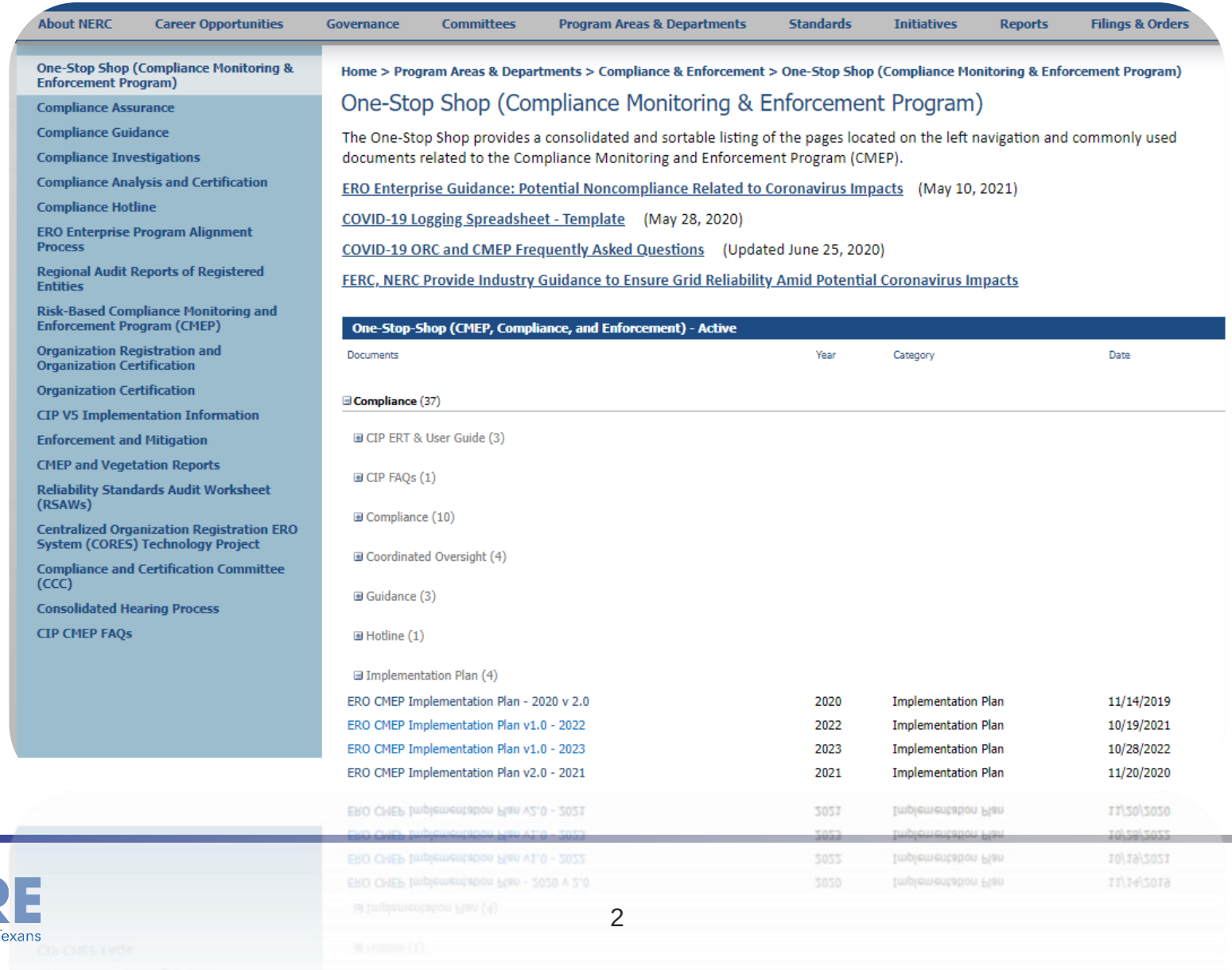
TEXAS RE

Ensuring electric reliability for Texans

CIP-005-7 R2 and R3 Remote Connectivity

Kenath Carver
Director, Cybersecurity Outreach
and CIP Compliance

ERO CMEP Implementation Plan 2023



About NERC | Career Opportunities | Governance | Committees | Program Areas & Departments | Standards | Initiatives | Reports | Filings & Orders

- One-Stop Shop (Compliance Monitoring & Enforcement Program)
- Compliance Assurance
- Compliance Guidance
- Compliance Investigations
- Compliance Analysis and Certification
- Compliance Hotline
- ERO Enterprise Program Alignment Process
- Regional Audit Reports of Registered Entities
- Risk-Based Compliance Monitoring and Enforcement Program (CMEP)
- Organization Registration and Organization Certification
- Organization Certification
- CIP V5 Implementation Information
- Enforcement and Mitigation
- CMEP and Vegetation Reports
- Reliability Standards Audit Worksheet (RSAWs)
- Centralized Organization Registration ERO System (CORES) Technology Project
- Compliance and Certification Committee (CCC)
- Consolidated Hearing Process
- CIP CMEP FAQs

Home > Program Areas & Departments > Compliance & Enforcement > One-Stop Shop (Compliance Monitoring & Enforcement Program)

One-Stop Shop (Compliance Monitoring & Enforcement Program)

The One-Stop Shop provides a consolidated and sortable listing of the pages located on the left navigation and commonly used documents related to the Compliance Monitoring and Enforcement Program (CMEP).

ERO Enterprise Guidance: Potential Noncompliance Related to Coronavirus Impacts (May 10, 2021)

COVID-19 Logging Spreadsheet - Template (May 28, 2020)

COVID-19 ORC and CMEP Frequently Asked Questions (Updated June 25, 2020)

FERC, NERC Provide Industry Guidance to Ensure Grid Reliability Amid Potential Coronavirus Impacts

One-Stop-Shop (CMEP, Compliance, and Enforcement) - Active

Documents	Year	Category	Date
Compliance (37)			
CIP ERT & User Guide (3)			
CIP FAQs (1)			
Compliance (10)			
Coordinated Oversight (4)			
Guidance (3)			
Hotline (1)			
Implementation Plan (4)			
ERO CMEP Implementation Plan - 2020 v 2.0	2020	Implementation Plan	11/14/2019
ERO CMEP Implementation Plan v1.0 - 2022	2022	Implementation Plan	10/19/2021
ERO CMEP Implementation Plan v1.0 - 2023	2023	Implementation Plan	10/28/2022
ERO CMEP Implementation Plan v2.0 - 2021	2021	Implementation Plan	11/20/2020

Risk Element Remote Connectivity

Remote Connectivity

The protection of critical infrastructure remains an area of elevated significance. This risk element focuses on the human element of security, one of the descriptors of cybersecurity vulnerabilities identified in the 2018 RISC report.[8] The 2021 RISC report[9] continues to emphasize the need to control poor cyber hygiene. The 2022 State of Reliability report[10] highlights supply chain compromise, geopolitical events, ransomware, and physical security threats as the primary cybersecurity threats to the BPS. A lesson learned from the coronavirus pandemic across all industries has been changes to the designed interaction between employees, vendors, and their workspaces which could have unintended effects on controls and protections of a remote workforce.

Regardless of the sophistication of a security system, there is potential for human error. Compliance monitoring should seek to understand how entities manage the risk of remote connectivity and the complexity of the tasks the individuals perform. If security has increased the difficulty in performing personnel's normal tasks, personnel may look for ways to circumvent the security to make it easier to perform their job. On the other hand, when an entity replaces complex tasks with automation, focus should be on: 1) whether the automation was correctly configured; 2) controls to ensure the automation is operating as intended; and 3) access controls to manage the granting and use of access.

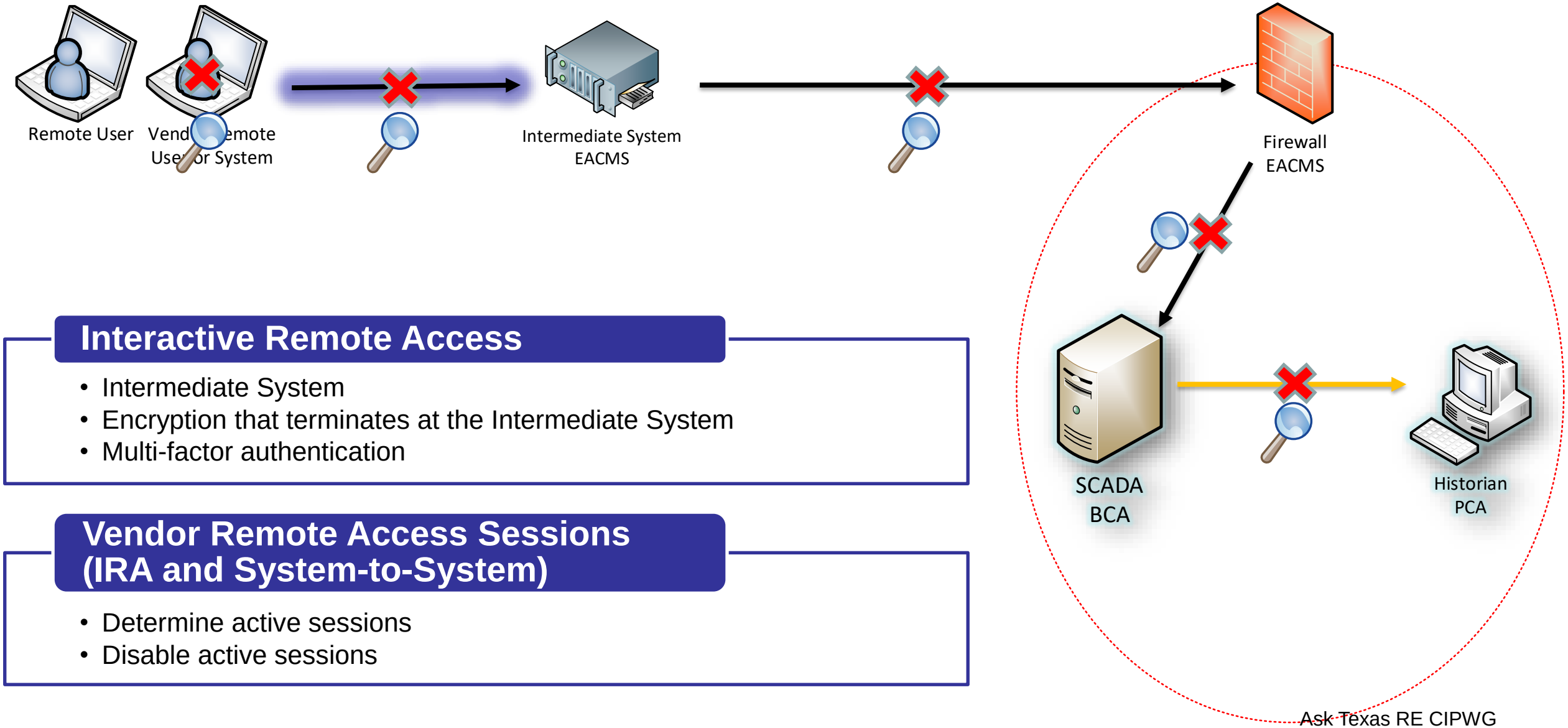
Harvesting credentials and exploiting physical and logical access of authorized users of BES facilities and Cyber Systems (BCSs) pose a major risk to systems that monitor and control the BES. With the target being users, privileged or non-privileged, who have authorized unescorted physical access and/or various levels of access to critical elements of the BES, the risk becomes elevated. By actively and covertly employing social engineering techniques and phishing emails, attackers may deceive authorized users to harvest credentials and gain unauthorized access.[11]

Areas of Focus

Table 3: Remote Connectivity

Rationale	Standard	Req	Entities for	Asset Types
Remote access to Critical Infrastructure Cyber Assets introducing increased attack surface, as well as possible increased exposure.	CIP-005-7	R2	Balancing Authority Distribution Provider Generator Operator Generator Owner Reliability Coordinator Transmission Operator Transmission Owner	Backup Control Centers Control Centers Data Centers Generation Facilities Transmission Facilities Substations
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	Backup Control Centers Control Centers Data Centers Generation Facilities Transmission Facilities Substations

CIP-005-7 R2



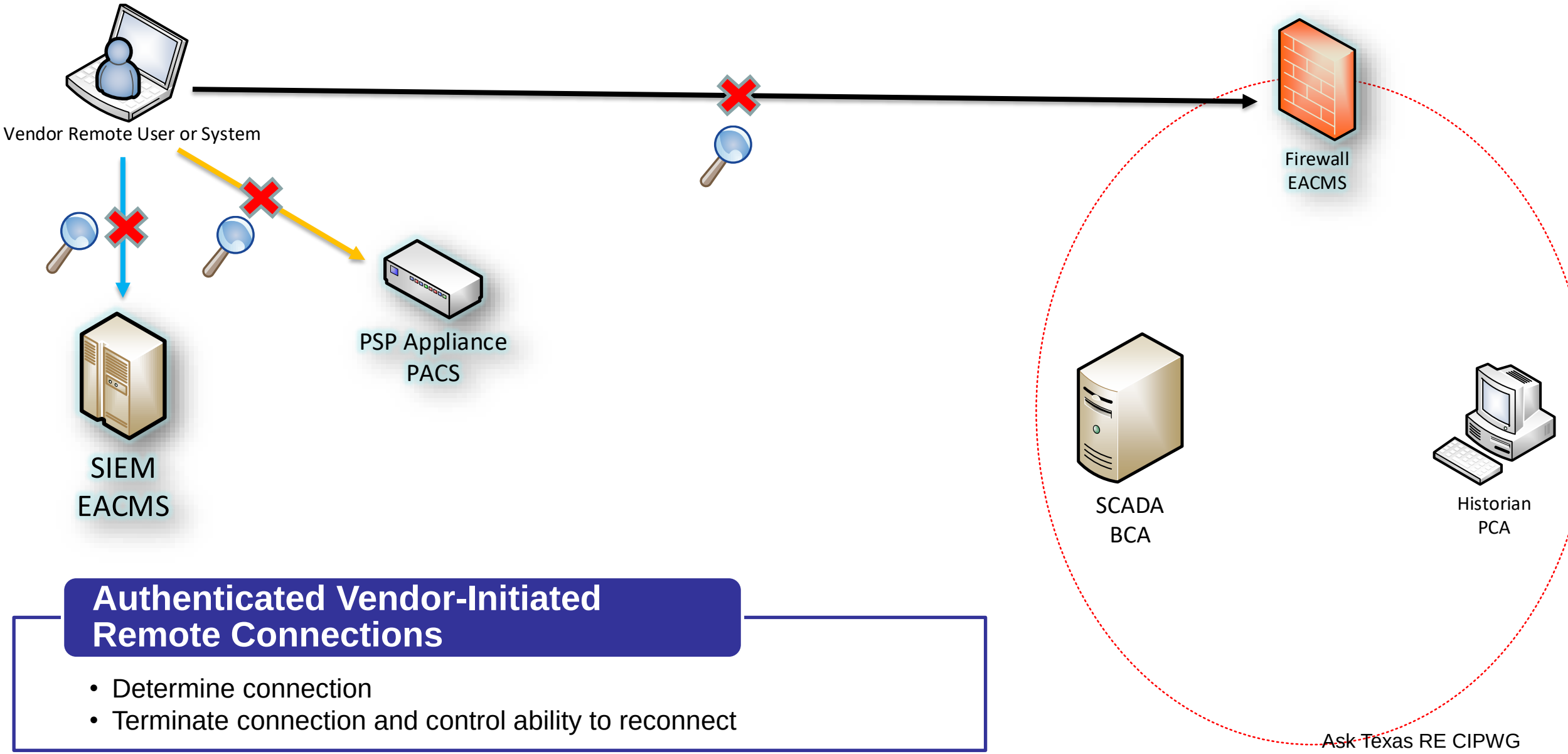
Interactive Remote Access

- Intermediate System
- Encryption that terminates at the Intermediate System
- Multi-factor authentication

Vendor Remote Access Sessions (IRA and System-to-System)

- Determine active sessions
- Disable active sessions

CIP-005-7 R3



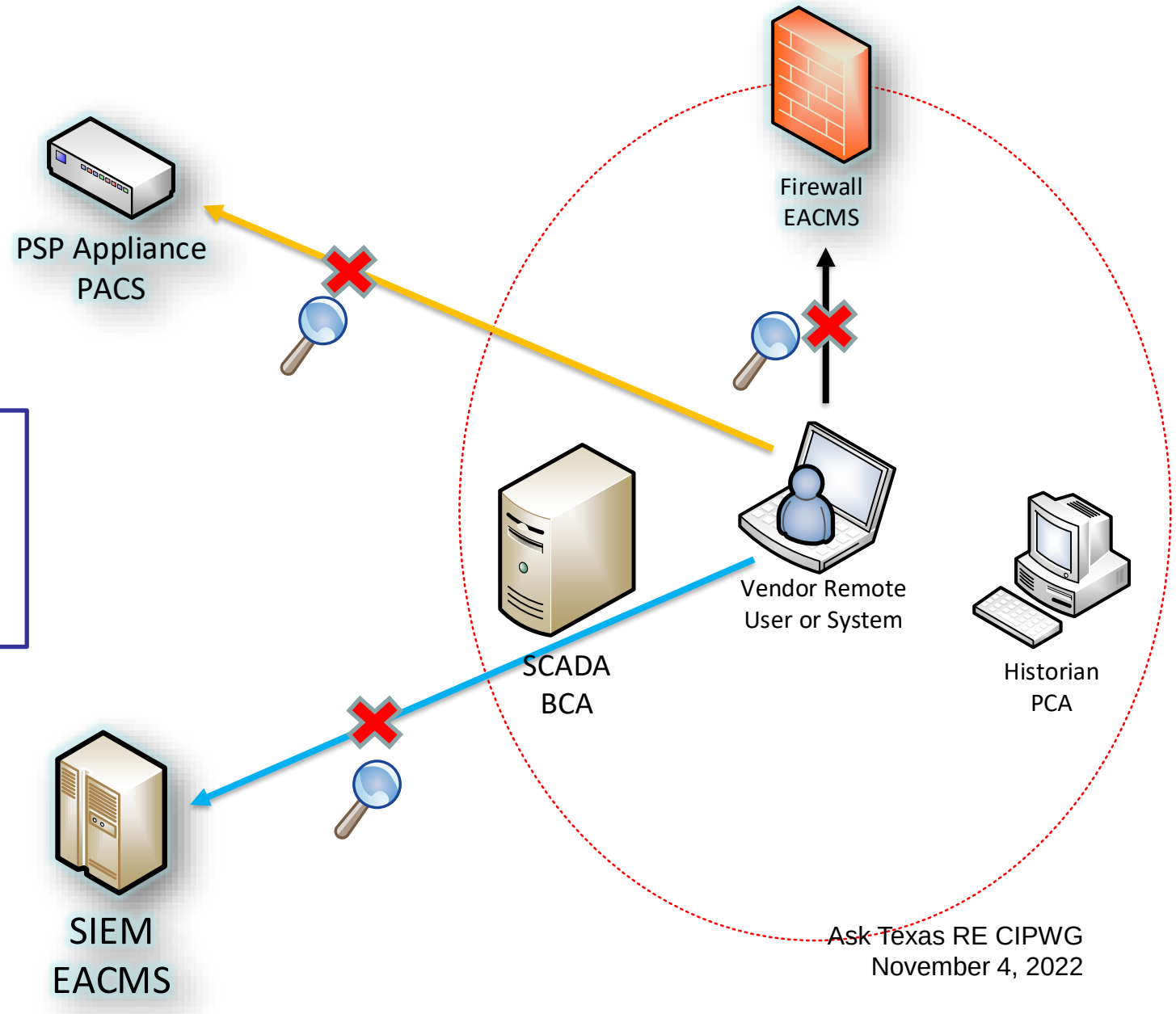
Authenticated Vendor-Initiated Remote Connections

- Determine connection
- Terminate connection and control ability to reconnect

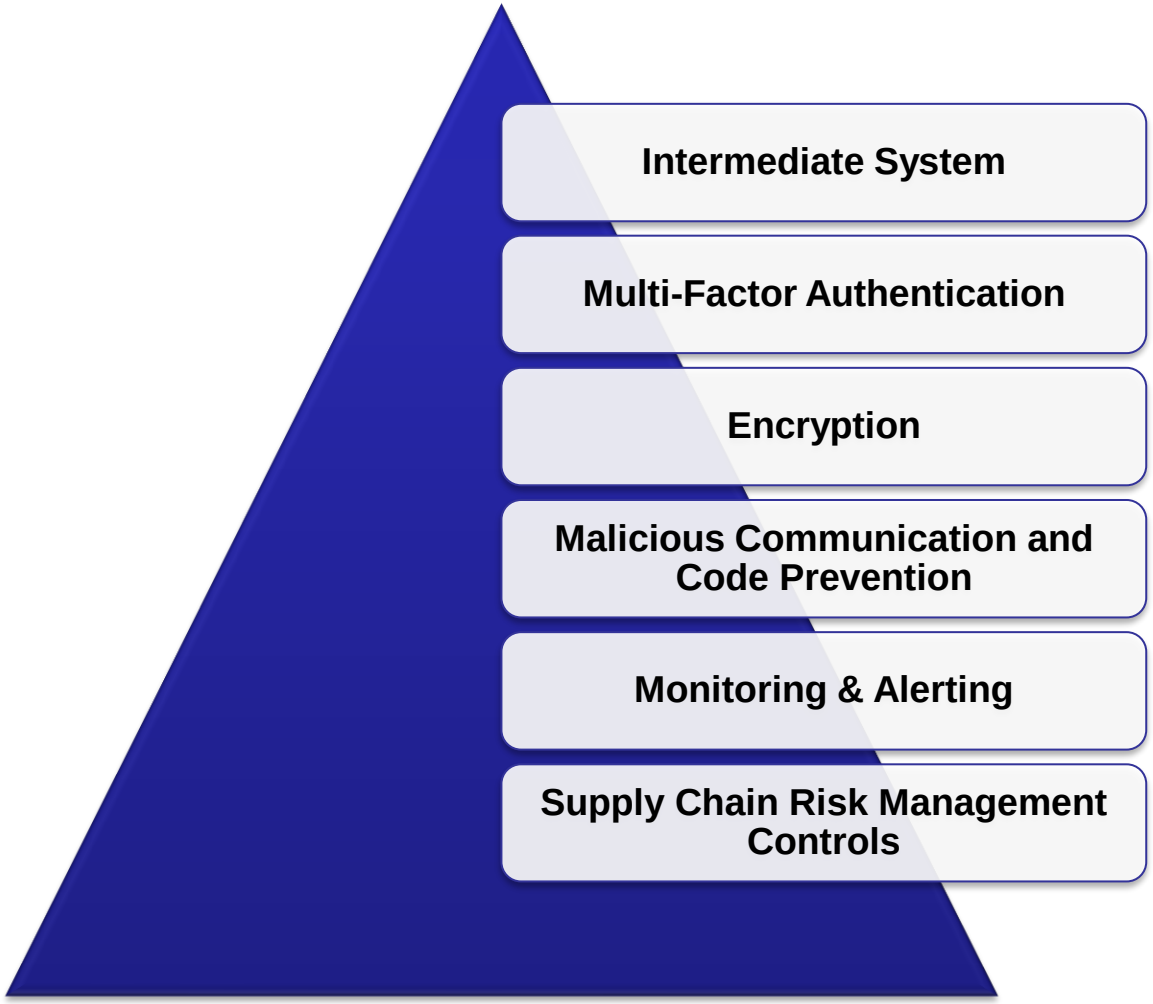
CIP-005-7 R3

Authenticated Vendor-Initiated Remote Connections

- Determine connection
- Terminate connection and control ability to reconnect



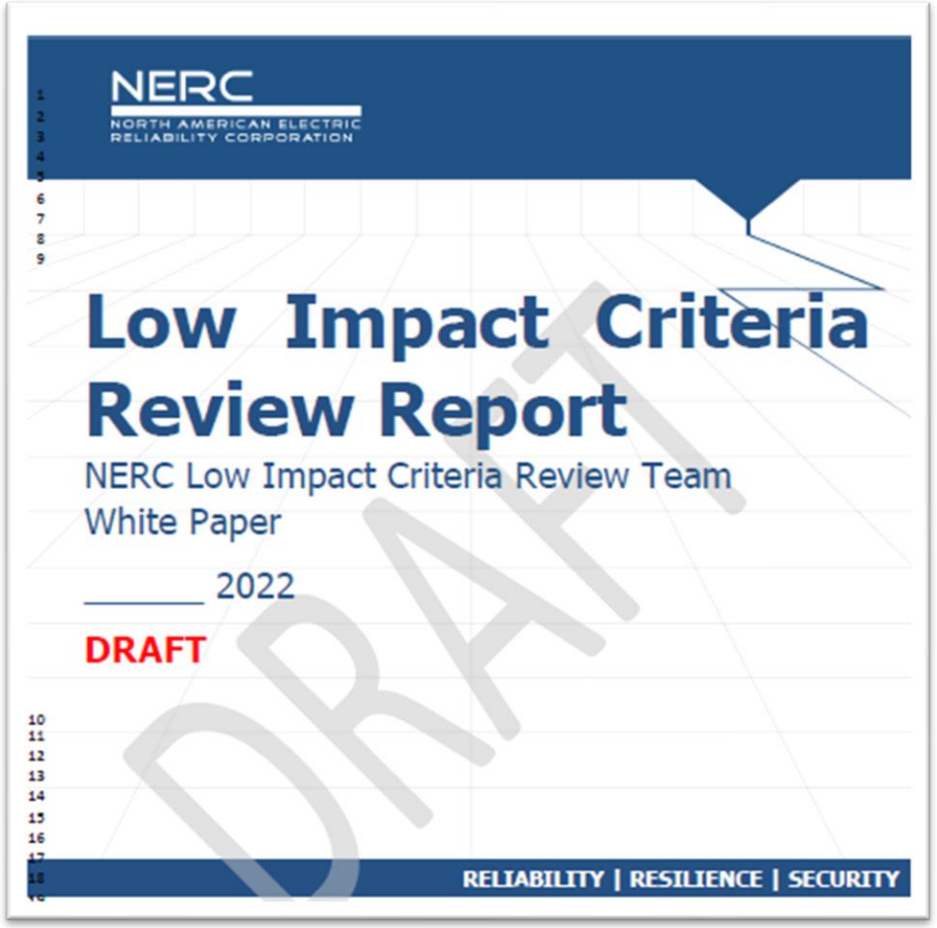
CIP Themes


Intermediate System
Multi-Factor Authentication
Encryption
Malicious Communication and Code Prevention
Monitoring & Alerting
Supply Chain Risk Management Controls

Project 2020-03 Supply Chain Low Impact Revisions

After considering policy input, the NERC Board adopted a resolution to initiate a project to modify Reliability Standard CIP-003-8 to include policies for low impact BES Cyber Systems to: (1) detect known or suspected malicious communications for both inbound and outbound communications; (2) determine when active vendor remote access sessions are initiated; and (3) disable active vendor remote access when necessary.

NERC Low Impact Criteria Review Team White Paper



CIP Standards Revisions

- Requirement(s) for authentication of remote users before access is granted to networks containing low impact BES Cyber Systems at assets containing those systems that have external routable connectivity.
- Requirement(s) for protection of user authentication information (e.g. combinations of usernames and passwords) for remote access to low impact BES Cyber Systems at assets containing those systems that have external routable connectivity.
- Requirement(s) for detection of malicious communications to/between low impact BES Cyber Systems at assets containing those systems that have external routable connectivity.

Security Guidelines

- Develop best practice guidance documents for protection of communications to and between low impact BES Cyber Systems across publicly accessible networks.
- Develop best practice guidance documents for procurement risk evaluation for low impact BES Cyber Systems.
- Develop best practice guidance documents for entities to voluntarily submit an E-ISAC report for unauthorized physical access attempts to low impact BES Cyber Systems.

Risk Monitoring

- Continuous monitoring of E-ISAC physical access attempt reports to low impact BES Cyber Systems to determine if the risk increases over time and should be addressed.

TEXAS RE
Ensuring electric reliability for Texans