RELIABILITY 101 & 201

CIP 201: Security Patch Management

Jonathan Espinosa
Physical and Cyber Security Analyst II

June 17, 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 Sessions

- June 3 – History and Introduction to Texas RE
- June 4 – Registration & Certification
- June 5 – Intro to Align
- June 6 – Risk-Based Approach to Reliability
- June 10 – Foundations of CIP Programs
- June 11 – Foundations of O&P Programs
- June 12 – Navigating Noncompliance Resolutions
- June 13 – NERC Data Collection, Events Analysis, and Guidelines
- June 17 – Reliability 201: Security Patch Management
- June 18 – Reliability 201: O&P
- June 24 – Reliability 201: CMEP Feedback Loop
- June 25 – Reliability 201: Compliance in Align Walkthrough
- June 25 – Reliability 201: Reliability Services

JUNE 2024

SUN	MON	TUE	WED	THU	FRI	SAT
						1
2	3 ●	4 ●	5 ●	6 ●	7	8
9	10 ●	11 ●	12 ●	13 ●	14	15
16	17 ●	18 ●	19 ✪	20	21	22
23	24 ●	25 ● ●	26 talk with TEXAS RE	27 talk with TEXAS RE	28	29
30						

TEXAS RE

Ensuring electric reliability for Texans

Cyber and Physical Security Workshop
August 28, 2024

Upcoming ERO Enterprise Events

May - July, 2024

GADS Wind & Solar Template and Application Training

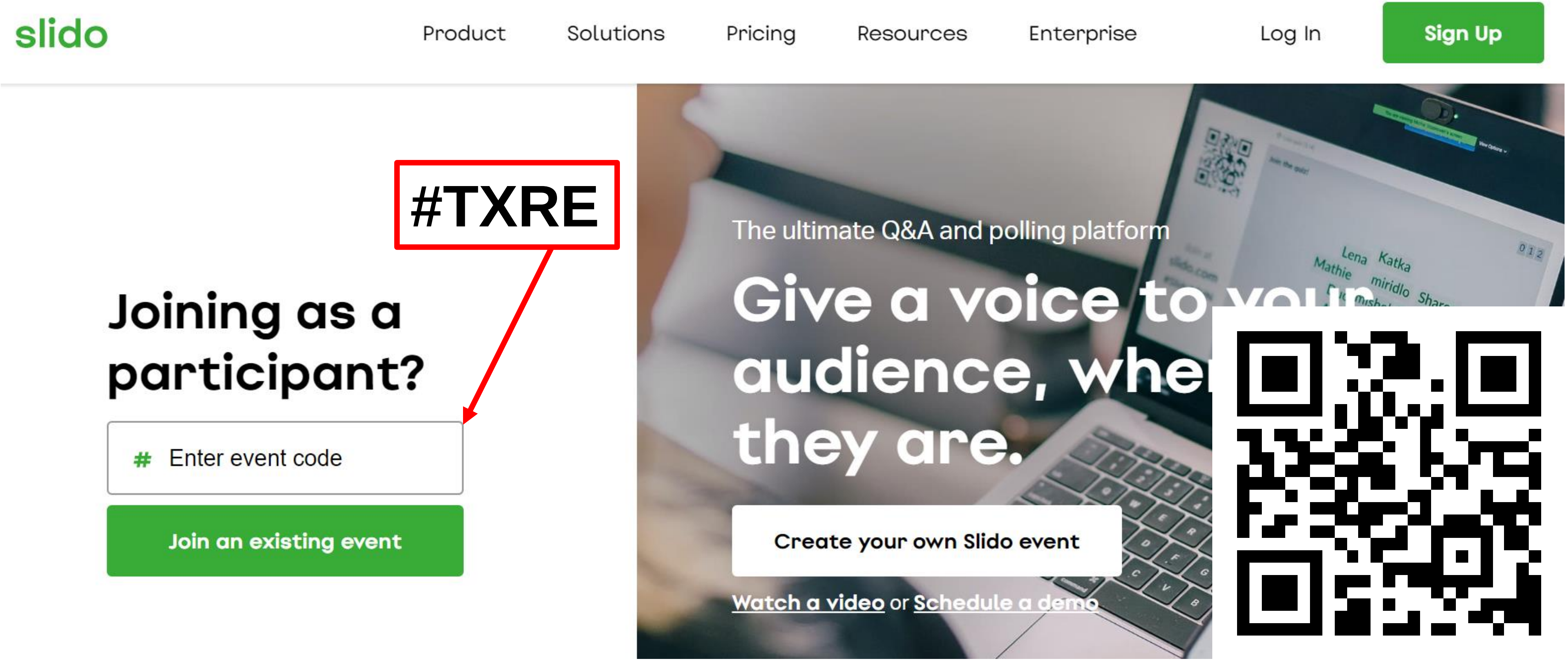
June 27, 2024

Regional Summer Assessment Webinar

July 16-18, 2024

Physical Security Workshop

Sli.do



#TXRE

Joining as a participant?

The ultimate Q&A and polling platform

Give a voice to your audience, wherever they are.

Agenda

CIP-007-6 R2

Topics of Consideration

Examples

Resources

Public

Why We Are Here

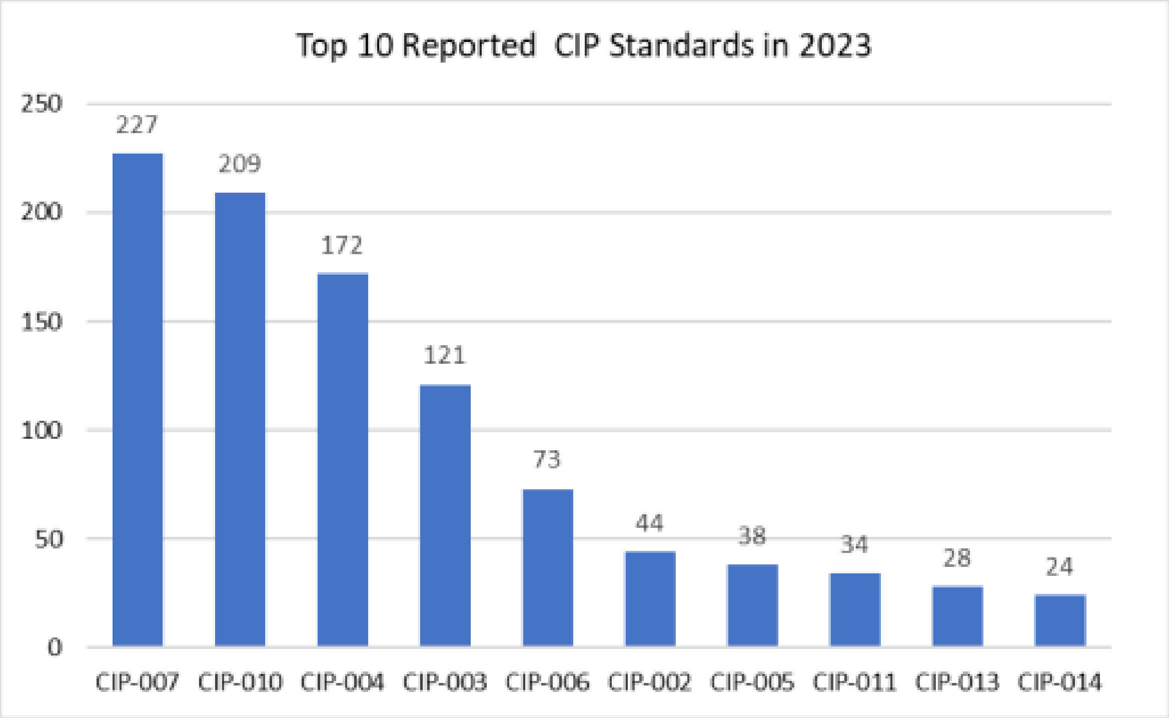
Continued risk from software and hardware vulnerabilities

- Vulnerabilities in the network equipment that protects BES Cyber Assets
- Other recent events include, MoveIT, Log4J, and SolarWinds

Why We Are Here (Cont.)

CIP Noncompliance Reported in 2023

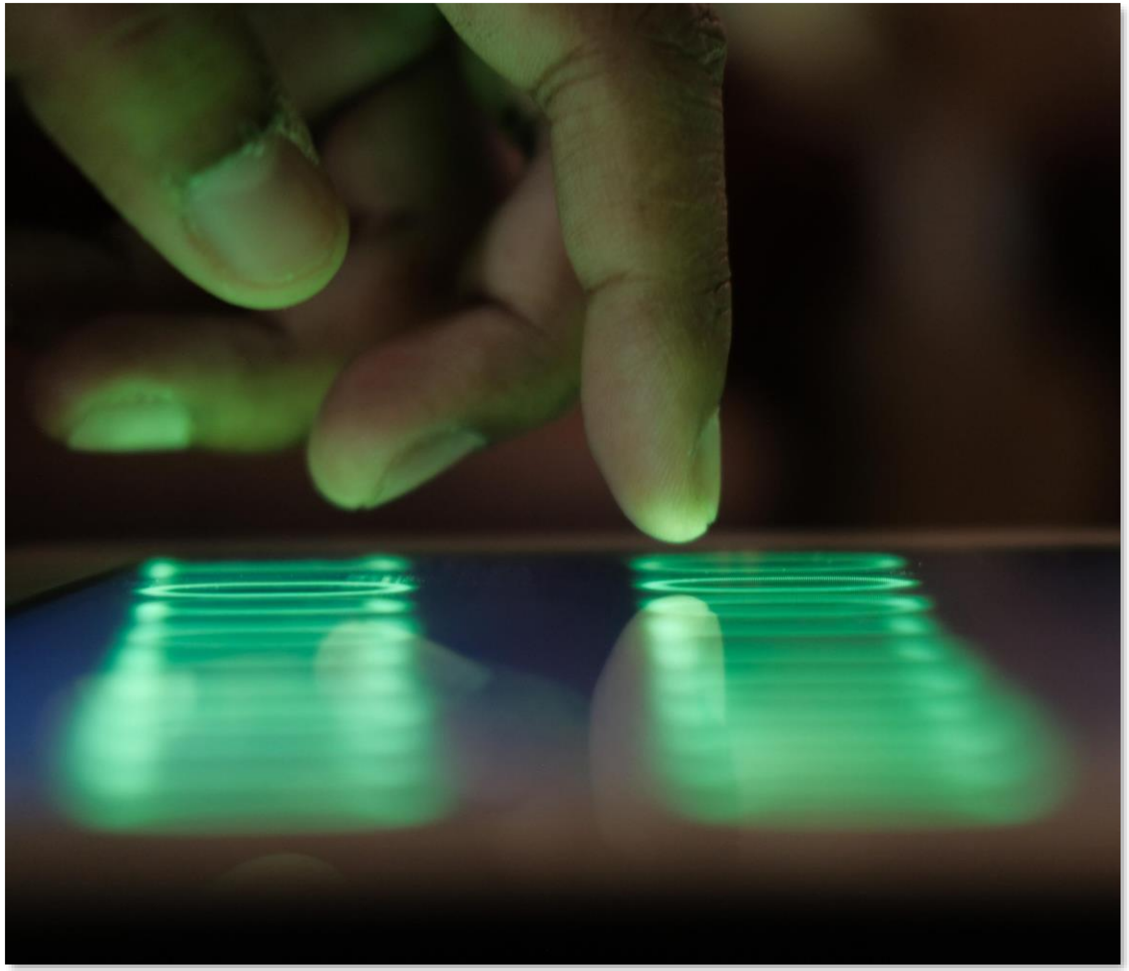
- The most frequently reported noncompliance involving CIP standards
- CIP-007 holds top spot
- Standards that involve high volume and high frequency conduct



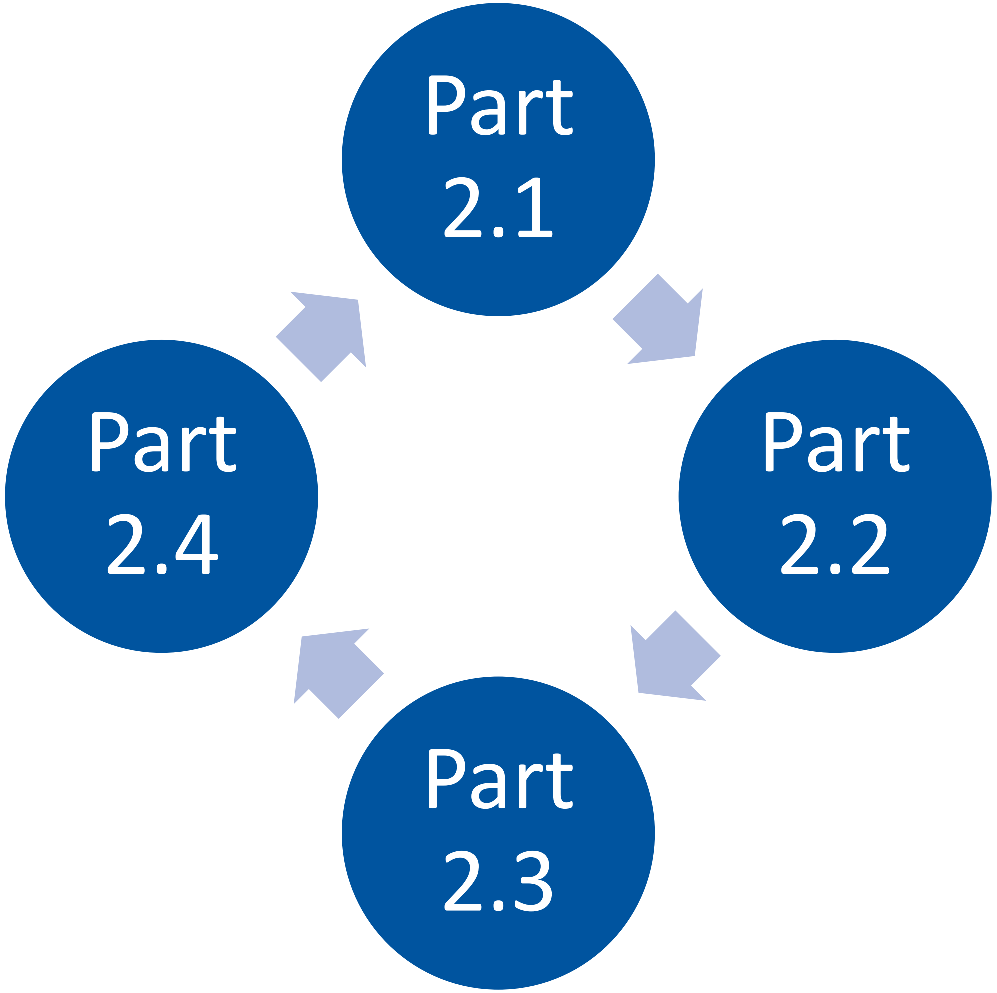
CIP-007-6 Cyber Security—Systems Security Management

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 Requirement 2



Sli.do (#TXRE)

Slido Question

What are some issues that can occur due to poor security patch management?

CIP-007-6 Requirement 2 (Cont.)

Applicable Systems

High Impact BES Cyber Systems and their associated:

- EACMS;
- PACS; and
- PCA

Medium Impact BES Cyber Systems and their associated:

- EACMS;
- PACS; and
- PCA

CIP-007-6 Part 2.1

A patch management process for tracking, evaluating, and installing cybersecurity patches for applicable Cyber Assets

The tracking portion shall include the identification of a source, or sources used for tracking

Cybersecurity Patches

Are:

- Patches that address a specific vulnerability in a hardware or software product

Are Not:

- Patches regarding functionality without a cybersecurity impact
- Patches that apply to a service or component that is not installed or enabled

CIP-007-6 Part 2.1 (Cont.)

Examples of Evidence

- Patch management Process
- List of monitored sources
  - BES Cyber System; or
  - BES Cyber Asset

CIP-007-6 Part 2.1 (Cont.)

Considerations

- Does your process language include detailed Instructions?
- How is compliance documentation stored?
- Does your process include controls to track applicable Cyber Assets?

CIP-007-6 Part 2.2

Requirement

At least once every 35 calendar days, **evaluate** security patches for applicability that have been released since the last evaluation from the **source or sources** identified in Part 2.1

Considerations

- Controls around requirement deadlines
- What is your process to verify the end date of the evaluation?

Examples of Evidence

An evaluation conducted by, referenced by, or on behalf of a Responsible Entity of security-related patches released by the document sources at least once every 35 calendar days

CIP-007-6 Part 2.3

For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion take one of the following actions:

- Apply the applicable patches
- Create a dated mitigation plan
- Revise an existing mitigation plan

Mitigation plans shall include the planned actions to mitigate the vulnerabilities addressed by each security patch and a timeframe to complete the mitigations

CIP-007-6 Part 2.3 (Cont.)

Example evidence

- Records of the installation of the patch; or
- A dated plan showing when and how the vulnerability will be addressed.

Considerations

- How do you verify the installation date of patches?
- What controls are in place to verify the patch was installed?
- Do your Mitigation plan’s actions address the vulnerabilities?

CIP-007-6 Part 2.4

For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.

CIP-007-6 Part 2.4 (Cont.)

Example evidence

- Records demonstrating mitigation plans were implemented
- Records demonstrating that a revision or extension specified in part 2.3 was approved by the CIP Senior Manager or their delegate

CIP-007-6 Part 2.4 (Cont.)

Topics of Consideration

- How are mitigation plan deadlines tracked?
- How is implementation evidence of mitigation plans stored?
- Do you have a process to ensure mitigation plan(s) are approved by the CIP Senior Manager or their delegate?

Sli.do (#TXRE)

Slido Question

What are some tools that can help achieve compliance with CIP-007-6 R2?

CIP-007-6 R2—Example

Cybersecurity Patch Tracking
BES Cyber System/BES Cyber Asset: Cyber Asset Index ID 1, 5, 6, 8, 9
Vendor: Network Equipment Vendor
Software/Hardware Product: Firewall 9000
Software/Firmware Version: Firewall OS v1.1
Source: www[.]networkdevices[.]com/downloads/firewall9000
Notes:

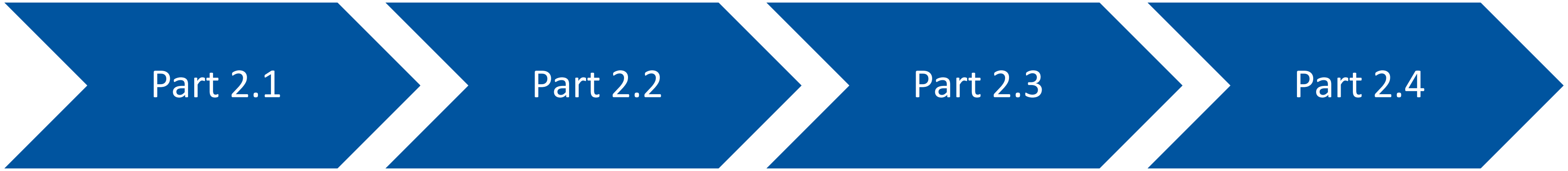
Cybersecurity Patch Management
Ticket Number: 23-0001
Date: 5/08/2024
Cybersecurity Patch Information: A cross-site scripting vulnerability exists in the web based configuration utility.
Impacted BES Cyber Assets: Cyber Asset Index ID 1, 5, 6, 8, and 9
Evaluation: Patch addresses vulnerability in the web based configuration utility used to manage Cyber Asset Index ID 1, 5, 6, 8, and 9. Date of Evaluation: 5/18/2024
Installation: Dated screenshot demonstrating patch was installed. 🗎 Install.png
Installation Date: 6/02/2024
Notes:

CIP-007-6 R2—Example (Cont.)

Cybersecurity Patch Management
Ticket Number: 23-0002
Date: 7/10/2023
Cybersecurity Patch Information: Remote Code Execution vulnerability that may allow a remote unauthenticated attacker to execute code on Cyber Assets Running OS Version v10.1.
Impacted BES Cyber Assets: BES Cyber Asset Index ID 15, 23, 32, 45.
Evaluation: Completed, patch is an applicable cybersecurity patch to address remote code execution. **Date of Evaluation:** 7/15/2023
Installation: Patch will not be installed due to impact on reliability. Mitigation Plan will need to be created.
Installation Date: N/A
Rollback Plan: N/A

Mitigation Plan
Ticket Number: 23-0002
Date: 8/02/2023
Mitigation Plan Information: Mitigation plan for OS vulnerability impacting four BES Cyber Assets.
Impacted BES Cyber Assets: BES Cyber Asset Index ID 15, 23, 32, 45
Planned Actions to Mitigate Vulnerabilities: Impacted Cyber Assets will be isolated from the rest of the network via the creation of VLANs, additionally we will limit access to the VLAN by limiting the number of Cyber Assets that are able to communicate to the created VLAN.
Timeframe to Complete Mitigations: 5 calendar days. To complete by 8/15/2023.
Revision/Extension: N/A
Approval by CIP Senior Manager or Delegate: N/A

CIP-007-6 Requirement 2 Recap



Part 2.1

- A patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets

Part 2.2

- At least once every 35 calendars days evaluate security patches for applicability

Part 2.3

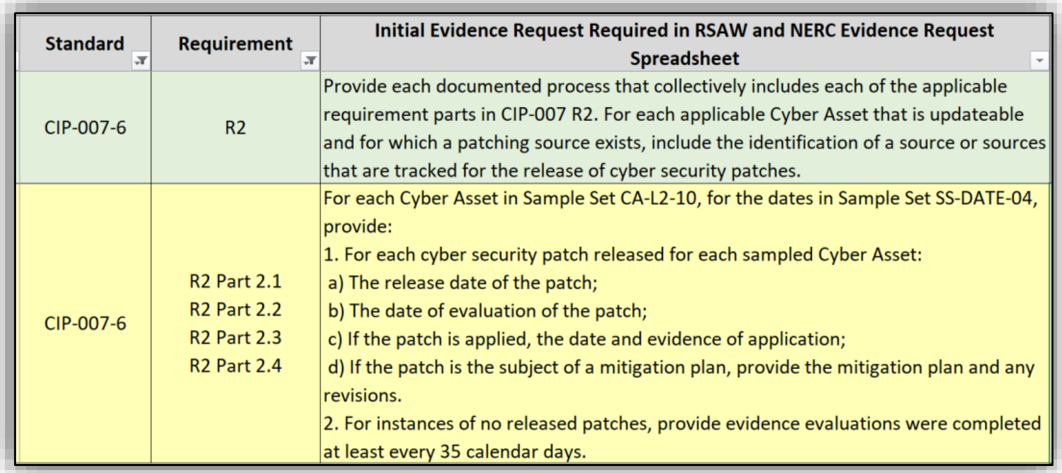
- Within 35 calendar days:
  - Apply the applicable patches; or
  - Create a dated mitigation plan; or
  - Revise an existing mitigation plan

Part 2.4

- For each revised or created mitigation plan implement the plan within the timeframe specified
- Unless a revision or extension is approved by CIP Senior Manager or Delegate

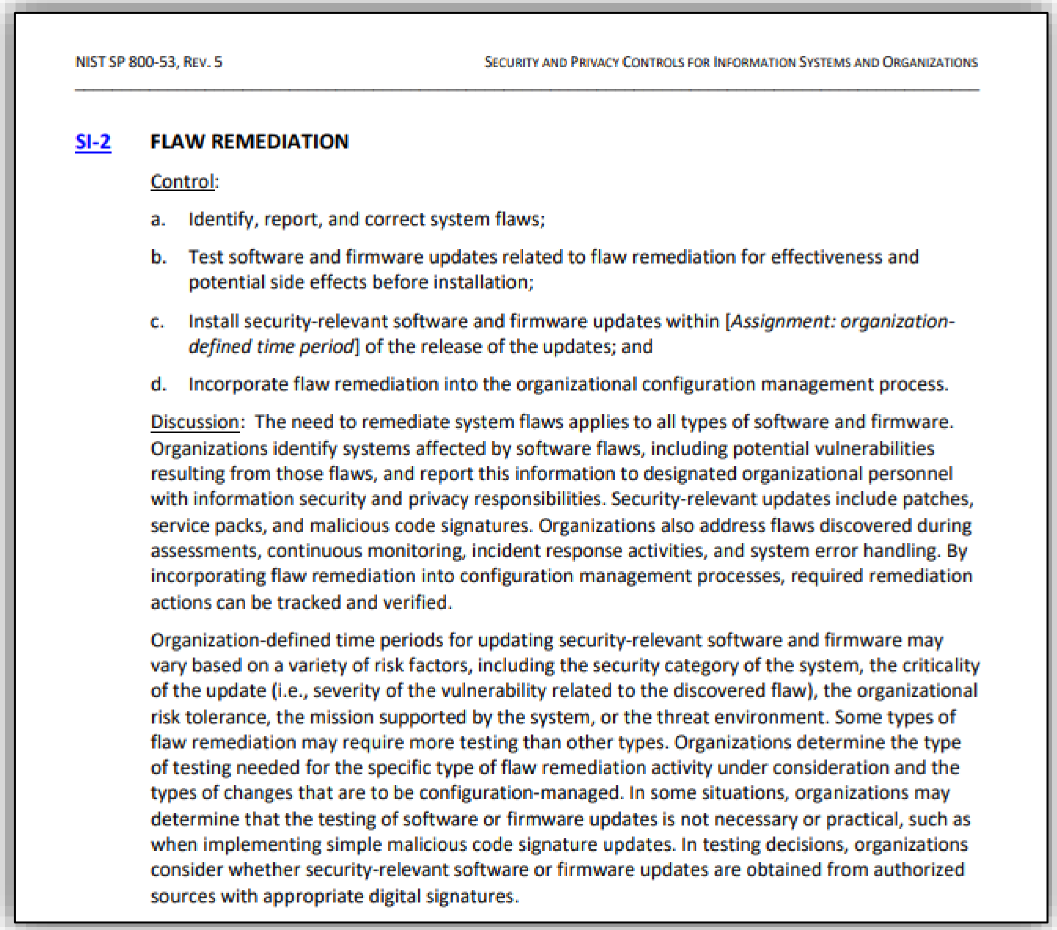
Implementation Resources

CIP Evidence Request Tool



Standard	Requirement	Initial Evidence Request Required in RSAW and NERC Evidence Request Spreadsheet
CIP-007-6	R2	Provide each documented process that collectively includes each of the applicable requirement parts in CIP-007 R2. For each applicable Cyber Asset that is updateable and for which a patching source exists, include the identification of a source or sources that are tracked for the release of cyber security patches.
CIP-007-6	R2 Part 2.1 R2 Part 2.2 R2 Part 2.3 R2 Part 2.4	For each Cyber Asset in Sample Set CA-L2-10, for the dates in Sample Set SS-DATE-04, provide: 1. For each cyber security patch released for each sampled Cyber Asset: a) The release date of the patch; b) The date of evaluation of the patch; c) If the patch is applied, the date and evidence of application; d) If the patch is the subject of a mitigation plan, provide the mitigation plan and any revisions. 2. For instances of no released patches, provide evidence evaluations were completed at least every 35 calendar days.

NIST SP 800-53, Rev. 5



NIST SP 800-53, Rev. 5 SECURITY AND PRIVACY CONTROLS FOR INFORMATION SYSTEMS AND ORGANIZATIONS

SI-2 FLAW REMEDIATION

Control:

a. Identify, report, and correct system flaws;

b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;

c. Install security-relevant software and firmware updates within [*Assignment: organization-defined time period*] of the release of the updates; and

d. Incorporate flaw remediation into the organizational configuration management process.

Discussion: The need to remediate system flaws applies to all types of software and firmware. Organizations identify systems affected by software flaws, including potential vulnerabilities resulting from those flaws, and report this information to designated organizational personnel with information security and privacy responsibilities. Security-relevant updates include patches, service packs, and malicious code signatures. Organizations also address flaws discovered during assessments, continuous monitoring, incident response activities, and system error handling. By incorporating flaw remediation into configuration management processes, required remediation actions can be tracked and verified.

Organization-defined time periods for updating security-relevant software and firmware may vary based on a variety of risk factors, including the security category of the system, the criticality of the update (i.e., severity of the vulnerability related to the discovered flaw), the organizational risk tolerance, the mission supported by the system, or the threat environment. Some types of flaw remediation may require more testing than other types. Organizations determine the type of testing needed for the specific type of flaw remediation activity under consideration and the types of changes that are to be configuration-managed. In some situations, organizations may determine that the testing of software or firmware updates is not necessary or practical, such as when implementing simple malicious code signature updates. In testing decisions, organizations consider whether security-relevant software or firmware updates are obtained from authorized sources with appropriate digital signatures.

Implementation Resources (Cont.)

NIST SP 800-53, Rev. 5

SI-2 Flaw Remediation

- Review “Related Controls.”

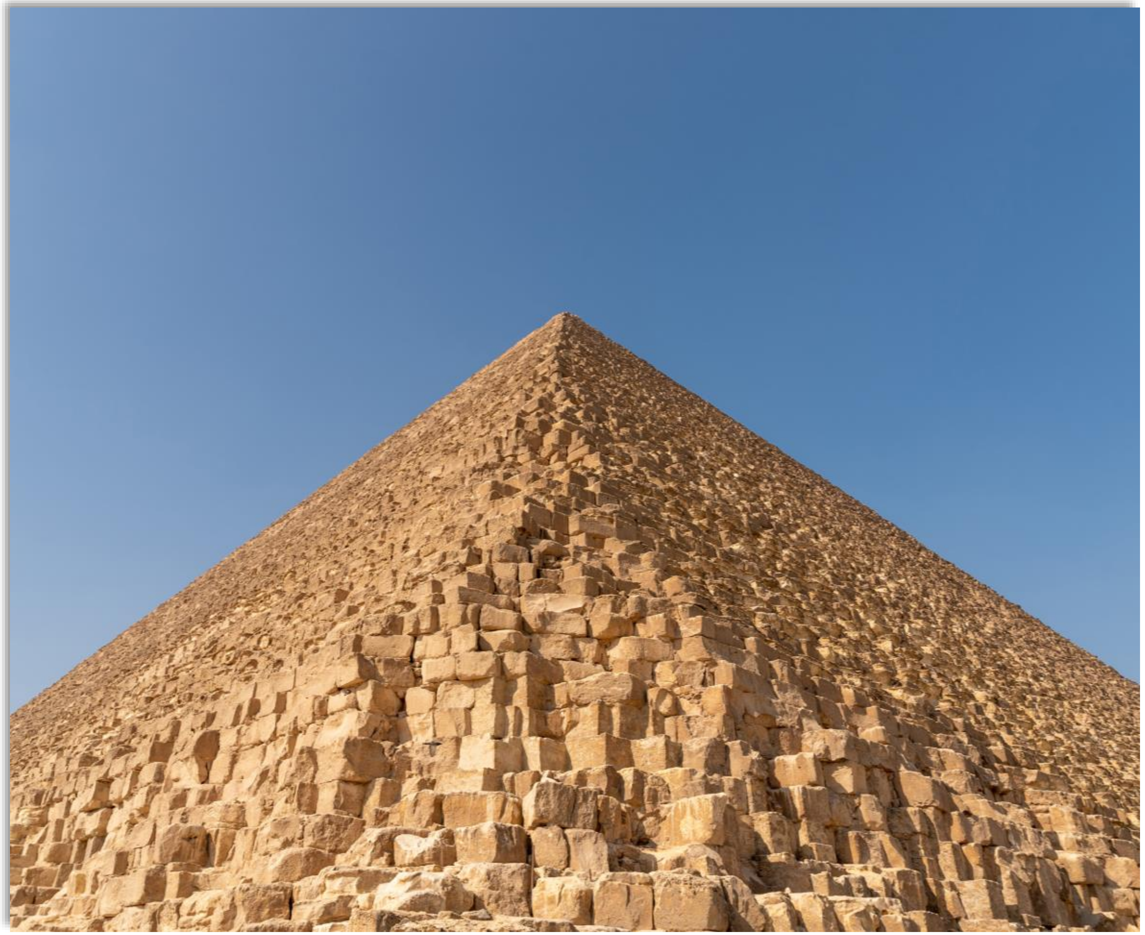
CA-5 Plan of Action & Milestones

- “Track planned remedial actions.”

CM-3 Configuration Change Control

- “Configuration change control for organizational systems involves the systematic proposal, justification, implementation, testing, review, and disposition of system changes, including system upgrades and modifications.”

Pyramid of Pain



TTPs

- Tough

Tools

- Challenging

Network/Host Artifacts

- Annoying

Domain Names

- Simple

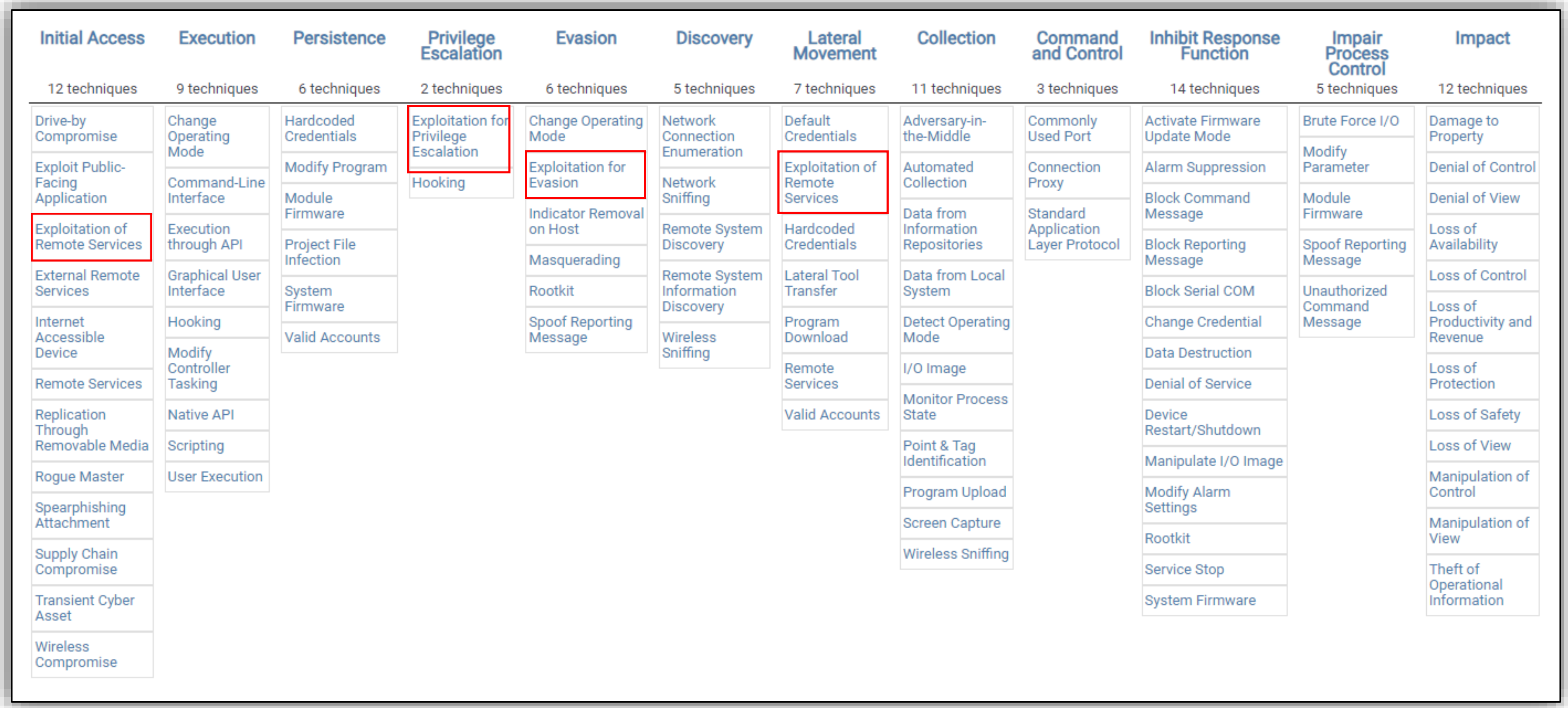
IP Addresses

- Easy

Hash Values

- Trivial

MITRE ATT&CK® for Industrial Control Systems



Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
12 techniques	9 techniques	6 techniques	2 techniques	6 techniques	5 techniques	7 techniques	11 techniques	3 techniques	14 techniques	5 techniques	12 techniques
Drive-by Compromise	Change Operating Mode	Hardcoded Credentials	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Adversary-in-the-Middle	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Exploit Public-Facing Application	Command-Line Interface	Modify Program	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Automated Collection	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Exploitation of Remote Services	Execution through API	Module Firmware		Indicator Removal on Host	Remote System Discovery	Hardcoded Credentials	Data from Information Repositories	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
External Remote Services	Graphical User Interface	Project File Infection		Masquerading	Remote System Information Discovery	Lateral Tool Transfer	Data from Local System		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Internet Accessible Device	Hooking	System Firmware		Rootkit	Wireless Sniffing	Program Download	Detect Operating Mode		Block Serial COM	Unauthorized Command Message	Loss of Control
Remote Services	Modify Controller Tasking	Valid Accounts		Spoof Reporting Message		Remote Services	I/O Image		Change Credential		Loss of Productivity and Revenue
Replication Through Removable Media	Native API					Valid Accounts	Monitor Process State		Data Destruction		Loss of Protection
Rogue Master	Scripting						Point & Tag Identification		Denial of Service		Loss of Safety
Spearphishing Attachment	User Execution						Program Upload		Device Restart/Shutdown		Loss of View
Supply Chain Compromise							Screen Capture		Manipulate I/O Image		Manipulation of Control
Transient Cyber Asset							Wireless Sniffing		Modify Alarm Settings		Manipulation of View
Wireless Compromise									Rootkit		Theft of Operational Information
									Service Stop		
									System Firmware		

Contact

Jonathan Espinosa
CIP Cyber and Physical Security Analyst
Jonathan.Espinosa@texasre.org
512-583-4930

Questions?

TEXAS RE

Ensuring electric reliability for Texans