NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# ERO Enterprise CMEP Practice Guide:

## Assessment of Virtualized Systems
## February 26, 2021

## Background

In support of successful implementation of and compliance with the North American Electric Reliability Corporation (NERC) Reliability Standards, the Electric Reliability Organization (ERO) Enterprise[1] adopted the Compliance Guidance Policy.[2] The Compliance Guidance Policy outlines the purpose, development, use, and maintenance of guidance for implementing Reliability Standards. According to the Compliance Guidance Policy, Compliance Guidance includes two types of guidance – Implementation Guidance and Compliance Monitoring and Enforcement Program (CMEP) Practice Guides.

## Purpose

This CMEP Practice Guide provides guidance to ERO Enterprise CMEP staff (CMEP staff) when assessing a Responsible Entity's Cyber Assets that host virtual machines through software hypervisors. This Practice Guide outlines risks that CMEP staff should consider when verifying methods used to meet the security objectives. This risk information informs CMEP staff's understanding of a Responsible Entity's security posture and commensurate Compliance Oversight (i.e., Compliance Oversight Plan, audit approach, etc.). CMEP Staff make compliance determinations in light of the specific facts and circumstances of the individual registered entities and the language of the Requirements.

## General Approach

CMEP staff should consider Cyber Assets providing functions for Cyber Assets within an Electronic Security Perimeter (ESP) and Cyber Assets outside an ESP to be shared infrastructure. CMEP staff should verify that the Responsible Entity identifies and protects any Cyber Asset providing shared infrastructure, regardless of type, to the "highest water mark" of CIP compliance. In other words, each Cyber Asset providing shared infrastructure must comply with the applicable CIP Requirements for all BES Cyber Systems to which it connects.

## Hypervisors

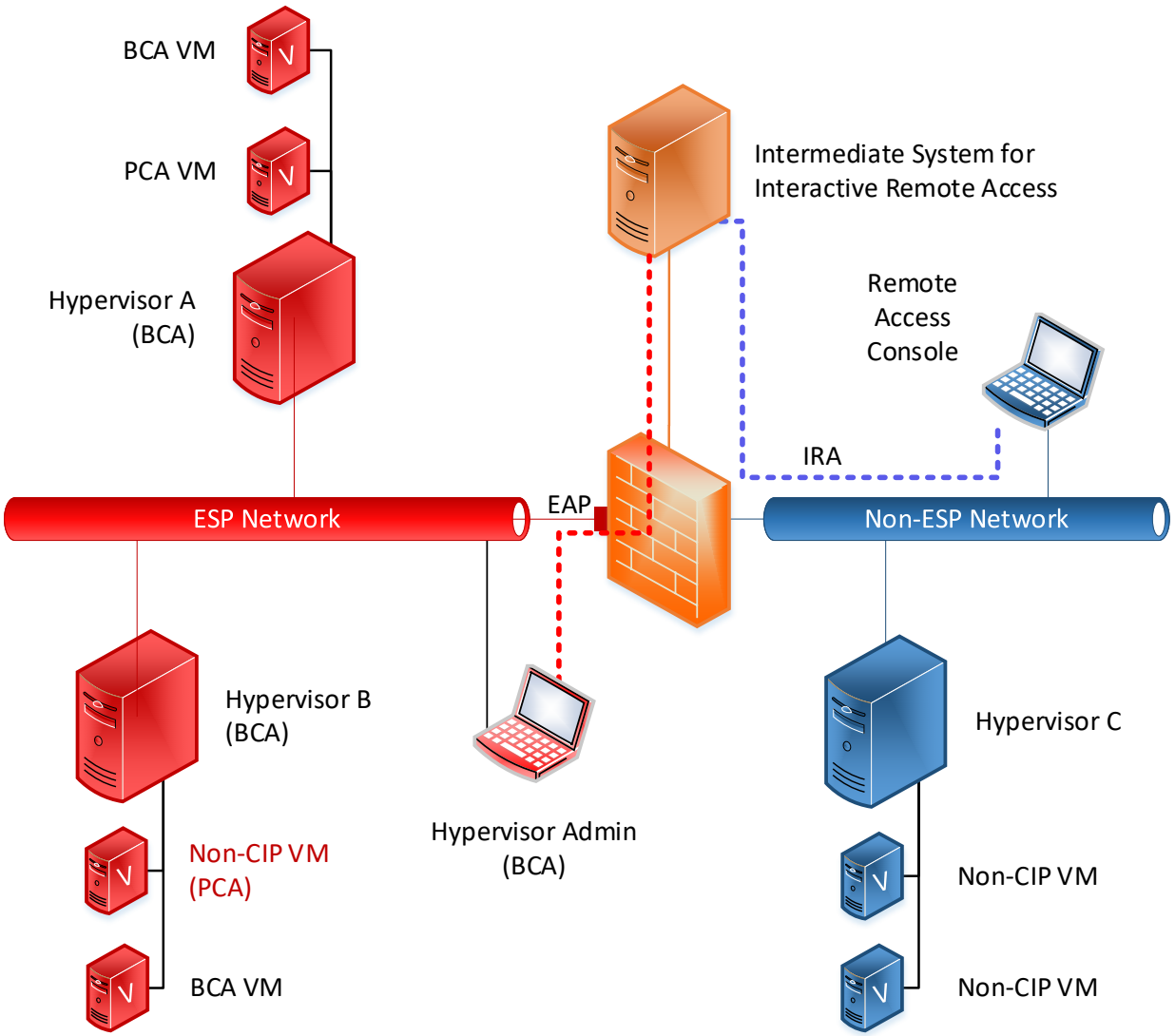
The virtual software industry defines "hypervisor" as the software that operates virtual machines (VM). The hypervisor allows one physical Cyber Asset to support multiple guest VMs by virtually sharing its hardware resources, such as memory and processing. Furthermore, multiple Cyber Assets providing hypervisor functionality often work together for redundancy and high availability purposes. Hypervisor management software tools allow common tasks, such as creation, duplication, deletion, and movement between hypervisors of guest VMs in addition to the allocation of system resources, such as memory and storage

[1] The ERO Enterprise consists of NERC and the Regional Entities.
[2] The ERO Enterprise Compliance Guidance Policy

space. Hypervisor management tools may allow complete interactive access to, and remote control of, guest VMs for ease of configuration.

Hypervisors allow multiple types and versions of operating systems to be installed and run as guest VMs. These guest VMs operate independently from one another. The guest VMs cannot communicate with one another or with other physical Cyber Assets across a local area network (LAN), unless purposefully configured with either a physical network interface card or virtual network connection. Devices hosting hypervisor software fulfill the required combination of hardware, software, and data for the definition of a Cyber Asset in the NERC Glossary. Additional information can be found in the National Institute of Standards and Technology (NIST) Special Publication 800-125: Guide to Security for Full Virtualization Technologies.[3]

## Virtualized Infrastructure for High or Medium Impact BES Cyber Systems




[3] http://csrc.nist.gov/publications/nistpubs/800-125/SP800-125-final.pdf

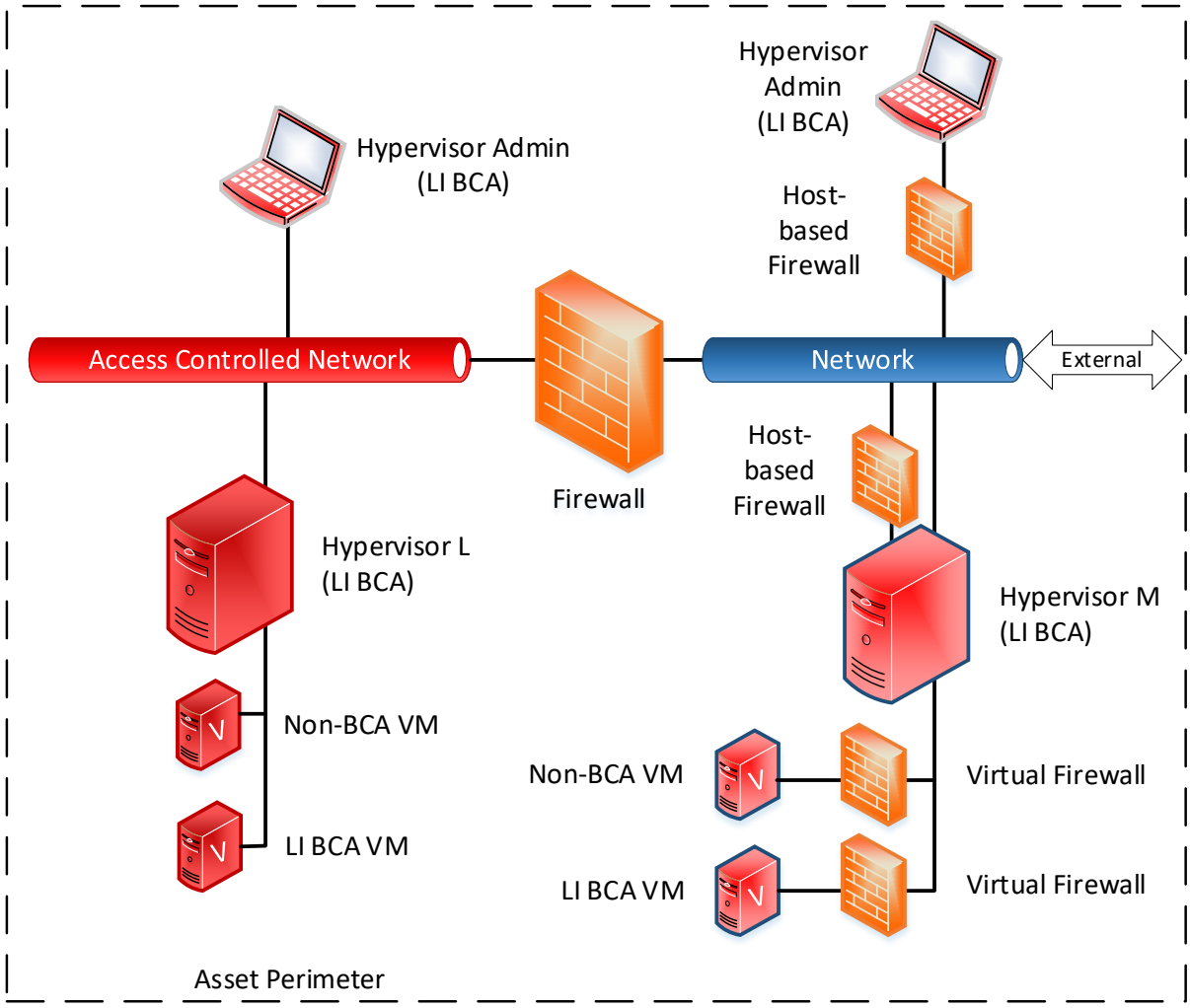
In the example illustrated above, the virtualized infrastructure supports BES Cyber Systems that are at a high or medium impact level. Hypervisor A is shown with two VMs running: a VM running an application that would be considered to be a BES Cyber Asset (BCA) if run on dedicated hardware, and an application that would be considered a Protected Cyber Asset (PCA) if run on dedicated hardware. Both of these VMs should be protected as a BCA and a PCA, respectively. These protections should follow each VM if it is migrated to Hypervisor B. Hypervisor B is shown with a non-CIP VM that could be outside of CIP scope if run on dedicated hardware outside of an ESP. However, this VM is running on a hypervisor within an ESP, and should be protected at the same level as a PCA associated with a BES Cyber System.

Also shown in the example above is a hypervisor administrative workstation. As this workstation could have a 15-minute impact on the operation or non-operation of one or more BES Cyber Systems, it may qualify as a BCA. If so, it must reside within an ESP and all applicable protections must be applied to it. Remote access to this system should follow the provisions of CIP-005.

Responsible Entities must demonstrate the appropriate identification of all BES Cyber Systems for each considered BES asset per CIP-002. For virtualized infrastructure, the hardware Cyber Asset and its hypervisor should be identified as a Cyber Asset and assigned the appropriate designation (BCA, PCA, Electronic Access Control or Monitoring Systems [EACMS], or Physical Access Control Systems [PACS]). The Responsible Entity is allowed flexibility in identifying the VMs as Cyber Assets of the appropriate type or as software within the hypervisor's Cyber Asset. In either event, the applicable protections (such as patch management, vulnerability assessments, anti-malware, etc.) should be applied and documented for each hypervisor and VM capable of running on the hypervisor.

If Cyber Assets providing virtualized infrastructure support only PACS or EACMS, CIP Standards do not require the Cyber Assets providing virtualized infrastructure to reside within an ESP. In this instance, however, CMEP staff would assess the virtualized infrastructure, including the hardware, hypervisor, and VMs essential to the PACS or EACMS service against the Requirements applicable for a PACS or an EACMS, respectively.

## Virtualized Infrastructure for Low Impact BES Cyber Systems




In the example illustrated above, the virtualized infrastructure supports BES Cyber Systems that are at a low impact level. Two hypervisors are shown each with a different method used to permit only necessary inbound and outbound electronic access to the hypervisor and its VMs.

Hypervisor L uses an external firewall to control electronic access to itself and its two VMs.

Hypervisor M uses a host-based firewall to control access to the hypervisor and virtual firewalls configured on the hypervisor to control access to each VM. Due to the high-water-marking of the non-BCA VM, access to it must also be protected.

Also shown in the example above are two hypervisor administrative workstations. As these workstations could have a 15-minute impact on the operation or non-operation of one or more BES Cyber Systems, they may qualify as BCAs. If so, electronic and physical access to these workstations must be controlled.

Responsible Entities must demonstrate the appropriate identification of all BES assets that contain low impact BES Cyber Systems per CIP-002. For virtualized infrastructure, the hardware Cyber Asset and its hypervisor should be identified as a Cyber Asset and assigned the appropriate designation. The Responsible Entity is allowed flexibility in identifying the VMs as Cyber Assets of the appropriate type or as software within the hypervisor's Cyber Asset. In either event, the applicable protections should be applied and documented for each hypervisor and VM capable of running on the hypervisor.

## Conclusion

Since Responsible Entities are allowed flexibility in how virtualized infrastructure (including the hypervisor and VMs) is identified and documented, CMEP staff should ensure that each Responsible Entity that implements a virtualized infrastructure in a CIP environment complies with each applicable Standard and requirement. In addition, CMEP staff should ensure the Responsible Entity protects any non-CIP Cyber Asset located within an ESP at the same level as a PCA associated with a BES Cyber System.