NRECA requests that the SDT clarify this going forward. NRECA recommends that the SDT be congnizant of the layering that can occur through virtualization, especially if the CIP requirements are already applying to the hardware. In this situation, any new requirements applying to virtual devices on that hardware should be limited or non-existent. The current CIP standards are unclear as to whether a programmable electronic device definition can exclude a virtual machine. NRECA recommends that the SDT take this into consideration while drafting new or revised requirements.

Likes 0	
Dislikes 0	

Response

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

Comment
We agree with the case for change for virtualization and classification of such assets. The suggested changes will allow entities to be much clear in classifying a Cyber Asset.

Likes 0	
Dislikes 0	

Response

Kagen DelRio - North Carolina Electric Membership Corporation - 3,4,5 - SERC	
Answer	Yes
Document Name	

Comment

NCEMC Agrees with the comments submitted by NRECA	
Likes 0	
Dislikes 0	
Response	
Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Seattle City Light finds the white paper to be an excellent summary of the technological evolution in virtualized systems and the challenges the standards drafting body faces in updating the standards to accommodate that evolution. We were very impressed by how well the technical concepts of virtualization were described for a non-technical audience and how they were cross-referenced to the existing physical asset-centric approach of the current standards. The Q&A document illustrated that, as good as the white paper was, there is still work to be done to help the industry not lose sight of the forest for the trees.	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
ERCOT requests that the SDT make clear whether the implementations referenced are for on-premises solutions only. If the intent is to include cloud provisions, that should be articulated specifically. There is a lot of dispute about cloud solutions for BES Cyber Systems and other asset types subject to NERC CIP Standards that may not make this the right venue to address and achieve a timely solution as noted in the paper. More concrete work is needed by NERC related to cloud services before it is appropriate to include those issues. Many of the concepts documented in the paper also apply to physical systems. The paper points out some significant vulnerabilities with current implementation. ERCOT requests that the SDT look at these issues as well as the virtualization issues to ensure that gaps are addressed with legacy systems.	
Likes 0	

Dislikes 0	

Response

Katherine Street - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	

Comment
Systems and technologies supporting Control Centers, where IT-based solutions are prevalent, are rapidly evolving beyond concepts that are foundational to the current NERC CIP Reliability Standards. Multiple vendors have indicated intentions to fully virtualize their offerings in the next few years, and hardware suppliers are hinting that the traditional rack-mount physical server will no longer be an option in the future. The SDT's case for change focuses on virtualization, but the concepts discussed apply to future-proofed network technologies that provide higher resiliency and flexibility for critical communication flows and to server hardware as it becomes hyper-converged with multiple individually-programmable components inside. The NERC CIP Reliability Standards must evolve to support these technology advances. Although some lag behind bleeding edge tech is expected regulatory standards should not preclude the use of resources that are generally available and meet security objectives, such that entities are forced to turn to grey-market sourcing in an effort to obtain compliant resources.

Likes 0	
Dislikes 0	

Response

Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5	
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	
Jonathan Robbins - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4, Group Name FirstEnergy Corporation	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE appreciates the standard drafting team's (SDT) effort to align the NERC Reliability Standards within the current technology. Texas RE agrees with the following concepts described in the white paper:	

- Identification of Virtual Cyber Assets: Texas RE believes providing clarity on how to identify and categorize Virtual Cyber Assets to ensure consistency across all regions would be beneficial for the industry.
- Virtual Storage Challenges: Texas RE agrees that with the proposed changes to CIP-011-2 R2 there may be difficulties proving compliance in a virtualized storage environment.
- Remediation VLANs: While it is technically possible to comply with CIP-010-2 R3.3 in a virtualized environment Texas RE recognizes that additional clarity on how to deploy this technology in a secure and compliant manner would benefit the industry.

The white paper appears to argue that certain components of virtualization are not possible due to the way the standards are written. While Texas RE agrees there could be additional clarity and specific mention of virtual machines, nothing prevents entities from implementing the following:

- Distributed firewalls: Perimeter controls would also need to be deployed to meet CIP compliance, however this existence of perimeter controls does not prevent entities from deploying additional controls.
- Zero Trust Models: Perimeter controls would also need to be deployed to meet CIP compliance, however this existence of perimeter controls does not prevent entities from deploying additional controls.
- Management Plane Isolation: Entities are capable of deploying secure management plane communications today.
- Privileged Introspection: CIP-007-6 R3.1 states “Deploy method(s) to deter, detect, or prevent malicious code.” An entity using privileged introspection would only need to document that this is their method of deterring, detecting, or preventing malicious code. The SDT also stated that this technology would require grouping VM’s protected by privileged introspection into a particular BES Cyber System. Texas RE is unsure why the SDT believes this to be the necessary.

Texas RE suggests that the discussion surrounding Multi-Site Data Center Extensions (Super ESP) is applicable to all Super ESPs, and is not a change specifically necessary for the standards to be able to successfully address virtualization.

Additionally, Texas RE is concerned with a mixed-trust environment. Due to the parent child relationship between host and virtual machine, you can never fully eliminate impacts a VM could have on other VM’s and the host.

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

Answer	
Document Name	

Comment

At the executive level – 1) Expect the SDT to provide virtualization benefits; 2) Request the SDT also provide virtualization challenges – operational, cyber security and compliance.

We are concerned that moving to “security objectives” will significantly impact auditors, starting with their training.

Chapter 2 is an excellent start to the conversation of challenges in moving CIP to a virtualization

Likes 0	
Dislikes 0	

Response

2. Do you agree with the proposed path forward as discussed in the white paper? Please provide comments.

Trevor Tidwell - PNM Resources - 1,3 - WECC,Texas RE	
Answer	No
Document Name	

Comment

The path forward should be more requirements focused on an objective and meeting that objective. Allow the entity to define how it is meeting the objective, so that it can be changed as security technologies change, but the objectives generally do not change as much over time. New threat vectors may arise and necessitate a change to the standards to add a new objective, but that is easier to achieve than rewrite the prescription on how to stay compliant.

The reason for the no vote is for two reasons. The first is that the proposed path forward isn't entirely clear. While the whitepaper appears to be suggesting that the path forward is more objective than prescriptive, it is short on detail. It gives only one example and would be better off with a couple of more if the intent is to truly move to objective level rather than prescribing the method of meeting the objective. In a world of Advanced Persistent Threats, we need to move to an objective model. While the threats are persistent, they are not static. Industry best practices typically are our defense playbook. These threats adapt to the playbook and find new ways defeat it. As a result, technology and practices used by industry change in response. Yet the security objectives remain the same, but the means of doing so have changed. Writing the NERC CIP Standards to mimic today's best practices do not allow industry to have the ability to adapt when those practices change. As a result, Entities are potentially more exposed to a threat because a new security method doesn't fit the prescription imposed on it. Technology is always changing and writing a prescription for security methods today and attempting to look to the future is a fool's errand. We cannot image today what technology will be like in 5 to 10 years. However, we can foresee what the security objectives are. It is much like war where the objectives are the same, but over the centuries the tools of warfare have greatly changed how you achieve those objectives.

The second reason for the no vote is that the current path forward does not address defense in depth. For example, if an entity implemented both a perimeter and distributed firewalls and had a failure of a perimeter control, but all the devices in the ESP had some compensating control that mitigated the risk of the failure then that should not be a violation of the standards. While one method of achieving the security, objective failed another remained in place. This would help encourage defense in depth if entities could have multiple controls that met the security objective if they could also mitigate risk of non-compliance. To be clear this would be multiple independent controls capable of meeting the security objective where failure of one doesn't result in failure of the other. It is not saying that an entity could have many controls with interdependency of meeting the security objective where a failure of one control results in a failure to meet the objective.

In summary, PNM Resources would encourage the drafting team to think of what the objectives are then rewrite the standards with those in mind. Do not try to keep the current framework as it is broken when trying to adapt to new technology. While this effort discusses virtualization, the reality cloud computing has resulted in a new effort on CIP-011. Thus, the current prescriptive paradigm needs to move to an objective paradigm where an SDT isn't formed with every new emerging technology. We would encourage the SDT to develop this new framework then map the old requirements to the new objective-based framework. Not everyone may appreciate another major paradigm shift with CIP. However, if the SDT can put out a good draft product of revised standards and framing it as more objective standards and less prescriptive standards are the right way to go, then the rest of the industry will hopefully agree. The SDT needs to stop framing this as a virtualization problem since many are already virtualized under v5. The problem is overly prescriptive standards preventing Entities from being able to change the methods of accomplishing the security objective in a compliant manner.

Likes 0	

Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	

While there may be some credence to modifying the definitions of what a BES Cyber Asset is to better accommodate virtual environments (see discussion above), for the most part, the Responsible Entities that RF audits correctly identify and protect Guest VMs, hypervisors, and supporting physical hardware. The Responsible Entities do not identify Guest VMs as “software” but as BES Cyber Assets, Protected Cyber Assets (PCA), or BES Cyber Systems (BCS). RF does not agree that Guest VMs are specifically excluded from the current CIP-007 Requirements as stated in Figure 2 on page 3.

Admittedly, there is a 1:1 relationship assumed between BES Cyber Assets and their underlying hardware, however, minor changes to current definitions will support one-to-many relationships afforded in VM environments without creating new asset classes.

The argument put forth under “Distributed Firewalls vs. Perimeter Models” on page 4 is already possible as mentioned above. Entities can choose to identify and protect each BCA in their own separate ESP, with their own separate EAP, under the current CIP Standards. While virtualization may reduce the amount of time and effort to implement such an environment, maintaining it with a high degree of confidence that it is performing as designed, and then explaining this environment to an outside auditor could prove challenging.

Further, current “Next Generation” firewalls are fully capable of limiting network access into and out of the ESP across most layers of the OSI model through security zones. Figure 4 compares Perimeter-based and Zero-Trust models, and as most Cyber Assets use the same LDAP or Active Directory (AD) access, the Zero-Trust model is not as secure as portrayed – unless there is the same granularity implemented within the AD or LDAP environment for Groups or ACL Sets and incorporated in the Guest VMs security group.

Remediation VLANs, as shown in Figure 10 on page 10, would be considered “above and beyond” the CIP Standards and would earn a Responsible Entity a Positive Observation, showing strong internal controls for patch management and malware detection.

RF already identifies Super-ESPs (mentioned on page10) and has multiple entities that have currently implemented and support these extended ESPs. There are no additional requirements or changes required for this to be implemented.

Best practices support rings of security in a “defense-in-depth” model that creates tighter security controls the closer you get to key systems. Access control applied at deeper levels as described within the white paper on page 13 does not require virtualization, but at the discretion of the Responsible Entity can be done through a combination of firewall rulesets or security zones, intelligent switches with ACLs or zones, host firewalls, Group Membership (AD), ACL Sets (LDAP), and individual Cyber Asset malware detection.

Regardless of what the paper calls “Shared Infrastructure,” there does not need to be new asset classes, as any new asset classes would still require identification at the high water mark to the level of highest Applicable System the Cyber Assets are controlling access within a distinct ESP. CIP definition changes to include “per device capability” would allow leeway for the auditors to have a conversation and draw conclusions based on professional judgment based on the story the Responsible Entity tells.

Conclusion

RF as a region supports virtualization; however, all supporting hypervisors and underlying physical hardware must be included and categorized correctly. Much in the same way that a network switch within the ESP cannot operate in mixed-mode, neither can Guest VMs that are categorized as PCA, BCA or part of a BCS operate in a mixed-mode environment with non-CIP Guest VMs. Only those Applicable Systems outside of the identified ESP – PACS and EACMS – may operate in a mixed-mode environment; and the underlying hypervisor and physical Cyber Assets must be protected as either a PACS, EACMS, or both – if both are running as Guest VMs.

Using virtualization completely within the ESP – or outside of the ESP for EACMS and PACS – leverages virtualization and captures many of the benefits while limiting the changes required to meet current or future CIP Standards and Requirements.

Likes 0	
Dislikes 0	

Response

Shirley Mayadewi - Manitoba Hydro - 1,3,5,6 - MRO

Answer	No
Document Name	

Comment

We disagree with the proposed path forward as discussed in the white paper. In our view, current CIP requirements can apply to virtualization environment smoothly without significant changes. Given that the CIP compliance program today works fairly smoothly by implementing the existing requirements, any changes of requirements and definitions beyond virtualization shouldn’t be targeted. SDT should focus on how to resolve CIP compliance in the virtualization environment without prohibiting the new technology rather than try to change the requirements for the defense in depth since it is not the driver for this project. Resulting from our comments in the above question 1, as long as the Cyber Asset definition are modified to include VM, most of existing CIP V5 requirements would apply to virtualization environment seamlessly.

Likes 0	
Dislikes 0	

Response

Teresa Cantwell - Lower Colorado River Authority - 1,5, Group Name LCRA Compliance	
Answer	No
Document Name	

Comment

The path forward is needed. However, two items are of concern from this statement:

A literal use of this foundational definition would mean a server hardware platform may be a BES Cyber System, the hypervisor software could be the "operating system", and all the virtual machines running on the hardware are applications or simply data.

1. It should be clear of the differences between an operating system and an application. NIST provides the following definitions.

Operating system: A computer program, implemented in either software or firmware, which acts as an intermediary between users of a computer and the computer hardware. The purpose of an operating system is to provide an environment in which a user can execute applications.

Application: A system for collecting, saving, processing, and presenting data by means of a computer. The term application is generally used when referring to a component of software that can be executed. The terms application and software application are often used synonymously.

The OS can prevent or allow the application to run, but not necessarily vice versa. A clear hierarchy is created. The hypervisor is then above both the OS and application for each VM instance and holds primary control. Therefore, it is recommended that changes to the CIP Standards have three clear tiers when addressing virtual environments to include 1) hypervisor, 2) VMs and OSs, and 3) applications. VMs/OSs and applications should not be grouped together.

2. With all the current discussions on BES Cyber Information and controls used to protect it in cloud environments, the SDT should use caution when using the word "data". Data is not useable until it is information. The SDT may have the opportunity to also address this issue as encryption, where information is turned to data, may be used in virtual environments.

Likes 0	
Dislikes 0	

Response

Katherine Street - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	

Comment

The path forward is reasonable given that current popular uses of virtualization technologies do not provide substantial direct benefits to many of the field systems that must comply with the NERC CIP Reliability Standards. Nonetheless Reliability Standards drafters, Registered Entities, Compliance

Auditors, and other stakeholders must have clarity and regulatory certainty regarding how newly proposed defined terms function in relation to current NERC Glossary of Terms Used in Reliability Standards definitions. The questions noted in the White Paper with respect to the Shared Infrastructure's possible 15-minute impact are indicative of the questions that will arise if the standards do not clearly address how to classify a given "asset" when multiple definitions align with that asset's function. Of particular concern is Shared Infrastructure supporting exclusively EACMS and PACS devices. There is no 15-minute impact question in this scenario, but if the Shared Infrastructure definition assumes a need for BCA-level protections, entities will be forced to add protections not otherwise anticipated for those environments. Similarly, the NERC Reliability Standards must provide Compliance Auditors and Registered Entities clear parameters for assessing regulatory compliance where Shared Infrastructure supports Virtual Cyber Assets that would be classified differently under current rules. For example, would a virtual BCA and virtual PACS be allowed to reside on the same Shared Infrastructure with different network protections deployed (one requiring an "ESP" and one not)? We support the SDT's efforts to develop the new NERC Glossary of Terms Used in Reliability Standards definitions, and look forward to working through these complex issues to arrive at a sustainable approach compatible with evolving technologies.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

Virtualized Firewall Interfaces: ERCOT questions whether the use of the term "firewall" is too specific. More generic terms should be used to allow for other device types that provide this security capability. If the concept of an EAP is maintained, this could result in a one-to-one definition of EAP to Cyber Asset. ERCOT requests consideration of how to define the access points without too much of an administrative burden.

Management Plane Isolation: ERCOT requests that "per asset capability" be included and added to requirements related to management plane isolation.

Multi-Site Data Center Extensions (Super ESP): ERCOT requests that any future requirements related to this subject be aligned to complement and not conflict with or extend the requirements of CIP-012.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

Seattle City Light generally agrees with the proposed path forward. In particular, we like the direction headed with the new “no trust” model.

We remain concerned about maintaining backward compatibility with existing CIP standard language and terminology, and encourage that, at least in certain cases (if not throughout all CIP requirement), the SDT consider use of “overlay” requirement language that accommodates virtualization approaches while also maintaining existing language and terms (i.e., give an entity the option to choose between the existing requirement—perhaps revised to focus on risk and result rather than prescriptive approach—and a new, alternative requirement for a virtualized system. This option would exist on a system-by-system basis).

We also are concerned that the virtualized shared storage (SAN) concepts require a closer look, in terms of treatment under CIP requirements. This area might be ideal for use of the virtualization “overlay” approach discussed above.

Likes 0	
Dislikes 0	

Response

Kagen DelRio - North Carolina Electric Membership Corporation - 3,4,5 - SERC

Answer	Yes
Document Name	

Comment

NCEMC Agrees with the comments submitted by NRECA

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

Answer	Yes
Document Name	

Comment

Our concern is that although the example (figure 12) follows the model given it does not represent the complexity under which the industry has implemented CIPv5

We request the SDT post updates to CIP-007 and CIP-010 sooner. Those Requirements are the biggest hurdles. The industry and SDT will quickly see if the new Requirements will be acceptable

We support the proposed creation of new “shared infrastructure” and “virtual machine” cyber asset types and new “objective-based” type requirements specifically for those virtual cyber assets (as per Chapter 3) which would allow entities to adopt virtualization incrementally and at their discretion without changing existing CIP programs for entities that choose not to adopt virtualization.

We request the SDT to describe how they plan to address mixed-use environments (hardware resources shared between CIP and non-CIP virtual machines)

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

While we are in favor of the proposed path forward, we feel like there is not enough evidence zero trust, software defined networking, and or other similar technologies are more reliable, less expensive, easier to manage, and provide better security in real-time controls networks ie: SCADA, DCS, ICS. These cybersecurity tools have been developed for rapidly changing IT envrionments and for highly exposed, high risk Cyber Assets. BES Cyber Systems are neither of those.

We feel the SDT should focus on the changes to virtualization in the two first bullet points in the whitepaper’s conclusion and let the “Virtualized Network” security product industry mature before changing the standard. We realize the standard is prescriptive in it’s nature around electronic border security, but does not preclude an entity from using other technologies to protect Cyber Assets discussed in the paper such as Management Plane Isolation, Privileged Introspection, etc.

Border firewalls are still considered a best practice and the cost of having a border firewall should not be considered “purchasing extra hardware to show compliance with prescribed technologies”. Firewalls are still a corner stone of protecting networks against attacks and modern firewalls are no longer confined to layer 3 of the OSI model. The standards require and EAP, but that does not preclude an entity from employing more protective and restrictive controls than the standard requires such as Next Generation Firewalls which operate up to Layer 7 of the OSI model and integrate with Identity and Access Management controls. If FERC and or NERC feel the modern threat landscape requires more granular controls then new requirements are warranted.

Likes 0	
Dislikes 0	

Response

Barry Lawson - National Rural Electric Cooperative Association - 3,4

Answer	Yes
Document Name	

Comment

NRECA appreciates the efforts of the SDT in addressing the complex but important issue of virtualization in the CIP standards.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

We do like the initial path that you have discussed and would like to see more information on:

a. direction and clarification on the Shared Storage and Shared Networks

b. examples of “access control at a deeper level”

Also, the webinars that were put together have been very helpful. We encourage you to continue to use them as an informative tool to illustrate your plan.

Finally, we feel it is important to reiterate that if an entity does not elect to leverage virtualized technologies, then they should not need to alter their programs at all to maintain compliance to any of the CIP requirements.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

EEI supports the path forward as described in the Virtualization white paper, which aligns well with EEI comments provided in December 2018 to the SDT. As stated in those comments, EEI urged the SDT “to focus more on how virtualization might be effectively integrated into BES Cyber Systems, under the current standards, rather than trying to solve all these issues at an early stage of industry adoption.” As a result, we are encouraged by the proposed concept as described but also recognize that much work remains, conceding that many of the concepts will need to be developed in greater detail and vetted by the industry. However, we believe that the SDT has proposed a concept that EEI member companies can support and look forward to reviewing and providing comments that align with the direction described in the white paper.

Likes 0	

Dislikes 0	
Response	
Neil Swearingen - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
No additional comments.	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Network and Security Technologies - 1 - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
N&ST recommends the frequent involvement of representatives from Regional Entity Compliance Monitoring and Enforcement groups, as audit approaches for virtualized CIP environments are likely to be significantly different than for non-virtualized environments.	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Idaho Power believes the proposed path forward appears to be an appealing approach. However, due to the amount of significant changes that will occur as a result of this approach, it appears that the proposed path forward could result in significant increases to a Responsible Entity's overhead costs and associated resources. In addition, when any newly approved CIP standard becomes effective, Responsible Entities require long lead times to plan, interpret, document, and implement changes into their compliance programs and processes in order to have a suitable and sustainable compliance program associated with the new CIP standard. At minimum, a 24-month implementation plan should be considered.	

Likes 0	
Dislikes 0	
Response	
Line Dufour - Hydro-Qu?bec Production - NA - Not Applicable - NPCC	
Answer	Yes
Document Name	
Comment	
No comments.	
Likes 0	
Dislikes 0	
Response	
Davis Jelusich - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Public Utility District No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
CHPD supports the proposed concept to include new language that specifically scopes virtual environments as an extention to the existing standards, while maintaining compatibility with the compliance approach used now for existing non-virtual systems. CHPD requests that the SDT consider developing language that is more specific and reduces the potential for scoping confusion. For example, the proposed Management Plane Isolation change could be written to ensure that only applicable virtual hosts (e.g., those hosting BCAs, EACMS, etc…) and their associated hypervisors are considered under new requirement language. This approach would prevent other CIP asset types like BCAs or PCAs from being unintentionally included.	
Likes 0	
Dislikes 0	
Response	
Jonathan Robbins - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	Yes
Document Name	
Comment	

1. In reviewing the comments on the Q&A, it's unclear as to whether the drafting team is treating a SAN as a separate BCA or only as a BCSI storage location. Could the SDT please clarify?

2. Seminole recommends the SDT to be cognizant of the layering that can occur through virtualization in that if CIP Requirements are already applying to the hardware that Seminole would prefer that the additional Requirements applying to the virtual devices on that hardware would be limited or non-existent.

3. The Standards are unclear as to whether a programmable electronic device definition can exclude a virtual machine. The SDT should take this into consideration while drafting revised Requirements.

Likes 0	
Dislikes 0	

Response

Alex Ybarra - Public Utility District No. 2 of Grant County, Washington - 1,4,5,6

Answer	Yes
Document Name	

Comment

No Comments

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

Reclamation supports the SDT's intent to create security objective-based requirements; however, the Case for Change White Paper seems to be addressing virtualization at too granular of a level. Many of the challenges and scenarios discussed are hypothetical, extremely detailed, and appear to require extremely detailed and complicated CIP requirements. Reclamation is concerned that the path forward as described will result in requirements with a compliance/documentation burden that is not commensurate with the level of risk reduction provided.

Reclamation recommends the SDT incorporate virtualization into the CIP standards by clearly identifying and defining the scope of what must be protected while retaining the language in the current versions of CIP standards. For example, a requirement might state that entities are required to protect against unauthorized access to BES Cyber Systems. To address this existing requirement for both virtualized and non-virtualized environments, Reclamation also recommends the SDT revise the definitions in the NERC Glossary of Terms to include virtualized systems and leverage the existing

requirement to protect against unauthorized access. Reclamation does not support creating a virtual counterpart definition for all existing physical definitions. Definitions should include physical and virtual aspects of the defined terms.	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
TVA concurs with the path forward, but "shared infrastructure" qualifications would need to be defined since this will be a new asset class. The standard should be as specific as possible to highlight the difference from existing hardware.	
Likes 0	
Dislikes 0	
Response	
Leanna Lamatrice - AEP - 3,5	
Answer	Yes
Document Name	
Comment	

AEP requests the SDT include sufficient flexibility to allow entities to transition from their current compliance strategy to a newly available strategy and remain compliant throughout the process. Further, AEP requests the SDT make any new or revised requirement language backward compatible to the current obligation for systems not affected by virtualization. AEP believes there should not be a cost to entities that results from changes made to requirements and definition to accommodate virtualization technology.	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO	
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	
Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	

Texas RE noticed that the SDT seems to have gone outside the scope of the 2016 Standard Authorization Request (SAR). Texas RE inquires as to whether a new SAR should be submitted.

The 2016 SAR states “Virtualization – The CIP V5 standards do not specifically address virtualization. Because of the increasing use of virtualization in industrial control system environments, V5TAG asked that the SDT consider CIP-005 and the definitions of Cyber Asset and Electronic Access Point regarding permitted architecture and the security risks of network, server and storage virtualization technologies.” Modifying the CIP standards to embrace new security techniques is not an issue that was included in the V5TAG Transfer Document nor was the SDT instructed to address issues with the standards’ adaptability to current and future technology innovation.

While Texas RE agrees that some changes should be made to the CIP standards, not all of the changes are necessary at this time, nor are all of the changes specific for virtualization.

Texas RE recommends the following path forward:

- Modify the Cyber Asset definition to include virtual machines, hosts, etc.
- Create a separate standard for virtualized environments or modifying CIP-005-6 to include security objectives for virtualized environments.
- Not making any changes to the ESP and EAP terms as they are defined broadly enough to give entities the flexibility in how they apply those terms within many types of network architectures.

Likes 0	
Dislikes 0	

Response