NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Comment Form

Project 2016-02 Modifications to CIP Standards Virtualization in the CIP Environment

Do not use this form for submitting comments. Use the electronic form to submit comments on the **use of Virtualization in the CIP environment**. The electronic form must be submitted by **8 p.m. Eastern, Tuesday, April 11, 2017**.

Additional information is available on the project page. If you have questions, contact Al McMeekin at (404) 446-9675.

Background Information

On January 21, 2016, the Federal Energy Regulatory Commission (Commission) issued Order No. 822, *Revised Critical Infrastructure Protection Reliability Standards,* approving seven CIP Reliability Standards and new or modified definitions. On March 9, 2016, the NERC Standards Committee authorized a Standards Authorization Request (SAR) to be posted for a 30-day informal comment period from March 23 – April 21, 2016. Based on the comments received, the Standard Drafting Team (SDT) made minor revisions to the SAR which was posted for an additional 30-day informal comment period June 1-30, 2016.

The purpose of this project is to; (1) consider the Version 5 Transition Advisory Group (V5TAG) issues identified in the CIP V5 Issues for Standard Drafting Team Consideration (V5TAG Transfer Document), and (2) address the Commission directives contained in Order 822. These revisions will increase reliability and security to the Bulk Power System (BPS) by enhancing cyber protection of BPS facilities.

The V5TAG, which consisted of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by the existing SDT for the CIP Reliability Standards. The V5TAG developed the V5TAG Transfer Document to formally recommend that the SDT address these issues during the standards development process and to consider whether modifications can be made to the standard language.

The current informal posting document is an effort to gather input on the V5TAG issue related to virtualization in the CIP environment. The CIP standards are based primarily on concepts dating back to Version 1 and as technology has evolved, issues have begun to arise as entities attempt to take new concepts and fit them into some of the Version 1 paradigms. These issues revolve around topics such as:

- Hypervisor – the virtualization component that manages the guest operating systems (OSs) on a host and controls the flow instructions between the guest OSs and the physical hardware.

- Virtual machines – With virtualization technologies, a single physical Cyber Asset can be used as an execution platform for numerous virtualized operating systems, micro-service containerized applications, and virtual network functions of all classifications. A single physical Cyber Asset can appear to an external network as many complete Cyber Assets. Virtual switches and networks can be defined so these virtual machines can communicate with each other as if they are separate physical nodes on the network. Virtual machines and functions can also migrate around a physically clustered cyber system such that the singular physical Cyber Asset where an application resides can change at any moment.

  The virtualization of Cyber Assets provides advantages for the availability, resiliency, and reliability of applications and functions hosted in such an environment and the CIP standards must not stand in the way of these benefits as long as they are implemented in a secure manner. Virtualization affords enhanced security in some cases as the security controls themselves can be virtualized and placed within the virtual environment closer to the workloads they are protecting. However, there are also different security risks introduced by these environments. The management systems or consoles for these environments allow for the complete control of numerous components of the infrastructure. Virtual machines or networks can be added, modified, or deleted from one central management system. For example, rogue virtual components can starve legitimate workloads of the shared resources (processor, memory, etc.) they need to reliably perform their function. In summary, changes to the CIP Requirements may be needed to account for virtualization.
- Virtual Networks – Electronic Security Perimeter (ESP) constructs within the current CIP standard are limited to defining security zones at Open Systems Interconnection (OSI) Layer 3 and do not support security zones defined at layers other than OSI Layer 3. With current, widely deployed technology, networks are no longer solely defined by the arrangement of physical hardware and cables *inside* or *outside* of a *perimeter*. Networks can exist as a mixture of physical and virtual segments or purely in a virtual state within one device. Virtual firewalls and other security tools are also available to help secure these environments. Typical hardware network switches can be configured with internal logical isolation to implement multiple virtual networks within them. Accordingly, the SDT is reviewing the CIP standards to validate that definitions, requirements, and guidance regarding ESPs and Electronic Access Points (EAPs) continue to provide for secure and reliable operations.
- Virtual Storage – Historically, servers were limited to dedicated storage within the device. Typically, the operating system and the applications resided in the server on hard drives. Virtual storage technologies such as Storage Area Networks (SANs) present virtualized logical drive storage units to all attached servers. These types of environments then become a shared resource among many physical and virtual hosts.

With all of this in mind, the SDT is considering:

1) Areas in the current CIP requirements that might prevent or hinder the adoption of virtualization technologies for BES Cyber Systems and related systems;
2) Areas of new risks introduced by virtualization technologies and how to address them in the standards.

Questions

The SDT has determined that some of the concepts in CIP Version 5 must be fully realized in order to support virtualization. For example, while Version 5 introduced the "cyber system" concept and most requirements are now written at the cyber system level, the advantages of this approach have not been fully integrated into all levels of planning, design or compliance assessment approaches. Most entities still manage their CIP programs at a device level and auditors still look for device-centric evidence of compliance. This paradigm poses substantial issues with the use of virtual technologies. Infrastructure resources are pooled, apportioned to a given workload, and withdrawn or re-assigned when no longer needed. Infrastructure components (including instances of operating systems) come and go according to the current workload, making individual Cyber Asset level inventories difficult or impossible. The mobility of these resources makes permanently describing their physical locations problematic. Hardware (both computer and network) becomes a general-purpose commodity — merely a pool of resources on top of which the actual infrastructure is designed and created at a logical/virtual level. As technology increasingly blurs the line between physical and virtual systems, managing compliance in terms of individual devices or Cyber Assets becomes more challenging.

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?

   ☒ Yes
   ☐ No

   Comments:

   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

~~*Programmable*~~*An electronic device*~~s~~ *(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).

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.

☒ Yes
☐ No

Comments:
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.

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

☐ Yes
☒ No

Comments:
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.

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

☒ Yes
☐ No

Comments:
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.

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.

☒ Yes
☐ No

Comments:

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.

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

☐ Yes
☒ No

Comments:

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.

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.

☐ Yes
☒ No

Comments:

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.

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.

☐ Yes
☒ No

Comments:

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.

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

☐ Yes
☒ No

Comments:

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.