Unofficial Comment Form

Project 2016-02 Modifications to CIP Standards

Concepts for Virtualization and Definitions

**Do not** use this form for submitting comments. [Standards Balloting and Commenting System (SBS)](https://sbs.nerc.net/) to submit comments on **Project 2016-02 Modifications to CIP Standards Virtualization in the CIP Environment.** The electronic form must be submitted by **8 p.m. Eastern, Thursday, November 2, 2017.**

**m. Eastern, Thursday, August 20, 2015**

Additional information is available on the [project page](http://www.nerc.com/pa/Stand/Pages/Project%202016-02%20Modifications%20to%20CIP%20Standards.aspx). If you have questions, contact [Katherine Street](mailto:katherine.street@nerc.net) (404) 446-9702 or [Mat Bunch](mailto:mat.bunch@nerc.net) (404) 446-9785.

# Background Information

The Standard Drafting Team (SDT) for Project 2016-02 Modifications to CIP Standards continues to work to address transferred issues from the Version 5 Transition Advisory Group (V5 TAG). The V5 TAG consisted of six volunteer Responsible Entities who worked with NERC and the Regional Entities to implement the CIP Version 5 standards in an accelerated time frame. During the implementation study, study participants focused on the technical solutions and processes needed to meet the standards. As a result of this effort, issues were identified with the definition of Cyber Asset as well as the use of virtualization. These issues were documented in [CIP V5 Issues for Standard Drafting Team Consideration](http://www.nerc.com/pa/Stand/Project%20201602%20Modifications%20to%20CIP%20Standards%20DL/Transfer_Issues_V5TAG-SDT_1st-final-03232016.pdf).

The SDT has conducted outreach to industry on the concepts of virtualization through webinars that are published on the [Project 2016-02 Modifications to CIP Standards related files page](http://www.nerc.com/pa/Stand/Pages/Project-2016-02-Modifications-to-CIP-Standards-RF.aspx). To address the topics of the Cyber Asset definition and virtualization, the SDT has developed concepts for which we are seeking informal comment to gather further input from stakeholders. In reviewing these concepts and risks, it became clear that other areas may need to be adjusted to provide a clearer categorization of assets and applicable requirements to address the risk of virtualization.

As a result of this work, this comment form introduces new concepts which may result in the development of new requirement language, new definitions, and modifications to existing definitions. SDT proposes these concepts to:

1. Refine terms related to virtualization, such as Cyber Asset and Centralized Management System (CMS).
2. Improve areas in the current CIP Standard requirements that might hinder the adoption of virtualization technologies for BES Cyber Systems and other related systems;
3. Address areas of new cybersecurity risks, technological concepts, and techniques introduced with virtualization technologies; and
4. Clarify the context of virtualization technologies and mixed physical and/or virtual environments where advancing technologies have blurred boundaries or made legacy approaches obsolete.

The concepts noted within this informal comment form are not an obligation for Responsible Entities to implement virtual technology. The target audience for this informal comment form are those Responsible Entities that have implemented or are planning to implement virtual technology.

# Concept 1: Modifications to allow use of secure multi-instance environments

## Cyber Asset Definition

The V5 TAG implementation study noted issues with the use of the term Cyber Asset in the context of virtualization. In virtual environment, how does the construct of a virtual system align to the definition when the various components are distributed across a vast array of infrastructure components? Additionally, the V5 TAG requested that the SDT clarify the intent of “programmable” by considering such factors as whether a device is merely configurable, its executable code is not field upgradable, or if its functionality can only be changed via physical DIP switches, swapping internal chips, etc.

In April 2017, the SDT received comment from industry that indicated that the definition of Cyber Asset would benefit from clarification how it relates to physical and virtual systems. Many comments also indicated that through broader industry implementation, issues with the meaning of “programmable” had been resolved and the definition of Cyber Asset did not need to be modified to address this. Additionally, ERO Enterprise-endorsed [Implementation Guidance](http://www.nerc.com/pa/comp/guidance/EROEndorsedImplementationGuidance/CIP-002-5.1_BES_Cyber_Assets_LL.pdf) exists on the term "programmable".

Due to the foundational nature of the Cyber Asset definition as well as the comments received in April 2017, the SDT seeks comment on the following conceptual definition of Cyber Asset in the Glossary of Terms Used in NERC Reliability Standards (NERC Glossary).

Current:

**Cyber Asset:**

Programmable electronic devices, including the hardware, software, and data in those devices.

Redline

**Cyber Asset:**

A programmable electronic physical or virtual device~~s~~, including the hardware, software, and data in th~~os~~e device~~s~~. Each virtual machine and host is a distinct device.

Clean

**Cyber Asset:**

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

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

Yes

No

Comments:

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

Yes

No

Comments:

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

Comments:

## Centralized Management Systems (CMS)

As the SDT worked through issues related to virtual systems, it became clear that there was no straightforward way within the current CIP Standards to adequately address the risk of systems used to manage virtual environments. Management systems in virtual environments, through their consolidated interfaces and automation, can modify and delete entire infrastructures including virtual servers, networks, and storage. Given the broad capabilities of management systems in a virtual environment, they present specific and significant risk to the reliability of the BES Cyber Systems associated with those management systems.

The SDT considered several options to address the risks of management systems such as grouping management systems into the existing EACMS definition. This, however, would place these assets inappropriately in the EACMS category when they do not perform access control or access monitoring. Using the EACMS category in this manner creates a one-size-fits-all approach to requirements that does not consider the degree of risk or technical constraints posed by the particular system. For example, a system that only monitors and logs access does not pose the same level of risk as a management system for a large virtualized Control Center with the capability to modify or delete a complete infrastructure. Technical controls to mitigate the risk may differ depending on the capabilities of the management system. An electronic access monitoring system presents a risk of leaking BES Cyber System Information; an electronic access control system presents a risk of unauthorized access to, or modification of, a BES Cyber System’s operational parameters; and a management system presents a risk of unwanted or unintended modification or deletion of a complete infrastructure.

Proposed requirements related to this definition are detailed below.

The SDT determined a more appropriate option was to create a new definition for Centralized Management System (CMS) and apply appropriate and specific security requirements. The SDT seeks comment on the following conceptual definition of Centralized Management System in the Glossary of Terms Used in NERC Reliability Standards (NERC Glossary).

**Centralized Management System (CMS):**

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

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

Yes

No

Comments:

## Virtualization Terms and Requirements

The foundational pieces have now been set for the use of virtualization solutions. However, these solutions still pose risk. These risks and the nature of virtual systems may require some modifications to Standards. The concepts being proposed include additional access control and separation of the management plane from the data plane. This can help to prevent users of the applications on a virtualized system gaining access to the management system that can modify and delete the underlying infrastructure including virtual servers, networks, and storage.

The SDT uses the terms “instance” and “multi-instance” within the proposed requirements below. For the purposes of these proposed changes, the SDT intends for “instance” and “multi-instance” to be understood as:

* Instance: Discrete organizational environments with specific privileges or security levels, consisting of functions that consume resources from the shared infrastructure. Instances are logically isolated but physically interconnected.
* Multi-instance: An environment where a shared infrastructure provides containers for more than one instance.

In reviewing the risks that are unique and inherent to the use of virtualization technologies, the SDT identified the following risks:

1. Shared infrastructure,
2. Span of control, insider threats, and lateral privilege expansion,
3. Misconfiguration, excessive privileges, and capability of administrators, and
4. Escalation of privilege.

The SDT proposes the following definition and requirements in support of the use of virtual technologies.

## Electronic Security Zone (ESZ)

The SDT contends that the Electronic Security Perimeter (ESP) definition does not accurately describe the proper isolation of virtual systems within shared infrastructure. Details of the analysis are captured in network isolation portion of the [industry webinar presented on March 21, 2017](http://www.nerc.com/pa/Stand/WebinarLibrary/2016-02_CIP_V5M_Webinar_Virtualization_slides_for_posting_with_notes_03212017.pdf). To address the concerns noted, the SDT seeks comment on the following conceptual definition of Electronic Security Zone (ESZ) in the Glossary of Terms Used in NERC Reliability Standards (NERC Glossary).

**Electronic Security Zone:**

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

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

Yes

No

Comments:

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

Yes

No

Comments:

## New Requirement CIP-005 Requirement 1, Part 1.6

The SDT proposes a new requirement part 1.6 for CIP-005 Requirement R1. This requirement part is for Responsible Entities to implement one or more Electronic Security Zones (ESZ) to meet the security objective of separating the management plane and the data plane of high and medium impact BES Cyber Systems in a multi-instance environment. Part 1.6 would also require Responsible Entities to implement one or more ESZs to meet the security objective of protecting the infrastructure associated with high and medium impact BES Cyber Systems in a multi-instance environment by limiting access to the Centralized Management Systems using a management plane ESZ.

Responsible Entities maintain the flexibility for grouping by cyber system function, by risk, by type of applicable security controls, or other logical groupings. The ESZ contains a distinct subset of the Responsible Entity's Cyber Assets. These are characterized as requiring (or benefiting from) similar security controls and separation from other distinct Cyber Assets. Properly implemented ESZs can limit damage and impact to availability to other surrounding ESZs, specifically by helping protect against span-of-control risks, insider threats, and lateral privilege expansion.

Again, the requirement would only be applicable to high and medium impact BES Cyber Systems residing in a multi-instance environment and their associated CMS.

Part 1.6:

Logically separate all Applicable Systems into defined groups of one or more Cyber Asset(s) to achieve the objective of mitigating the risks of span-of-control, insider threats, and lateral privilege expansion. At a minimum:

1. The management plane and the data plane of the applicable BES Cyber System shall be separated;

2. The CMS of the applicable BES Cyber System shall be separated from its data plane

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

Yes

No

Comments:

## New Requirement CIP-005 Requirement 1, Part 1.7

Similarly to CIP-005 Requirement R1, Part 1.3, the SDT proposes new requirement Part 1.7. Part 1.7 requires Responsible Entities to identify, control, and explicitly allow only necessary inbound and outbound communication between ESZs of high and medium impact BES Cyber Systems residing in a multi-instance environment. Part 1.7 would be added to CIP-005 to reduce the risks inherent to virtualization related to misconfiguration, excessive privileges, capability of administrators, as well as information protection and data leakage.

The requirement would be applicable to high and medium impact BES Cyber Systems residing in a multi-instance environment and their associated CMS(s).

Part 1.7:

Implement technical controls that enforce separation between ESZs by allowing only necessary inbound and outbound communication between the separated Cyber Asset(s) residing in a multi-instance environment.

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

Yes

No

Comments:

## New Requirement CIP-005 Requirement 1, Part 1.8

Through the SDT work on virtualization, situations have been identified where a Responsible Entity may choose to share the same system infrastructure between applicable Cyber Assets and other programmable devices. As the footprint of cyber assets outside the scope of the CIP Standards in an organization might be significantly larger in size from the Cyber Assets in scope of the CIP Standard, a Responsible Entity may invest in its IT infrastructure with greater capability and more robust features. As presented in the third webinar on virtualization, this is particularly true with storage virtualization implementations. Under certain circumstances, leveraging enterprise infrastructure solutions will provide a better security posture for applicable Cyber Assets. Part 1.8 has been drafted with the objective of allowing such leverage as long as controls mitigating the additional risks are implemented.

A CIP Standard requiring the complete physical separation of applicable Cyber Assets and other programmable devices might adversely affect the overall security posture and reduce operational efficiency for the Responsible Entity through unnecessary expense and complexity of processes or technical implementation. Security controls exist to manage secure logical separation in multi-instance environments and there are operational benefits to sharing a common infrastructure as well. Technological advancements are often coupled with new security mechanisms which often benefit legacy infrastructure.



The diagram above shows an example of a shared multi-instance environment. The green arrows in the diagram represent the data communication. To exchange data between Partition 1 and 2, communication has to go through an EAP represented in the diagram by a firewall. The blue arrows in the diagram represent the management communication. In order to manage Partition 2, or any Cyber Asset hosted by the multi-instance environment and outside the ESP, IP communication to the management plane from outside the ESP has to go through the EAP since the management plan of shared multi-instance environment has to reside inside the ESP. The yellow arrows in the diagram represent the resource management activities performed by the multi-instance operating system necessary to ensure separation of data plane and management plane as well as partitions between Cyber Assets inside the ESP and Cyber Assets outside the ESP.

The SDT proposes CIP-005 Requirement 1, Part 1.8 to provide protection where the infrastructure used in a multi-instance environment is shared between applicable Cyber Assets and other programmable devices. This allows Responsible Entities to leverage the investments and protection of infrastructure shared between applicable Cyber Assets and other programmable devices. The requirement would be applicable to high and medium impact BES Cyber Systems residing in a multi-instance environment and their associated CMS(s).

Part 1.8:

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

1. The BES Cyber System, the management plane of the shared infrastructure, and any hosted Cyber Assets not part of a BES Cyber Systems shall all be separated; and

2. Communications between the BES Cyber System and any hosted Cyber Assets not part of a BES Cyber System shall all be denied by default

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

Yes

No

Comments:

## New Requirement CIP-005 Requirement 3, Part 3.1

In reviewing the risks associated with communications in a virtual environment, the SDT identified a gap with remote access used to perform CMS functions. These communications using a CMS do not align appropriately to Interactive Remote Access. Tasks may be performed from outside the ESP that are a blend of interactive and automated tools, allowing for misinterpretation and unjustified relaxation of security mechanisms required for Interactive Remote Access. Using jump servers to perform CMS functions might not be the most effective or the most secure. Also, remote access to a Cyber Asset inside an ESP could benefit from other methods besides Interactive Remote Access for performing CMS functions.

CIP-005 Requirement R3, Part 3.1 allows for a new type of remote access to be used to perform CMS functions from outside of an ESP. Part 3.1 allows the CMS function to be performed outside an ESP using an access method other than an Intermediate Systems to fix the gap that may exist between Interactive Remote Access and system-to-system communication. It does this by introducing requirements that are commensurate with the risk inherent to the management function in a multi-instance environment.

The SDT proposes new requirement CIP-005 Requirement 3, Part 3.1. Part 3.1 would be applicable to high and medium impact BES Cyber Systems.

Part 3.1:

Require authentication, integrity and non-repudiation controls for all sessions initiated outside of the ESZ, whether user initiated or system-to-systems communications, used to perform CMS functions.

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

Yes

No

Comments:

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

Yes

No

Comments:

## New Requirement CIP-004 Requirement 4, Part 4.5

The SDT has identified “too much privilege” as an inherent risk in virtualization. This risk can be reduced by adding controls in CIP-004. Limiting of the privileges granted to the minimum necessary is only present in the guidance. It is not a requirement. This security risk can be mitigated, however, by implementation of least privilege access and separation of duties in the requirement language. This means fewer people get high level privileges, and no single individual gets privileges that are too broad. For efficiency, it can be implemented via role-based access control (RBAC), which requires an initial effort to define roles properly. But also provides an opportunity for internal review of the span-of-control risk. Role-based access control and separation of duties are both available in virtual environments. Implementation of RBAC varies by vendor but is generically the same in principle.

The SDT proposes new requirement CIP-004 Requirement 4, Part 4.5. Part 4.5 would be applicable to high and medium impact BES Cyber Systems.

Part 4.5:

The Responsible Entity shall document and implement process(es), except under CIP Exceptional Circumstances, to authorize electronic and unescorted physical access to BES Cyber Systems and BES Cyber Systems Information that implements the principles of need-to-know, least privilege, and separation of duties as determined by the Responsible Entity, as per system capability.

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

Yes

No

Comments:

# Concept 2: Modifications to the EACMS definition

As noted above, the SDT reviewed the scope of the current definition, the requirements, and risk of the types of assets contained within EACMS. The current construct does not differentiate controls based on the functionality and risk of the system. The current construct does, however, create what is known as the “hall of mirrors” effect. Specifically, there may be some types of EACMS that should be required to be inside an ESP and behind a firewall. An example could be the management system of a firewall that is categorized in such a way that it must reside within an ESP. That requirement, however, cannot exist for all EACMS because a firewall is itself an EACMS. Without defining a new category, the result would be that every EACMS would need to be inside an ESP and therefore protected by another EACMS. This creates the recursive "hall of mirrors" effect.

There are a number of systems that both monitor and provide part of the solution of controlling access, but do not actually control traffic at the point of entry. These devices or systems may or may not benefit from being inside a protected boundary, or they may form part of the strategy that protects BES Cyber Assets. The technical means of implementing some multi-part systems may require components to be outside, or span the ESP.

To address this, the SDT proposes breaking up the EACMS categorization of applicable systems by function so that the appropriate requirements for each can be applied. The SDT does not, however, want to create a reclassification and documentation exercise for Responsible Entities who would not see benefit and would try to create a way for those Responsible Entities to continue to use EACMS with no changes. There are also other options in addition to these two.

## Electronic Access Control System (EACS)

The SDT seeks comment on the following conceptual definition of Electronic Access Control System in the Glossary of Terms Used in NERC Reliability Standards (NERC Glossary).

**Electronic Access Control System (EACS):**

Cyber Assets that perform electronic access control of the BES Cyber Systems. This includes Intermediate Systems.

An Electronic Access Control System performs authentication and authorization of traffic or users. This is the “gatekeeper” function or the classic authentication and authorization functions of standard AAA. In many cases these systems do not perform any active filtering of the traffic passing through any particular interface. The primary duty of EACS is to authenticate and authorize. EACS move beyond the risk of unauthorized access to meta-information about an environment, to unauthorized access to BES Cyber Systems and modification of their operational parameters.

## Electronic Access Gateway (EAG)

The SDT seeks comment on the following conceptual definition of Electronic Access Gateway in the Glossary of Terms Used in NERC Reliability Standards (NERC Glossary).

**Electronic Access Gateway:**

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

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

## Electronic Access Monitoring Systems

As technologies and cyber attacks advance and become more complex, Responsible Entities are becoming increasingly interested in collecting and correlating electronic access monitoring events across their enterprises. This broad-based information collection provides Responsible Entities with more visibility into emerging threats and trends. Responsible Entities can then analyze and share this information more readily and take action to improve the overall cybersecurity and reliability of the BES through early detection of compromise.

Under the currently effective CIP Reliability Standards, if a Responsible Entity uses enterprise wide electronic access monitoring tools, the Cyber Assets used to perform the monitoring may meet the definition of EACMS and become subject to the CIP Reliability Standards applicable to EACMS. This may discourage or prevent Responsible Entities from using enterprise wide electronic access monitoring due to the device level requirements of an EACMS. Responsible Entities may be discouraged from providing and correlating security events across enterprise and control networks, even though cyber-attacks against control systems could enter through business networks. The SDT concludes there is value in correlating security events across both control and enterprise networks.

The SDT proposes that the information within the electronic access monitoring systems should be protected as a BCSI repository, rather than having the system categorized as an EACMS. The systems performing electronic access monitoring are used to monitor and collect information about BES Cyber Systems or Electronic Security Perimeter(s) and pose a risk of information leakage. These monitoring systems are not used to control access to the BES Cyber Systems or Electronic Security Perimeter(s). The monitoring function has been in scope of the EACMS definition due to the sensitivity of certain information that may be collected. The proposed change is to treat the data collected through the monitoring capability as BCSI rather than having the monitoring systems categorized as EACMS. This change will enable Responsible Entities to better leverage enterprise-wide monitoring to improve overall situational awareness, and in the process more proactively address security events.

This will result in improved security and reliability. This does not change a Responsible Entity’s obligations to monitor under CIP-007 R4.

To transition electronic access monitoring from EACMS to BCSI, the SDT seeks comment on the following conceptual modification to the definition of BES Cyber System Information in the Glossary of Terms Used in NERC Reliability Standards (NERC Glossary).

Clean:

**BES Cyber System Information:**

Data about the BES Cyber System that is processed, organized, structured, or presented in a context that could be used to gain unauthorized access or pose a security threat to the BES Cyber System.

BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to gain unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual or collections of IP addresses without context of location and purpose, ESP names, individual security logs, or policy statements.

Examples of BES Cyber System Information may include, but are not limited to: security procedures, collections of security logs, or security configuration information about BES Cyber Systems, Physical Access Control Systems, Electronic Access Control Systems, Electronic Access Gateway Systems, Centralized Management Systems, and Electronic Access Control or Monitoring Systems that are not publicly available; and network topology with network addresses of the BES Cyber System.

Redline:

**BES Cyber System Information:**

Data ~~Information~~ about the BES Cyber System that is processed, organized, structured, or presented in a context could be used to gain unauthorized access or pose a security threat to the BES Cyber System.

BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual or collections of IP addresses without context of location and purpose, ESP names, individual security logs, or policy statements.

Examples of BES Cyber System Information may include, but are not limited to:~~,~~ security procedures, collections of security logs, or security configuration information about BES Cyber Systems, Physical Access Control Systems, Electronic Access Control Systems, Electronic Access Gateway Systems, Centralized Management Systems, and Electronic Access Control or Monitoring Systems that is not publicly available ~~and could be used to allow unauthorized access or unauthorized distribution~~; ~~collections of~~ ~~network addresses~~; and network topology with network addresses of the BES Cyber System.

Current:

**BES Cyber System Information:**

Information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context, ESP names, or policy statements. Examples of BES Cyber System Information may include, but are not limited to, security procedures or security information about BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber System.

## Proposed Requirements Related to EACMS Changes

Based on the concepts presented above, the table below lists the current requirement scope of EACMS and those proposed for CMS, EACS, and EAG. In the table below, the “X” indicates where the requirement currently applies to the system category in the Applicable Systems column of CIP Standards. The “+” sign indicates an additional requirements being considered to address risk for that specific system category in the Applicable Systems column of CIP Standards. To the extent that there is no difference in requirement applicability, the SDT would look to consolidate the terms into as few classifications as necessary.

Please keep in mind that the SDT does not want to create a reclassification and documentation exercise for Responsible Entities who would not see sufficient benefit and would look to create a way for those Responsible Entities to continue to use EACMS with no changes.

| Requirement | EACMS | CMS (+) | EACS (+) | EAG (+) |
| --- | --- | --- | --- | --- |
| CIP-004 R1.x |  | **+** | **+** | **+** |
| CIP-004 R2.x | X | X | X | X |
| CIP-004 R3.x | X | X | X | X |
| CIP-004 R4.x | X | X | X | X |
| CIP-004 R5.x | X | X | X | X |
| CIP-005 R1.x |  | **+** | **+** | X (Part 1.5) |
| CIP-005 R2.x |  | **+** |  |  |
| CIP-005 R3 |  | **+** |  |  |
| CIP-007 R1.1 | X | X | X | X |
| CIP-007 R2.x | X | X | X | X |
| CIP-007 R3.x | X | X | X | X |
| CIP-007 R4.x | X | X | X | X |
| CIP-007 R5.x | X | X | X | X |
| CIP-009 R1.x | X |  | X | X |
| CIP-009 R2.1 | X |  | X | X |
| CIP-009 R2.2 | X |  | X | X |
| CIP-009 R2.3 |  |  | **+** | **+** |
| CIP-009 R3.x | X |  | X | X |
| CIP-010 R1.x | X | X | X | X |
| CIP-010 R2.x | X | X | X | X |
| CIP-010 R3.1 | X | X | X | X |
| CIP-010 R3.2 |  | X | **+** | **+** |
| CIP-010 R3.3 | X | X | X | X |
| CIP-010 R3.4 | X | X | X | X |
| CIP-010 R3.5 | X | X | X | X |
| CIP-011 R1.x | X | X | X | X |
| CIP-011 R2.x | X | X | X | X |

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

Yes

No

Comments:

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

Yes

No

Comments:

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

Yes

No

Comments:

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

Yes

No

Comments:

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

Yes

No

Comments:

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

Yes

No

Comments:

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

Yes

No

Comments:

# Concept 3: Compliance Guidance

The SDT has explored the idea that no changes are necessary to the CIP Standards to address virtualization. ERO Enterprise-endorsed [Compliance Guidance](http://www.nerc.com/pa/comp/guidance/EROEndorsedImplementationGuidance/CIP-002-5.1_BES_Cyber_Assets_LL.pdf) could be used to address many industry concerns with the proper implementation of virtualization.

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

Yes

No

Comments:

# Summary

The SDT has provided very diverse concepts for your consideration. Each of these concepts can be moved forward in the drafting process independently. Please provide your responses to each of the questions below.

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

Yes

No

Comments:

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

Yes

No

Comments:

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

Yes

No

Comments:

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

Comments: