North American Transmission FORUM

Community Confidentiality Candor Commitment

This document was submitted to NERC for consideration as "Implementation Guidance." NERC chose not to endorse the document. Visit the NERC compliance guidance website for more information. The NATF is reviewing to determine next steps.

Cyber Security – Vendor Support via Web Conferencing

Implementation Guidance for CIP-005-6 Parts 2.4 and 2.5

Open Distribution

Disclaimer

This document was created by the North American Transmission Forum (NATF) to facilitate industry work to improve reliability and resiliency. The NATF reserves the right to make changes to the information contained herein without notice. No liability is assumed for any damages arising directly or indirectly by their use or application. The information provided in this document is provided on an "as is" basis. "North American Transmission Forum" and its associated logo are trademarks of NATF. Other product and brand names may be trademarks of their respective owners. This legend should not be removed from the document.

Version 1.0
Document ID: 1502
Approval Date: 03/08/2021

Versioning and Acknowledgments

Version History

Date	Version	Notes
03/08/2021	1.0	Initial version

Review and Update Requirements

- Review: every 3 years
- Update: as necessary

Table of Contents

Introduction

NERC Reliability Standard CIP-005-6, Requirement 2, Parts 2.4 and 2.5 went into effect on October 10, 2020 and are intended to address security risks posed by vendor remote access (VRA).

Goal/Problem Statement

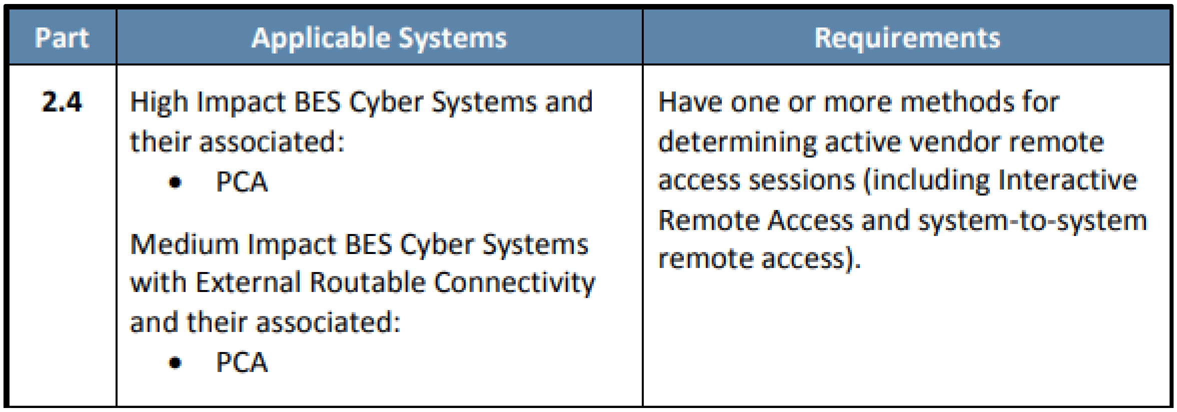
A responsible entity may require support from a vendor to assist in troubleshooting or for general maintenance of a Cyber Asset. It is not always practical to have a vendor come to the physical location. Emerging web conferencing and remote assistance capabilities provide new options to allow vendors to provide timely remote support. However, if a responsible entity permits the use of such technology with vendors, as it relates to its High Impact BES Cyber Systems and Medium Impact BES Cyber Systems with External Routable Connectivity (ERC), it may not be clear as to what evidence would be necessary or sufficient to demonstrate compliance with CIP-005-6 Requirement 2, Parts 2.4 and 2.5.

Scope

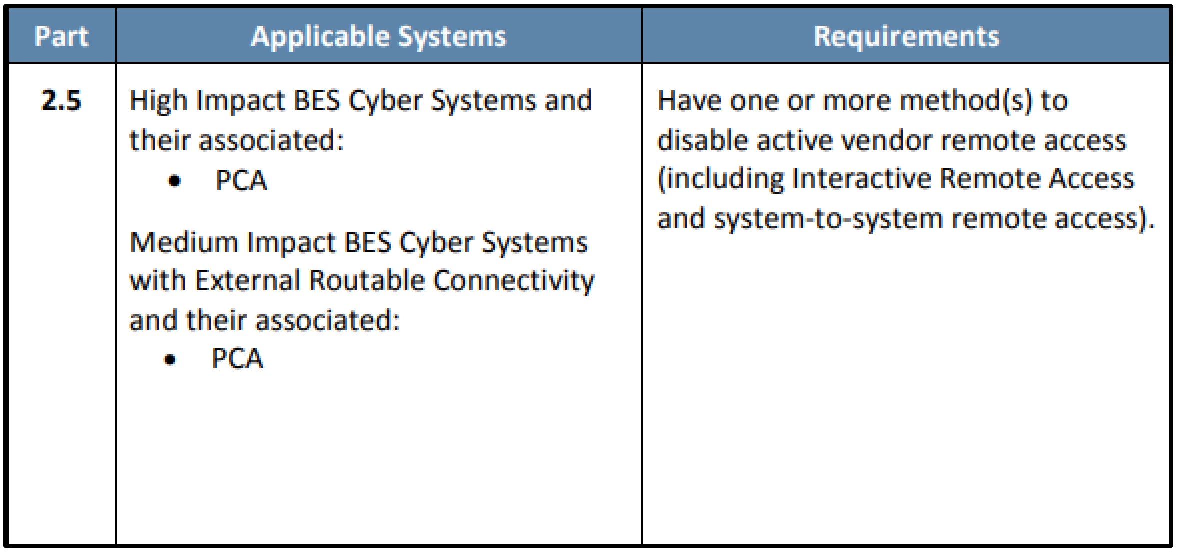
This Implementation Guidance addresses the use of web conferences with vendors, where the responsible entity does not turn over control of the session to the vendor. Control is considered the ability to control the keyboard and/or mouse. This Implementation Guidance does not address the use of web conferences with vendors where the responsible entity permits control of the session to be turned over to the vendor. Following this Implementation Guidance does not guarantee compliance and is based on precise language of the standard, individual facts, circumstances, system configuration, quality of evidence, etc.

Reliability Standard

CIP-005-6, Requirement 2, Parts 2.4 and 2.5



Part	Applicable Systems	Requirements
2.4	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).



Part	Applicable Systems	Requirements
2.5	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access).

Commonly Used Terms Within This Implementation Guidance

The following terms used in this Implementation Guidance are not defined within or intended to be included in the NERC Glossary of Terms[1]. These definitions are provided to ensure a common industry understanding of how they are applied solely within this Implementation Guidance. Where available, references to industry standardized definitions have been provided.

Vendor Remote Access (VRA)
Vendor Remote Access is the act of a vendor performing command and control and/or modification of a Cyber Asset while not physically touching the Cyber Asset's directly connected input device such as keyboard, mouse, touch panel, or console connection.

An entity may require support from a vendor to assist in troubleshooting or for general maintenance of a Cyber Asset. It is not always practical to have a vendor come to the physical location. Emerging web conferencing and remote assistance capabilities provide an option to allow vendors to provide timely remote support.

Requirement 2 Part 2.4

Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).

[1] Glossary of Terms Used in NERC Reliability Standards https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf

Requirement 2 Part 2.5

Have one or more method(s) to disable active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).

Vendor remotely viewing a responsible entity's Interactive Remote Access session (view only mode)

There may be times when a vendor is remotely viewing an interactive remote access (IRA) session initiated by a responsible entity's personnel. If the vendor representative is never given the ability to control the session, this would not be considered VRA. Additionally, since these sessions are not VRA, there is no compliance evidence to retain for each such session.

To address Parts 2.4 and 2.5, a responsible entity should have a documented process describing to personnel the expectations as to whether VRA is allowed, and any methods for determining that a VRA session is active and disabling active VRA sessions. If a responsible entity does not permit its personnel to turn over control to a vendor during web conferences, then the responsible entity should document such disallowance to address Parts 2.4 and 2.5.

As an additional security measure, responsible entities may also implement and document technical or procedural controls to prevent or deter personnel from turning control over to a vendor during a web conference session. For example, some web conferencing platforms can be configured such that giving control to another participant is not an available option.

Periodic Review

The NATF will review this implementation guidance every three years to verify continued applicability.