TEXAS RE

Vendor Remote Access Management

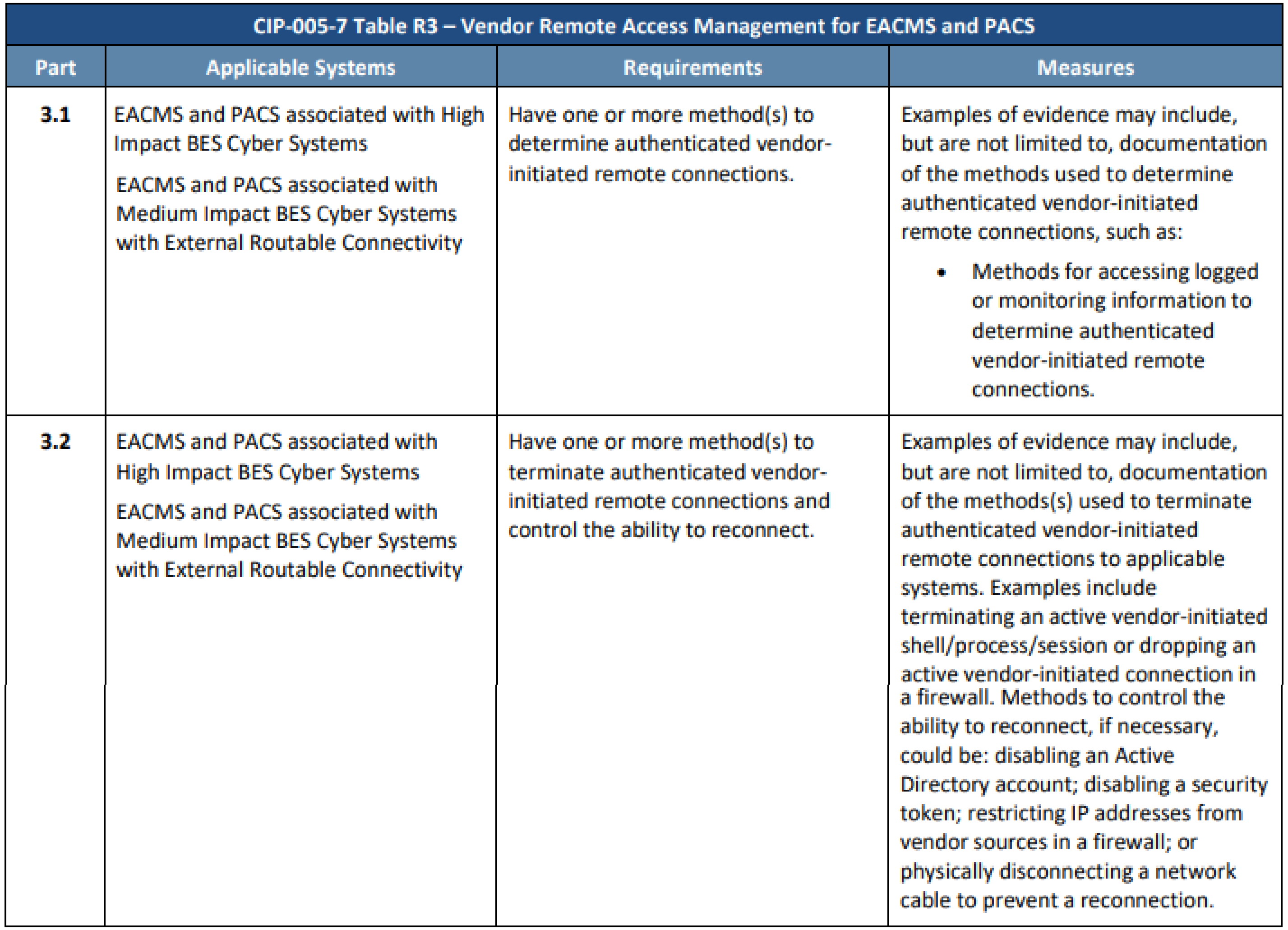
Paul Hopson
Compliance Team Lead

June 6, 2024

Purpose of CIP-005-7 R3

Ensure that Electronic Access Control or Monitoring Systems (EACMS) and Physical Access Control Systems (PACS) are not vulnerable to some of the threats introduced by having vendors and suppliers manage and/or support your assets remotely

Vendor Remote Access Management for EACMS and PACS



CIP-005-7 Table R3 – Vendor Remote Access Management for EACMS and PACS

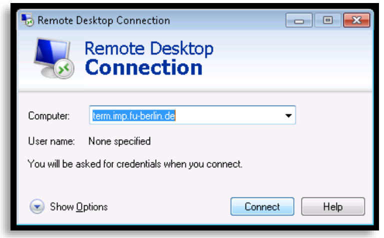
Part	Applicable Systems	Requirements	Measures
3.1	EACMS and PACS associated with High Impact BES Cyber Systems EACMS and PACS associated with Medium Impact BES Cyber Systems with External Routable Connectivity	Have one or more method(s) to determine authenticated vendor-initiated remote connections.	Examples of evidence may include, but are not limited to, documentation of the methods used to determine authenticated vendor-initiated remote connections, such as: • Methods for accessing logged or monitoring information to determine authenticated vendor-initiated remote connections.
3.2	EACMS and PACS associated with High Impact BES Cyber Systems EACMS and PACS associated with Medium Impact BES Cyber Systems with External Routable Connectivity	Have one or more method(s) to terminate authenticated vendor-initiated remote connections and control the ability to reconnect.	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to terminate authenticated vendor-initiated remote connections to applicable systems. Examples include terminating an active vendor-initiated shell/process/session or dropping an active vendor-initiated connection in a firewall. Methods to control the ability to reconnect, if necessary, could be: disabling an Active Directory account; disabling a security token; restricting IP addresses from vendor sources in a firewall; or physically disconnecting a network cable to prevent a reconnection.

Vendor Remote Access Risk

Your BES Cyber Assets (BCAs) and Protected Cyber Assets (PCAs) probably have more cybersecurity controls deployed around them than the network that is hosting your laptop or desktops. When a remote connection is established, the less secured remote device now introduces foreign threats to the environment.

Remote access by a vendor further elevates this risk because you are not in control or knowledgeable of how strong their security posture is. Just by allowing a remote connection from a vendor, your organization has assumed a certain level of risk.

Some Things to Consider

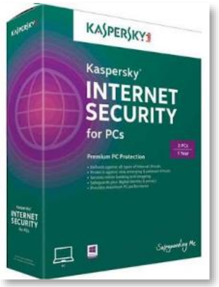

Remote Desktop Connection

Remote Desktop Connection

Computer: term.imp.fu-berlin.de

User name: None specified

You will be asked for credentials when you connect.



How well do you trust the vendor's cybersecurity posture at their facility?

Are you comfortable that the tools they use have been secured appropriately to the level of criticality of your environment?

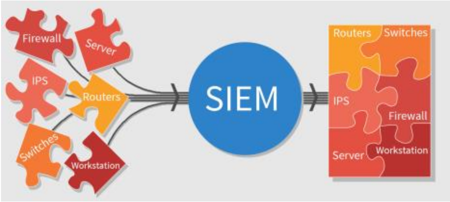
Do you trust the actions they are performing within the environment? Can you validate that work?

How do you know their login ID has not been compromised?

What You Can Do to Meet Compliance Objectives

ZERO TRUST ARCHITECTURE

NEVER TRUST, ALWAYS VERIFY



Zero Trust: Deny-by-Default

Control Each Connection

Ensure You Are Logging and Auditing

Isolate Your Supply Chain

Contact Info

Paul Hopson

Compliance Team Lead

Paul.Hopson@texasre.org

512-583-4972

Questions?

TEXAS RE

Ensuring electric reliability for Texans