



TEXAS RE

Remote Connectivity

Chris Jeffery
CIP Cyber & Physical Security Analyst

November 05, 2024

Antitrust Admonition

Texas Reliability Entity, Inc. (Texas RE) strictly prohibits persons participating in Texas RE activities from using their participation as a forum for engaging in practices or communications that violate antitrust laws. Texas RE has approved antitrust guidelines available on its website. If you believe that antitrust laws have been violated at a Texas RE meeting, or if you have any questions about the antitrust guidelines, please contact the Texas RE General Counsel.

Notice of this meeting was posted on the Texas RE website and this meeting is being held in public. Participants should keep in mind that the listening audience may include members of the press, representatives from various governmental authorities, and industry stakeholders.



Upcoming Texas RE Events



November 20, 2024

Fall Standards,
Security &
Reliability
Workshop



December 5, 2024

2025
Implementation
Plan



December 11, 2024

Texas RE
Quarterly &
Annual Meetings



Upcoming ERO Enterprise Events



November 5, 2024

Grid Fundamentals



November 13, 2024

IBR Registration Initiative
Webinar



November 18, 2024

Technical Talk with RF



slido

Product

Solutions

Pricing

Resources

Enterprise

Log In

Sign Up

Joining as a participant?

Enter event code

Join an existing event

#TXRE

The ultimate Q&A and polling platform

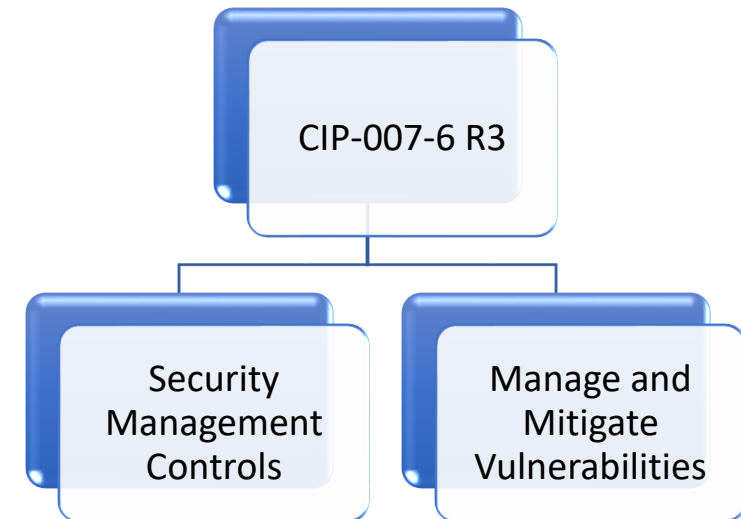
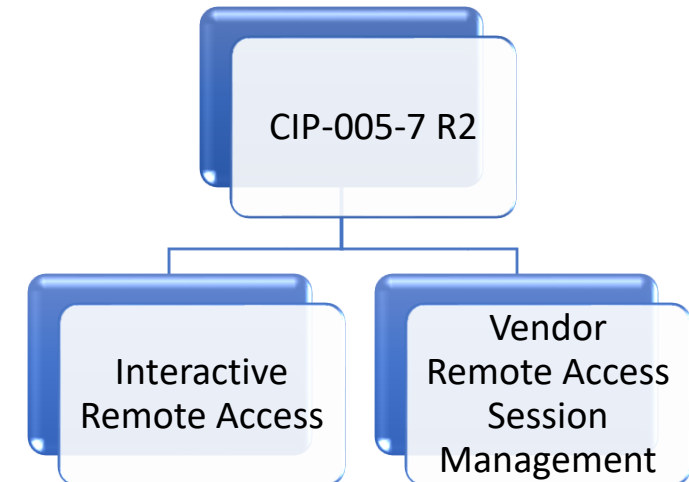
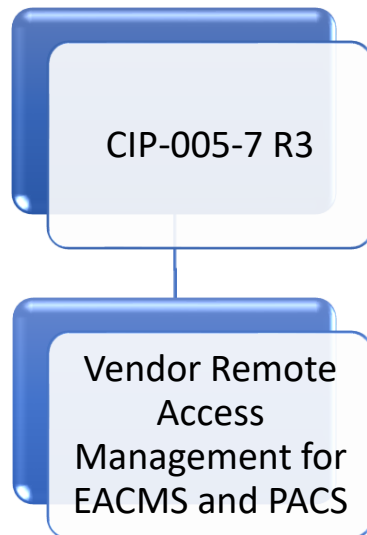
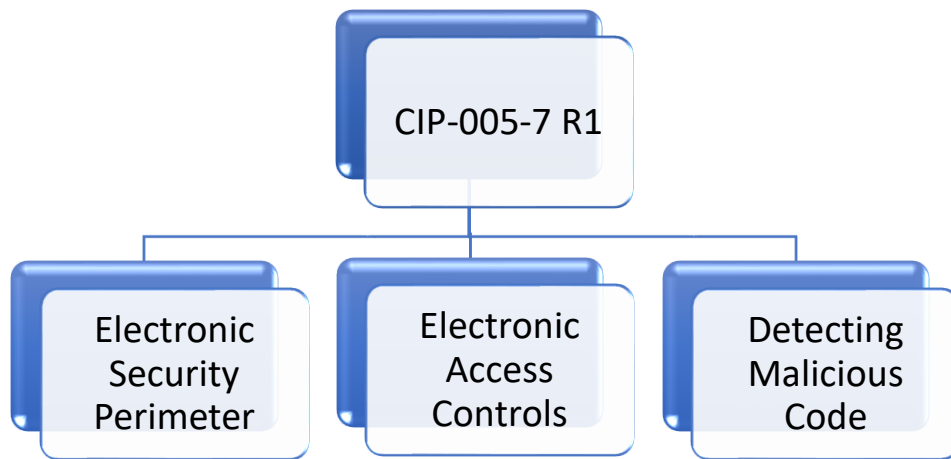
Give a voice to your audience, wherever they are.

Create your own Slido event


[Watch a video](#) or [Schedule a demo](#)



Overview



2024 CMEP IP





2024 ERO Enterprise Compliance Monitoring and Enforcement Program Implementation Plan

Version 1.0

October 2023

RELIABILITY | RESILIENCE | SECURITY



3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table 2: Remote Connectivity

Rationale	Standard	Req	Entities for Attention
Remote access to Critical Infrastructure Cyber Assets introducing increased attack surface, as well as possible increased exposure.	CIP-005-7	R2, R3	Balancing Authority Distribution Provider Generator Operator Generator Owner Reliability Coordinator Transmission Operator Transmission Owner
Malware detection and prevention tools deployed at multiple layers (e.g., Cyber Asset, intra-Electronic Security Perimeter, and at the Electronic Access Point) are critical in maintaining a secure infrastructure.	CIP-007-6	R3	Balancing Authority Distribution Provider Generator Operator Generator Owner Reliability Coordinator Transmission Operator Transmission Owner



Agenda

CIP-005-7 R1, R2, R3

CIP-007-6 R3

Examples of Evidence

Best Practices

NIST Internal Controls



CIP-005-7 – Electronic Security Perimeter

A. Introduction

1. **Title:** Cyber Security — Electronic Security Perimeter(s)
2. **Number:** CIP-005-7
3. **Purpose:** To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.



CIP-005-7 R1 – Electronic Security Perimeter

Part 1.1

- Cyber Assets with a routable protocol shall reside in the Electronic Security Perimeter

Part 1.2

- External Routable Connectivity (ERC) must travel through an Electronic Access Point (EAP).

Part 1.3

- Inbound and outbound access must have network permissions and justifications, all other traffic is denied by default.

Part 1.4

- Dial-up must be authenticated where technically feasible.

Part 1.5

- Have methods for detecting known or suspected malicious communications for both inbound and outbound communications.



CIP-005-7 R2 – Remote Access Management

Part 2.1

- Use an intermediate system for all Interactive Remote Access (IRA) so that the Cyber Asset initiating the IRA does not directly access an applicable Cyber Asset.

Part 2.2

- Utilize encryption on all IRA sessions that terminate at an intermediate system.

Part 2.3

- Require multi-factor authentication (MFA) for all IRA sessions.

Part 2.4

- Have methods for determining active vendor remote access sessions.

Part 2.5

- Have methods to disable active vendor remote access.



Part 3.1

- Have methods to determine authenticated vendor initiated remote connections.

Part 3.2

- Have methods to terminate authenticated vendor initiated remote connections and control ability to reconnect.



CIP-005-7 – Evidence Examples

CIP-005-7 R1	CIP-005-7 R2	CIP-005-7 R3
ESP Lists Network Diagrams Access Control Lists Documented processes Malicious communication detection methods	Network Diagrams Encryption MFA Documentation Live Demos	Documentation Screenshots Live Demos

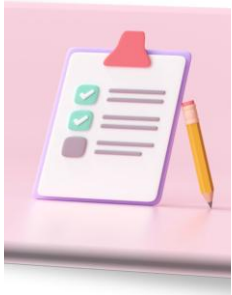


Slido Question

What are some best practices that you have developed to ensure you meet the CIP-005-7 requirements?



CIP-005-7 – Best Practices



Internal Audits



Maintain Logs



Access Controls



Documentation



CIP-007-6 R3 – Malicious Code Prevention

A. Introduction

1. **Title:** Cyber Security — System Security Management
2. **Number:** CIP-007-6
3. **Purpose:** To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).



CIP-007-6 R3 – Malicious Code Prevention

Part 3.1

- Have methods to deter, detect or prevent malicious code

Part 3.2

- Mitigate threat of detected malicious code

Part 3.3

- For methods pursuant to 3.1, have process to update signatures/patterns which addresses testing and installing of signatures or patterns



CIP-007-6 R3 – Evidence Examples

Documented
Processes

Malware,
deterrent,
detection or
prevention tools

Signature
Updates

Testing of
signatures



CIP-007-6 Best Practices



Slido Question

What are some internal controls that you have developed to help you meet the CIP-007-6 R3 requirements?



NIST SP 800-53 Controls

AC-17 REMOTE ACCESS

Control:

- a. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and
- b. Authorize each type of remote access to the system prior to allowing such connections.



Remote Access Control Enhancements

R1

Employ automated mechanisms to monitor and control remote access methods

R2

Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions

Provide the capability to disconnect or disable remote access to the system within

R3

Protect information about remote access mechanisms from unauthorized use and disclosure

Implement organization-defined mechanisms to authenticate organization-defined remote commands



CIP-005 NIST Cybersecurity Framework (CSF)

Function	Category	CSF SubCat ID	Subcategory
IDENTIFY (ID)	Asset Management (AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	ID.AM-4	ID.AM-4: External information systems are catalogued
PROTECT (PR)	Access Control (AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, or devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	PR.AC-3	PR.AC-3: Remote access is managed
PROTECT (PR)	Data Security (DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	PR.DS-2	PR.DS-2: Data-in-transit is protected
PROTECT (PR)	Maintenance (MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	PR.MA-2	PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access
PROTECT (PR)	Protective Technology (PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	PR.PT-4	PR.PT-4: Communications and control networks are protected
DETECT (DE)	Anomalies and Events (AE): Anomalous activity is detected and the potential impact of events is understood.	DE.AE-2	DE.AE-2: Detected events are analyzed to understand attack targets and methods
DETECT (DE)	Security Continuous Monitoring (CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	DE.CM-1	DE.CM-1: The network is monitored to detect potential cybersecurity events
DETECT (DE)	Detection Processes (DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	DE.DP-2	DE.DP-2: Detection activities comply with all applicable requirements



CIP-007 NIST Cybersecurity Framework (CSF)

Function	Category	CSF SubCat ID	Subcategory
PROTECT (PR)	Data Security (DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	PR.DS-5	PR.DS-5: Protections against data leaks are implemented
PROTECT (PR)	Information Protection Processes and Procedures (IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	PR.IP-12	PR.IP-12: A vulnerability management plan is developed and implemented
DETECT (DE)	Security Continuous Monitoring (CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	DE.CM-4	DE.CM-4: Malicious code is detected
DETECT (DE)	Security Continuous Monitoring (CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	DE.CM-5	DE.CM-5: Unauthorized mobile code is detected
DETECT (DE)	Security Continuous Monitoring (CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	DE.CM-7	DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed
DETECT (DE)	Detection Processes (DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	DE.DP-2	DE.DP-2: Detection activities comply with all applicable requirements



Resources

- ❑ [CIP-005-7 \(nerc.com\)](#)
- ❑ [CIP-007-6 \(nerc.com\)](#)
- ❑ [NIST Internal Controls](#) | [NIST 800-53 SP](#)
- ❑ [CIP Evidence Request Tool](#) | [Engagement Common Questions](#)
- ❑ [2024 ERO Enterprise Compliance Monitoring and Enforcement Program Implementation Plan](#)



The background of the slide features a blurred image of the Texas state flag on the left and a close-up of a wind turbine's hub and blades on the right. The blades are white with red tips. A dark blue rounded rectangle is centered over the image.

Questions?



TEXAS RE

Ensuring electric reliability for Texans