Critical Infrastructure Protection WORKSHOP

June 3, 2021

Agenda

Intro and Instructions

Supply Chain Compliance Presentation

Supply Chain Security Panel

CIP-012 Compliance Presentation

CIP-012 Security Panel

CIP-008-6 Compliance Presentation

CIP-008-6 Security Panel

E-ISAC Update Presentation

Wrap-Up

TEXAS RE

Ensuring electric reliability for Texans

Welcome and Instructions

Matthew Barbour

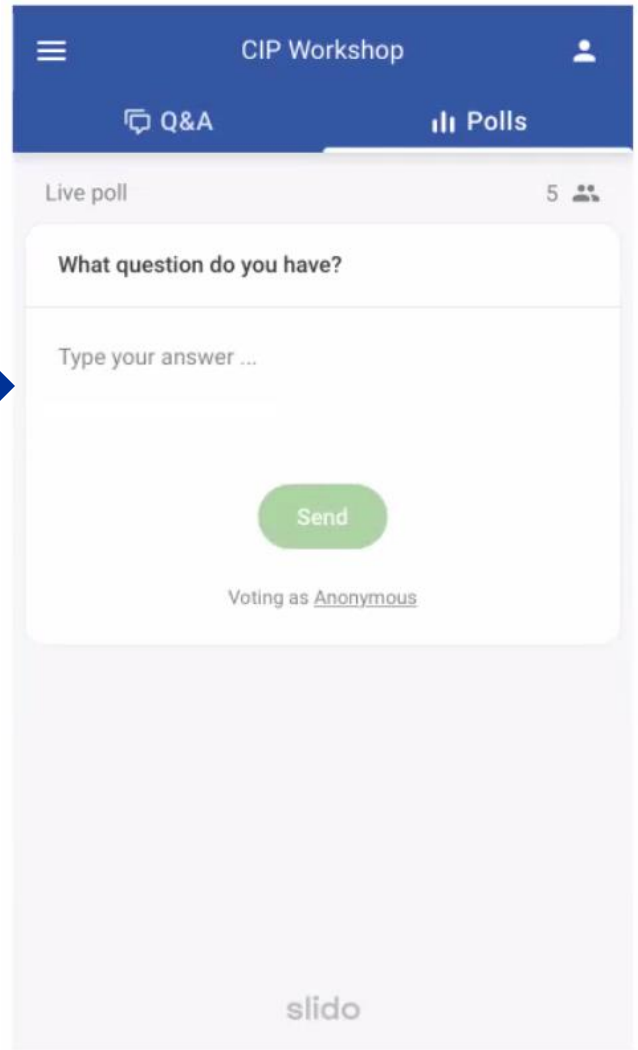
Manager, Communications and Training

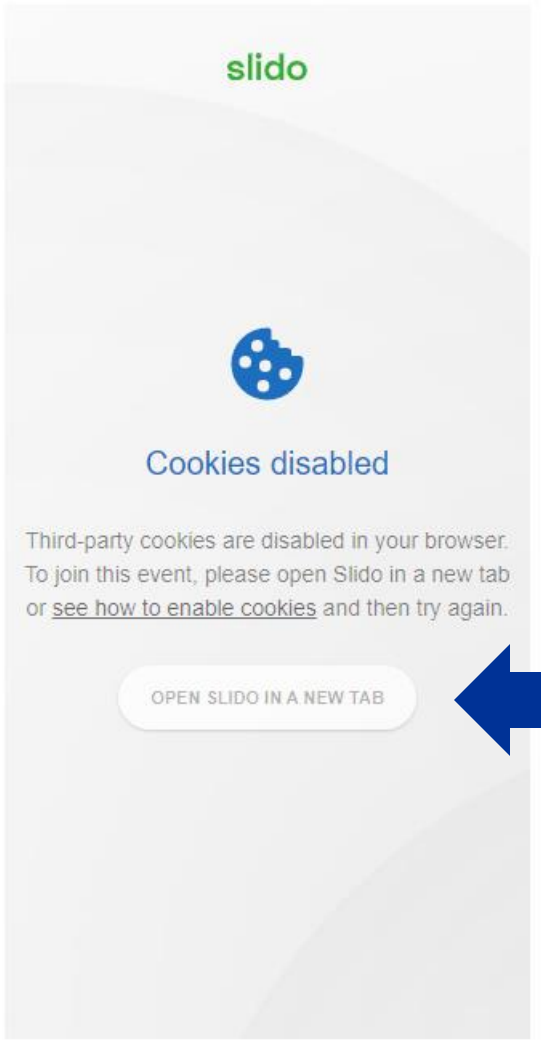
Antitrust Admonition

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 the open portion of 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.

Feedback


CIP Workshop
Q&A
Polls
Live poll
5
What question do you have?
Type your answer ...
Send
Voting as Anonymous
slido


slido
Cookies disabled
Third-party cookies are disabled in your browser. To join this event, please open Slido in a new tab or see how to enable cookies and then try again.
OPEN SLIDO IN A NEW TAB

Sli.do Participation Alternatives

Enter the participant code at Slido.com

#TXCIP

OR

Scan the QR code

Survey

CIP Workshop Survey

* 1. How was your overall workshop experience?

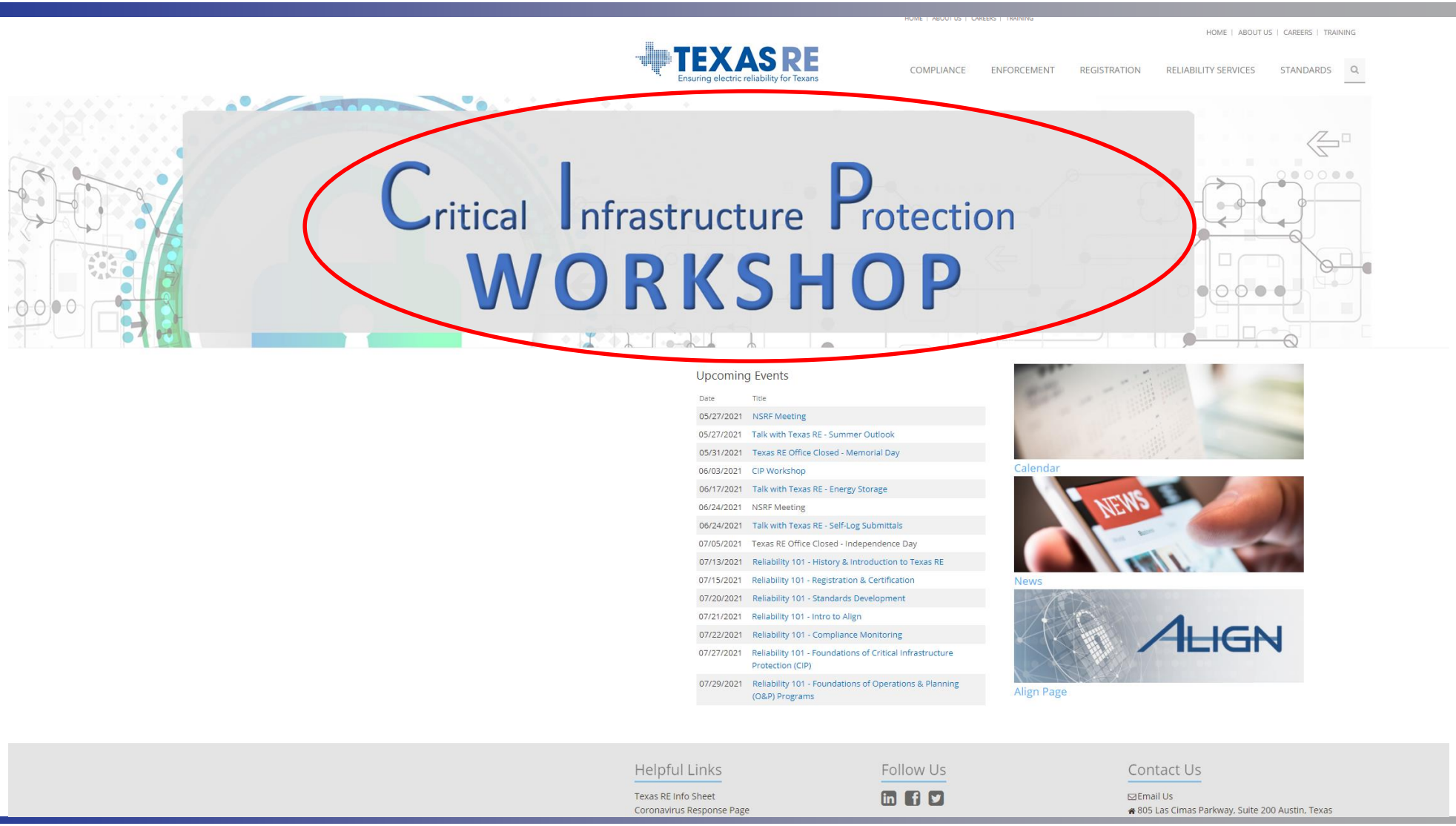
- ◯ Excellent
- ◯ Below Average
- ◯ Good
- ◯ Poor
- ◯ OK

Comment

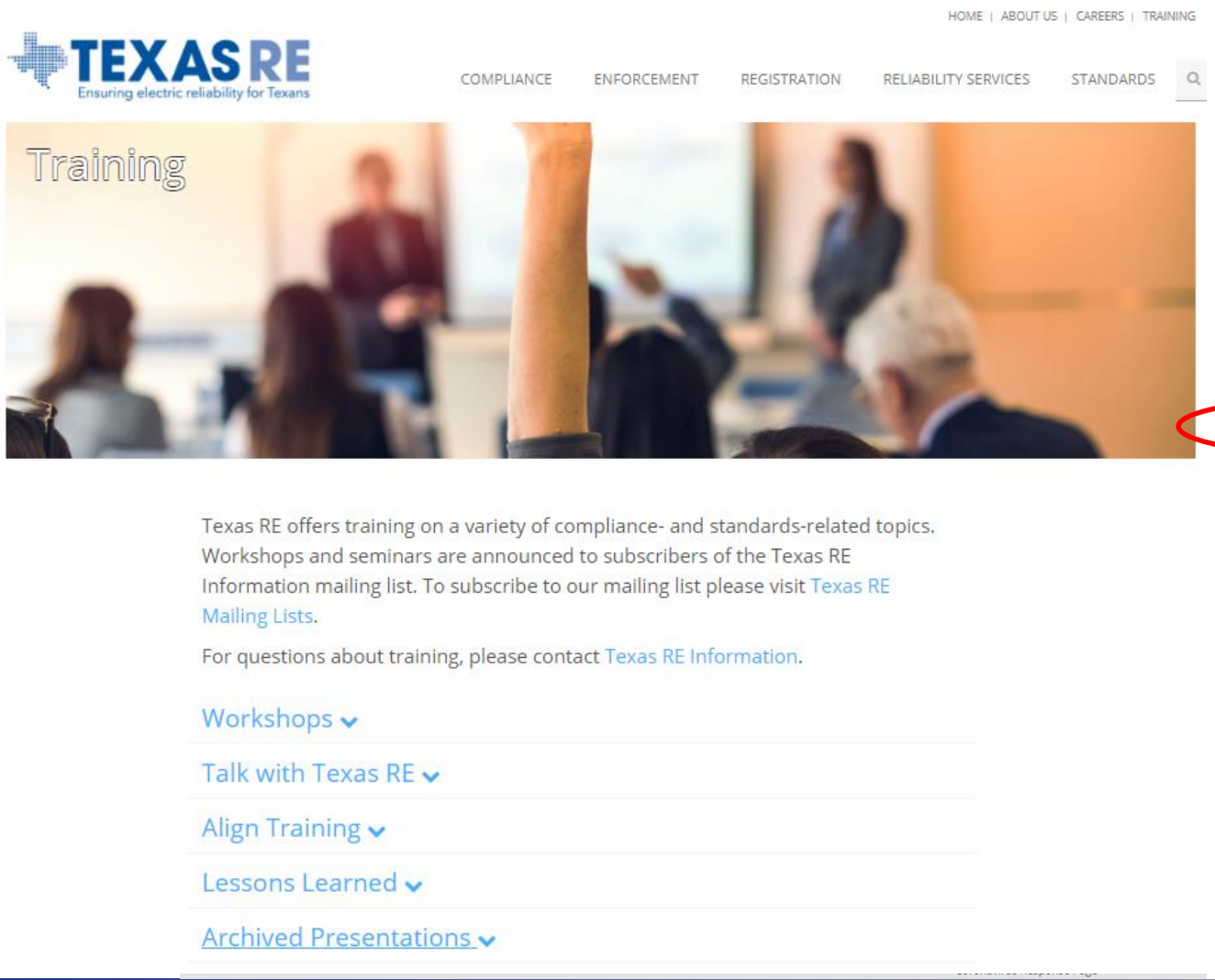
2. How would you rate the Supply Chain Compliance presentation?

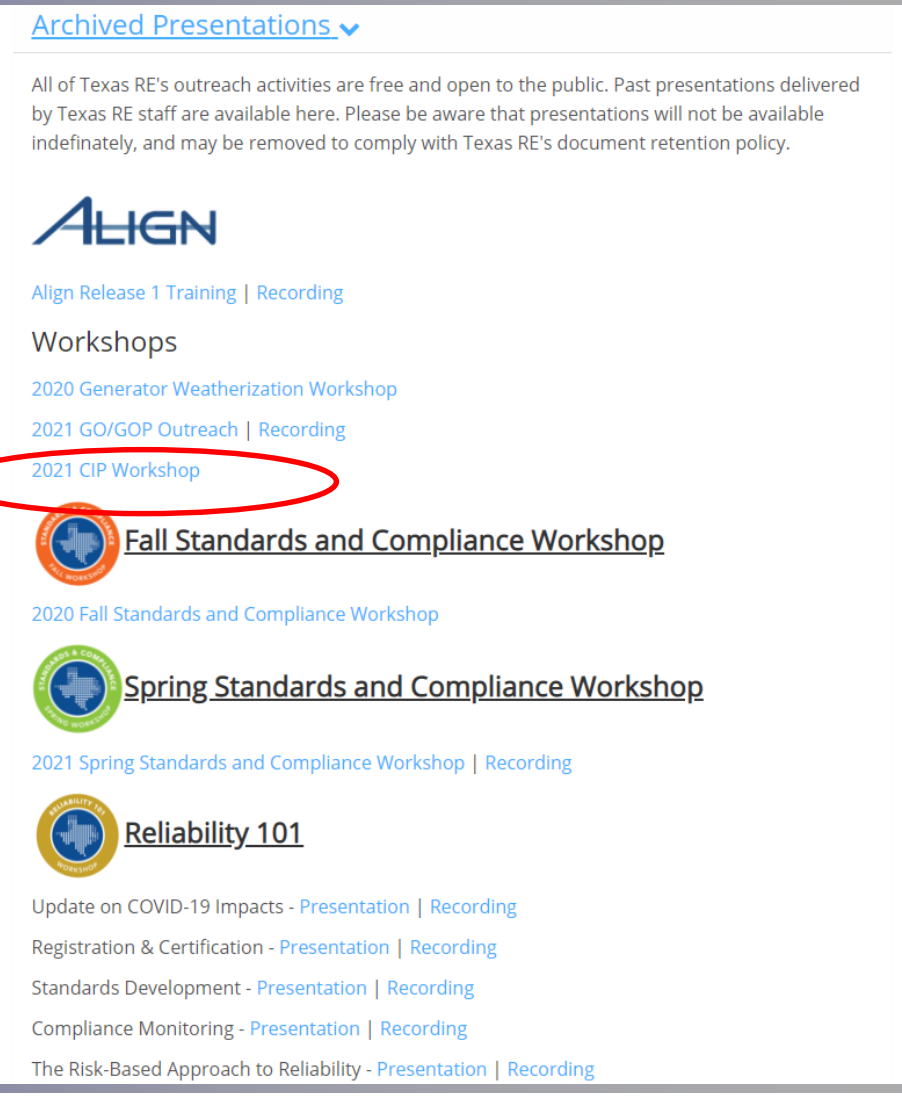
Lowest Presentation Rating Highest

Workshop Materials



Training Page





Social Media

/texas-reliability-entity-inc

@Texas_RE_Inc

/TexasReliabilityEntity

Sli.do (#TXCIP)

Slido Question

Where are you joining us from today?

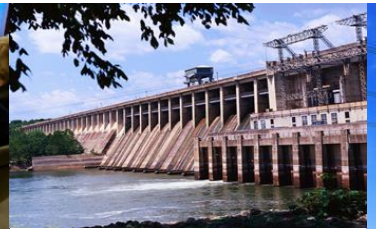
Supply Chain Risk Management

Zack Brinkman, RF

Manager, CIP Compliance Monitoring

John Graminski, WECC

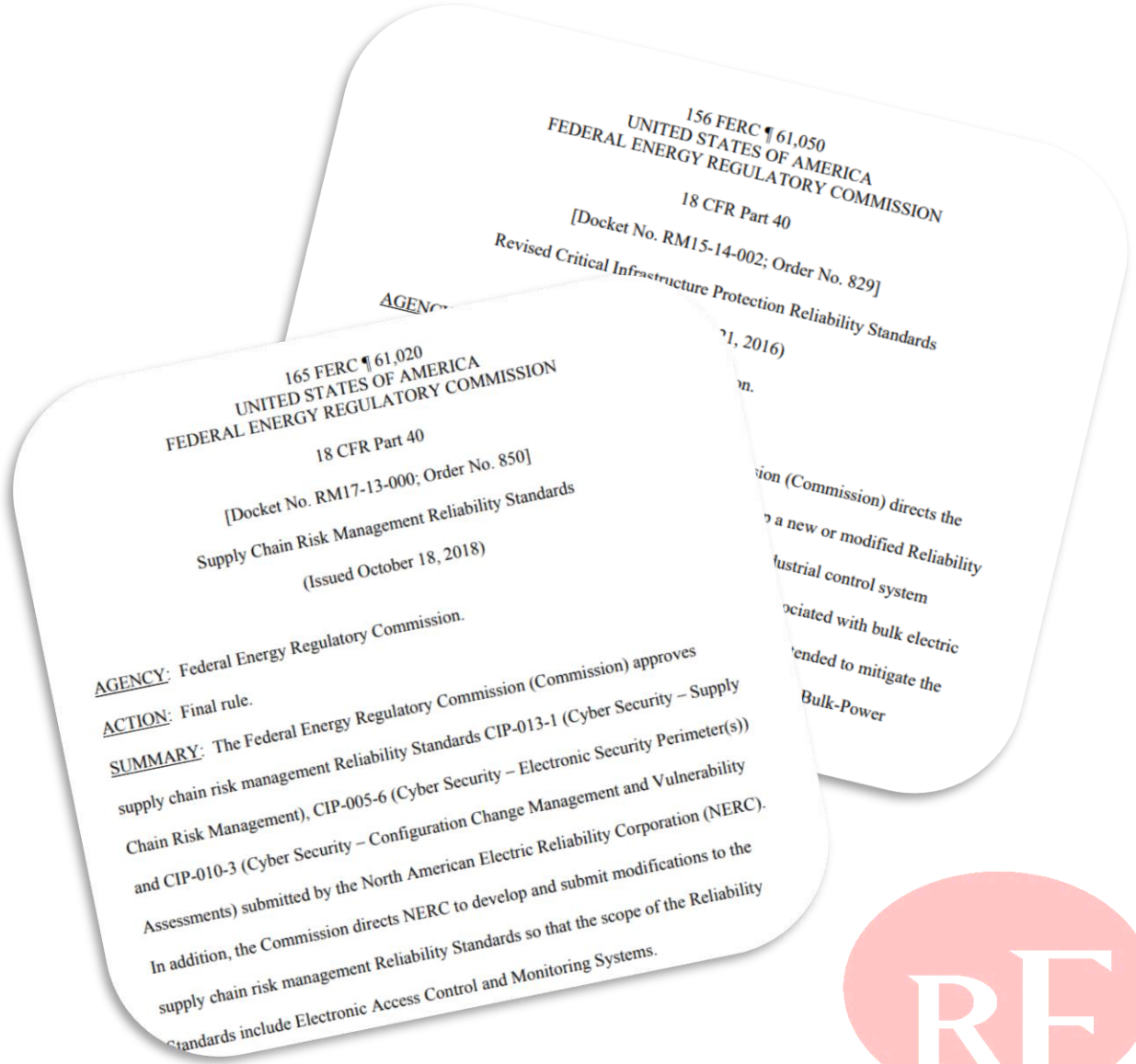
Sr. Compliance Auditor, Cyber Security



Background

- **Order #829**
- **Order #850**
- **Effective date October 1, 2020**



Learning Objectives

Purpose, expectations, challenges, and best practices of the CIP-013 standard:

- R1: Develop a supply chain risk management (SCRM) plan
- R2: Implement the SCRM plan
- R3: Review and approve the SCRM plan

John Graminski - Sr. Compliance Auditor, Cyber Security - WECC

- CIP-005-6
- CIP-010-3

Purpose of Supply Chain Standards

To **mitigate** cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems (BCS)

CIP-013 R1

Each Responsible Entity shall develop a documented supply chain cyber security risk management plan for high and medium impact BES Cyber Systems.

R1: Possible Challenges / Best Practices

Challenges

- Failure to:
  - Identify, assess and mitigate cyber security risk(s)

Best Practices

- Document processes to:
  - Identify and assess cyber security risks to include a risk assessment
  - Manage procurement controls
  - Identify the actual list of risks and add additional risks
- Apply the SCRM Plan to everything procured from a vendor

Document SCRM Plan

CIP-013 Part 1.1

One or more process(es) used in planning for the procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the Bulk Electric System from vendor products or services resulting from:
i. procuring and installing vendor equipment and software; and
ii. transitions from one vendor(s) to another vendor(s)

Risk Assessment

Determine your Risk Tolerance

Create or adopt a methodology to assess vendors/products/services

- Identify risks that could be posed by a vendor
- Develop a forum to collect information and integrate that into standing process
  - Verify the information provided back from the vendor
- Assess the risks that were identified
  - Determine what controls would be needed by a vendor to address those risks
- Risk Treatment
- Document every step of this process and results

Part 1.1: Possible Challenges/ Best Practices

Challenges

- Failing to have a process that plans for future acquisitions of products or services that are applicable to BES Cyber Systems and mitigate vendor transition risk

Best Practices

- Develop an alternative, if the vendor goes out of business

Future Acquisitions & Transitions

CIP-013 Part 1.2

One or more process(es) used in procuring BES Cyber Systems that address the applicable subparts in CIP-013 R1 P1.2

Part 1.2: Possible Challenges/ Best Practices

Challenges

- Failing to address all required process types in the SCRM Plan
- Vendor non-compliance

Best Practices

- Address all required process types
- Ensure vendors understand the cyber security expectations
- Document during procurement contract negotiations
- Develop your mitigation with an assumption of non-compliance

Part 1.2.1 & P1.2.2: Possible Challenges/ Best Practices

Challenges

- Vendor refuses to adhere to notification process
- Vendor declines to collaborate
- Undocumented or no controls to ensure collaboration

Best Practices

- Require vendor provides defined information
- Designated point of contact
- Technical controls to collaborate
- Upon an incident, require vendor to perform follow up

Vendor Identified Incidents

Part 1.2.3 Possible Challenges/ Best Practices

Challenges

- Vendor fails to provide notification
- Ensuring/confirming vendor compliance

Best Practices

- Develop criteria with vendor to revoke a vendor's staff access
- Develop a technical process to ensure notification
- Establish a revocation notification period
- Develop a process to ensure third-party contractors adhere to Entity's established process

Notification of Access Removal

Part 1.2.4: Possible Challenges/ Best Practices

Challenges

- Vendor fails to disclose ALL known vulnerabilities
- Unexploited vulnerabilities

Best Practices

- Require the vendor provides documentation of all vulnerabilities
- Establish a process to review vendor summary documentation of publicly disclosed vulnerabilities
- Identify and monitor vulnerabilities - National CVSS database, CVE, or other reporting mechanisms

Disclosure of Known Vulnerabilities

Part 1.2.5: Possible Challenges/ Best Practices

Challenges

- Failure to verify the integrity and authenticity of all software/patches

Best Practices

- During procurement, obtain vendor documentation that describes their:
  - Update process
  - Process to validate the integrity of the patch
  - Method to deliver the software
  - Methods to verify the integrity and authenticity of the software
- In an RFP or during contract negotiations, request documentation of Vendor requirements

Software Integrity and Authenticity

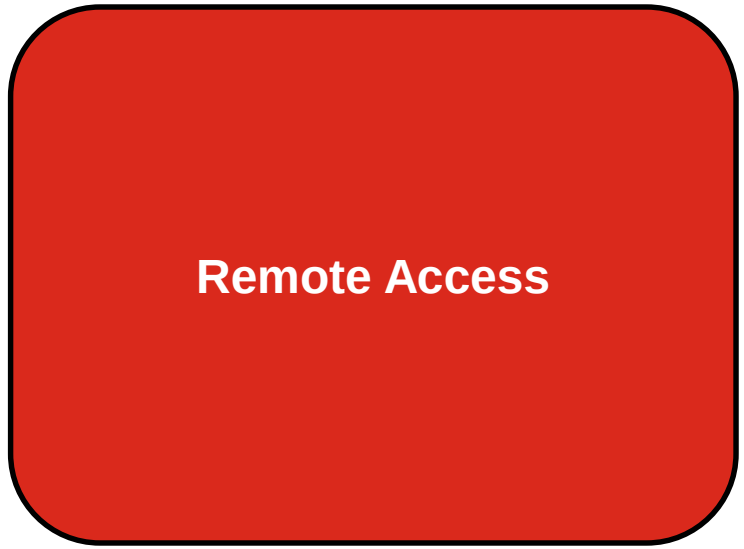
Part 1.2.6: Possible Challenges/Best Practices

Challenges

- Failing to identify and/or coordinate controls for vendor remote access

Best Practices

- Identify, control, and monitor all vendor remote access
- Coordinate controls with vendor
- Request specific vendor information
- Require the vendor to maintain data associated with their access



CIP-013 R1: What do Auditors Expect?

Detail Tab or Request ID	Standard	Require-ment	Initial Evidence Request Required in RSAW and NERC Evidence Request Spreadsheet
Procurement	CIP-013		Provide a listing of each procurement of vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s) during the audit period for high and/or medium impact BES Cyber Systems, during the audit period by using the Procurement tab of this spreadsheet.
CIP-013-R1-L1-01	CIP-013	R1	Provide each documented plan(s) that addresses the applicable requirement parts in CIP-013 R1.

CIP-013 R2

Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1

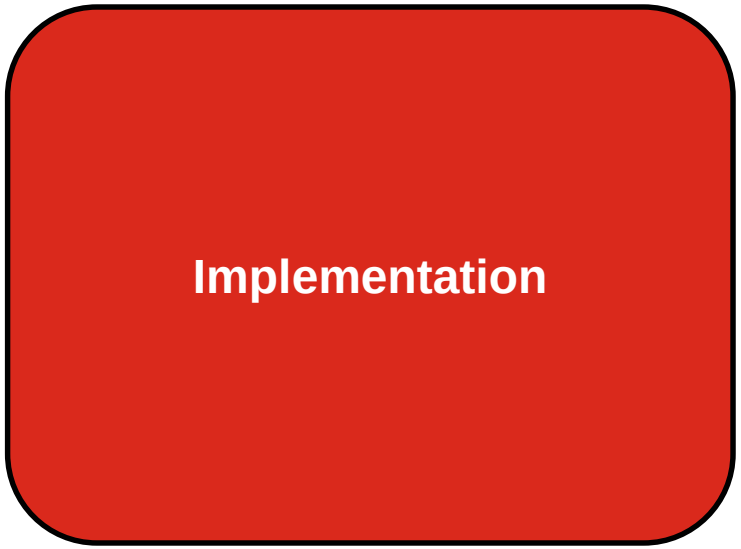
R2: Possible Challenges/Best Practices

Challenges

- Failing to implement the process(es) identified in the SCRM Plan

Best Practices

- Contract language and vendor performance reflect the requirements/parts
- Do not rely on contract language to demonstrate your implementation of the requirement/parts
- Document the step-by-step implementation of SCRM processes



CIP-013 R2: What do Auditors Expect?

Detail Tab or Request ID	Standard	Require-ment	Initial Evidence Request Required in RSAW and NERC Evidence Request Spreadsheet
CIP-013-R2-L1-01	CIP-013	R2	Provide a listing of persons, companies, or other organizations with whom the responsible entity, or its affiliates, contract with to supply BES Cyber Systems and related services.

Request ID	Standard	Require-ment	Sample Set	Sample Set Source & Description	Sample Set Evidence Request
CIP-013-R2-L2-01	CIP-013	R2	SS-013-R2-L2-01	Source Tab: Procurement Description: Sample of Unique IDs	For each Unique ID in Sample Set SS-013-R2-L2-01, provide evidence of the identification and assessment of cyber security risk(s) to the Bulk Electric System from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).
CIP-013-R2-L2-02	CIP-013	R2	SS-013-R2-L2-01	Source Tab: Procurement Description: Sample of Unique IDs	For each Unique ID in Sample Set SS-013-R2-L2-01, related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity, provide evidence of the implemented processes used in procuring that address the following, as applicable: 1. Notification by the vendor of vendor-identified incidents; 2. Coordination of responses to vendor-identified incidents; 3. Notification by vendors when remote or onsite access should no longer be granted to vendor representatives; 4. Disclosure by vendors of known vulnerabilities; 5. Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System; and 6. Coordination of controls for (i) vendor-initiated Interactive Remote Access, and (ii) system-to-system remote access with a vendor(s).

CIP-013 R3

Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months

R3: Possible Challenges/Best Practices

Challenges

- CIP Senior Manager or delegate fails to approve SCRM Plan
- CIP Senior Manager or delegate approves SCRM Plan without understanding the document

Best Practices

- Review the SCRM Plan on a shorter timeframe
- Establish processes to:
  - Review the SCRM Plan based on need
  - Update the SCRM Plan when a new risk is identified as a result of a procurement
- Document each plan review, revision, and approval

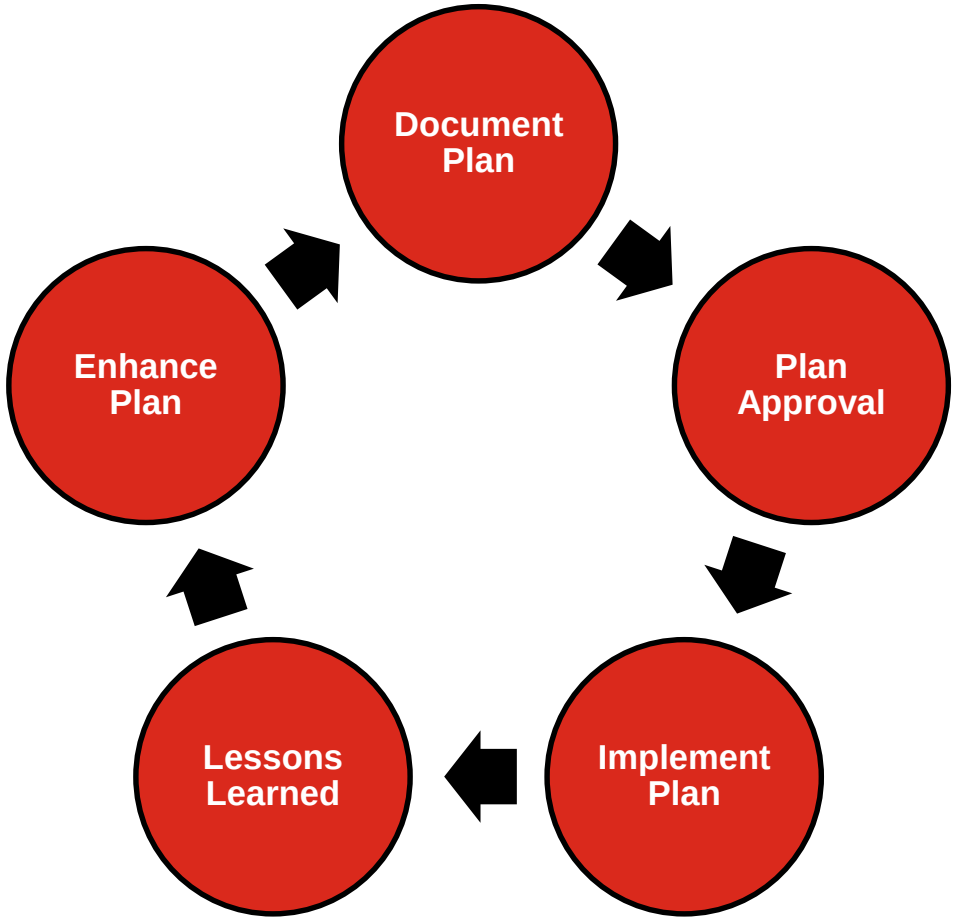
15 Month Approval

R3: What do Auditors Expect?

Detail Tab or Request ID	Standard	Require-ment	Initial Evidence Request Required in RSAW and NERC Evidence Request Spreadsheet
CIP-013-R3-L1-01	CIP-013	R3	Provide evidence that the documented plan(s) in CIP-013 R1 and its parts were reviewed and approved by the CIP Senior Manager or delegate(s) at least once every 15 calendar months during the audit period. Also provide evidence of the most recent review and approval performed prior to the audit period. Include the date of each review and the results, if any, of the review.

Recap CIP-013

- Document plan
- CIP Sr. Manger Approval
- Implement your plan
- *Lessons Learned
- *Enhance your plan
- Tell your Story



CIP-005-6 and CIP-010-3 Learning Objectives

Purpose, expectations, challenges, and best practices of the CIP-005 and CIP-010 Standard modifications for SCRM:

- CIP-005-6: Develop and implement methods for managing vendor remote access
- CIP-010-3: Develop and implement plans for managing software acquisitions

High Level CIP-005-6 R2, Parts 2.4-2.5

Part 2.4 – Determining active vendor remote access sessions

Part 2.5 – Disabling active vendor remote access sessions

CIP-005-6 R2, 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)

Part 2.4: Possible Challenges / Best Practices

Challenges

- Failure to:
  - Identify which remote users are vendors
  - Determine active vendor remote access sessions
  - Navigate multiple technologies (IRA, system-to-system, Web conferencing)

Best Practices

- Document processes to:
  - Identify vendors who are permitted remote access to applicable systems
  - Identify which specific remote access methods are available for each vendor
  - Determine when vendor remote access sessions are active
- Develop internal controls to ensure processes are followed

Part 2.4: What do Auditors Expect?

Primary evidence:

- Documented method(s) for determining active vendor remote access sessions
- Evidence may include (not limited to):
  - Methods for accessing logs or monitoring information in Intermediate Systems to determine active vendor remote access sessions
  - Methods for monitoring activity in a firewall, or user activity or open ports to determine active system to system remote access sessions
  - Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access

CIP-005-6 R2, Part 2.5

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

Part 2.5: Possible Challenges / Best Practices

Challenges

- Failure to:
  - Determine active vendor remote access sessions
  - Disable active vendor remote access sessions
  - Navigate multiple technologies (Interactive Remote Access (IRA), system-to-system, Web conferencing)

Best Practices

- Document processes to:
  - Identify when it is necessary to disable an active vendor remote access session
  - Identify clear roles and responsibilities for disabling remote access sessions
- Develop internal controls to ensure processes are followed

Part 2.5: What do Auditors Expect?

Primary evidence:

- Documented method(s) for disabling active vendor remote access sessions
- May include (not limited to):
  - Methods to disable vendor remote access at the applicable Electronic Access Point for system-to-system remote access sessions
  - Methods to disable vendor IRA at the applicable Intermediate System for IRA remote access sessions

Recap CIP-005-6 R2, Parts 2.4-2.5

- Identify vendors that require remote access to applicable systems
- Identify types of vendor remote access required
- Develop method(s) to determine active vendor remote access sessions
- Develop methods to disable active vendor remote access sessions
- Develop internal controls to ensure methods(s) are followed
- Implement your methods and monitor them

High Level CIP-010-3 R1, Part 1.6

Part 1.6.1: Verify the identity of software sources

Part 1.6.2: Verify the integrity of software obtained from the software sources

CIP-010-3 R1, Part 1.6

Prior to a change that deviates from the existing baseline configuration associated with baseline items in Parts 1.1.1 (operating systems/firmware), 1.1.2 (commercial/open-source software), and 1.1.5 (security patches), and when the method to do so is available to the Responsible Entity from the software source:

- 1.6.1. Verify the identity of the software source; and
- 1.6.2. Verify the integrity of the software obtained from the software source

Part 1.6: Possible Challenges / Best Practices

Challenges

- Failure to:
  - Identify which software is applicable
  - Verify the identity of the software source
  - Verify the integrity of the software obtained from the software source

Best Practices

- Document processes to:
  - Identify applicable software and baseline changes
  - Identify methods for verifying the identity of the software source
  - Identify methods for verifying the integrity of the software
- Develop internal controls to ensure processes are followed

Part 1.6: What do Auditors Expect?

Primary evidence:

- Documented methods for verifying the identity of the software sources
- Documented methods for verifying the integrity of applicable software
- Evidence of implementation, which may include (not limited to):
  - A change request record that demonstrates the verification of identity of the software source and integrity of the software was performed prior to the baseline change
  - A process which documents the mechanisms in place that would automatically ensure the identity of the software source and integrity of the software

Recap CIP-010-3 R1, Part 1.6

- Verify the identity of software sources
- Verify the integrity of software obtained from the software sources
- Develop internal controls to ensure methods(s) are followed
- Implement your methods and monitor them

Critical Infrastructure Protection WORKSHOP

June 3, 2021

Agenda

Intro and Instructions

Supply Chain Compliance Presentation

Supply Chain Security Panel

CIP-012 Compliance Presentation

CIP-012 Security Panel

CIP-008-6 Compliance Presentation

CIP-008-6 Security Panel

E-ISAC Update Presentation

Wrap-Up

TEXAS RE
Ensuring electric reliability for Texans

CIP-012

Jess Syring, Midwest Reliability Organization
CIP Compliance Monitoring Manager

Krinken Rohleder, Texas RE
CIP Cyber and Physical Security Analyst

What are we going to discuss?

- History & Purpose
- A Summary Of The Standard
- Expectations & Obligations
- Implementation Guidance
- Request for Information
- Risk Based Questions
- Best Practices
- Resources

Why CIP-012?

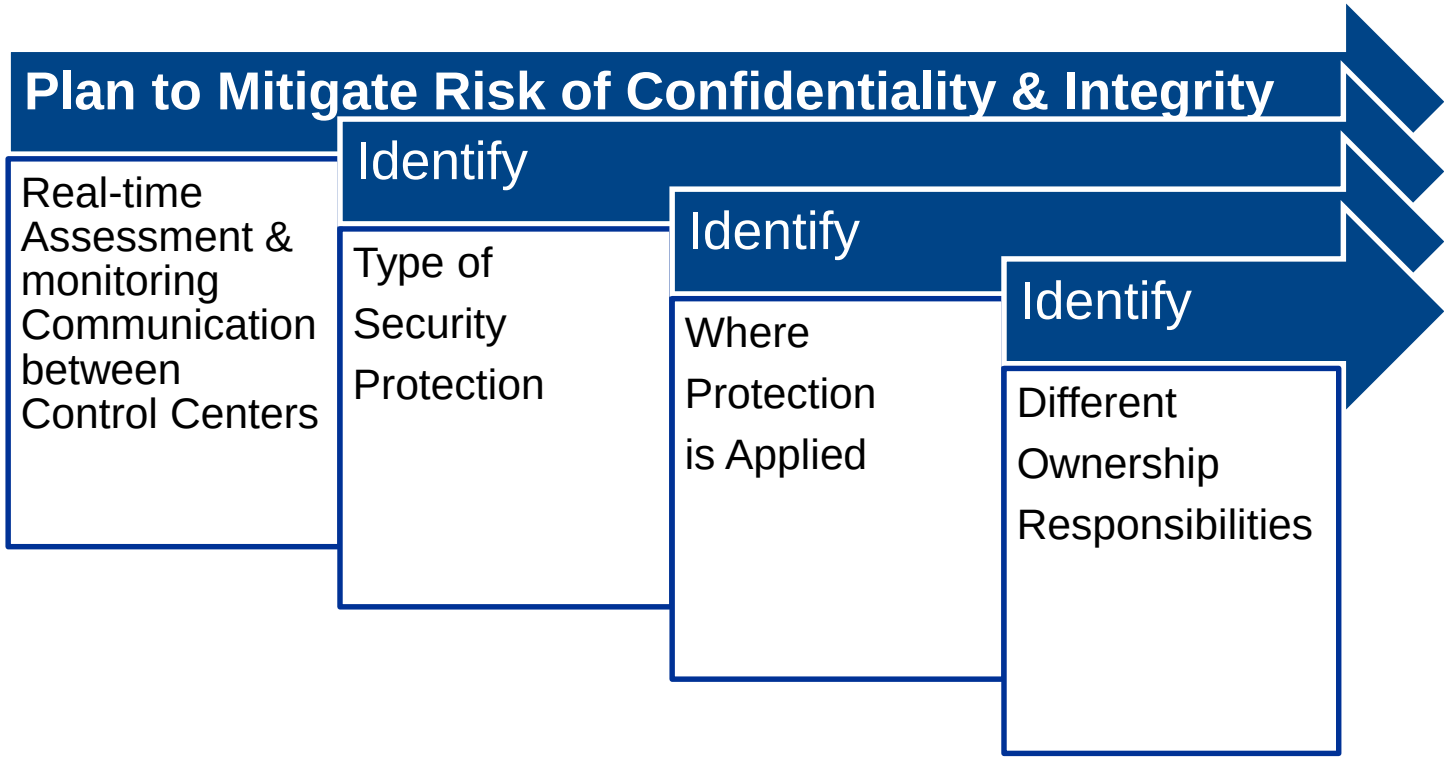
- On January 21, 2016, FERC ordered a new standard to protect communication of sensitive bulk electric system data between Control Centers.
- This new standard is CIP-012.
- CIP-012 seeks to mitigate the risk of confidentiality, integrity, and availability threats against Real-time Assessment and Real-time monitoring data being transmitted between Control Centers.

Slido Question

Select all of the following that are considered to be key aspects of CIP-012:

- Identify Type of Security Protection
- Identify Who Your Manager Is
- Identify Where the Protection is Applied
- Identify Different Ownership Responsibilities

A Summary of CIP-012 R1



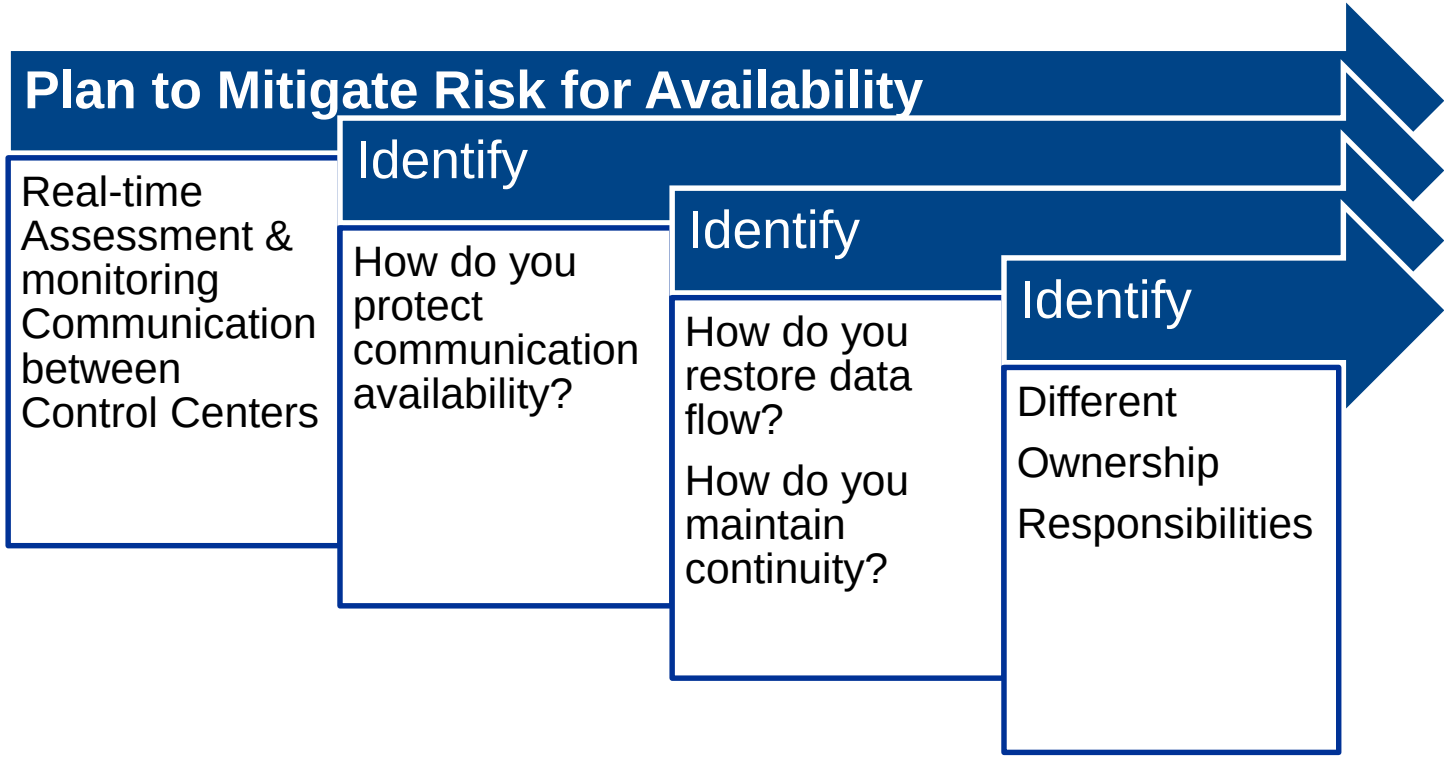
- **R1.** The Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) to mitigate the risks posed by unauthorized disclosure and unauthorized modification of Real-time Assessment and Real-time monitoring data while being transmitted between any applicable Control Centers. The Responsible Entity is not required to include oral communications in its plan. The plan shall include:
  - **1.1.** Identification of security protection used to mitigate the risks posed by unauthorized disclosure and unauthorized modification of Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers;
  - **1.2.** Identification of where the Responsible Entity applied security protection for transmitting Real-time Assessment and Real-time monitoring data between Control Centers; and
  - **1.3.** If the Control Centers are owned or operated by different Responsible Entities, identification of the responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring data between those Control Centers.

Future of CIP-012

There is a newer version of CIP-012 that is currently out for ballot

- **Part of Project 2020-04**
  - Adds an additional R2
    - Adds consideration needed for availability of the applicable data and communication lines
    - Does not include oral communications

A Summary of CIP-012 R2



- **R2.** The Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) to provide for the availability of communications links and data used for Real-time Assessment and Real-time monitoring while being transmitted between Control Centers. The Responsible Entity is not required to include oral communications in its plan. The plan shall include:
  - **2.1.** Identification of how the Responsible Entity has provided for the availability of communications links and data used for Real-time Assessment and Real-time monitoring while being transmitted between Control Centers;
  - **2.2.** Identification of how the Responsible Entity has addressed communications and data flow restoration to maintain continuity of operations in the Responsible Entity's plan; and
  - **2.3.** If the Control Centers are owned or operated by different Responsible Entities, identification of the responsibilities of each Responsible Entity for providing availability of communications links and data used for Real-time Assessment and Real-time monitoring while being transmitted between Control Centers.

What are the Compliance Obligations & Expectations?

Registered Entities

- **Understand the communications that are applicable**
- **Document your plan**
- **Provide evidence showing implementation**
  - Logical protection or,
  - Physical protection or,
  - Both
- **Consider additional protections even if they consider themselves not applicable for the protections**
- **Must address unauthorized disclosure, modification, and availability risks**

Sli.do (#TXCIP)

Slido Question

Name some examples of physical or logical implementation.

Entities

- **Physical Implementation Examples**
  - Applicable Control Center floor plan with security measures
  - Physical security measures to protect communication link
- **Logical Implementation Examples**
  - Device configuration which applies protection
  - Security control monitoring
  - Encryption

Slido Question

What additional protections is your organization considering (going beyond CIP-005 ESP and CIP-006 PSP protections)?

What will the ERO Enterprise be asking for?

- **Level 1**
  - **CIP-012-R1-L1-01** - Provide each documented plan(s) that addresses the applicable requirement parts in CIP-012 R1.
  - **CIP-012-R1-L1-02** - Provide evidence of the documented specification for data necessary to perform Real-time Assessments and Real-time monitoring, per IRO-010 and/or TOP-003.

Sli.do (#TXCIP)

Slido Question

What real-time communications (applicable to CIP-012) does your organization use?

Regions Request for Information

What communications will the ERO Enterprise want to be considered?

- ICCP
- PMU
- OPC
- VRTU
- Any protocol consideration

Note: Only communications applicable is information exchanged between Control Centers and not between a Control Center and a corresponding generation or transmission station

What communications are exempt?

- **Technical Rationale indicates the following are exempt**
  - Operational Planning Analysis data
  - Weather data
  - Market data
  - Additional data that is not used by the RC, BA, and TOP to perform real-time reliability assessments and analysis identified in TOP-003 and IRO-010

What will the ERO Enterprise be asking for?

- **Level 2**
  - **CIP-012-R1-L2-01** - For each BES Asset in Sample Set SS-012-R1-L2-01, for Real-time Assessment and Real-time monitoring data being transmitted between Control Centers, provide the following evidence:
    - 1. Identification of security protection used to mitigate the risks posed by unauthorized disclosure and unauthorized modification;
    - 2. Identification of where the Responsible Entity applied security protection for transmitting; and
    - 3. If the Control Centers are owned or operated by different Responsible Entities, identification of the responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring data between those Control Centers.

Sampling Methodology

- **Since Level 2 is limited to Control Centers this may be a limited population**
  - Based on the Sampling Methodology guidelines on NERC's website this most likely means it will be a full population sample size (less than nine to select from)

What Regions are Considering as Risk

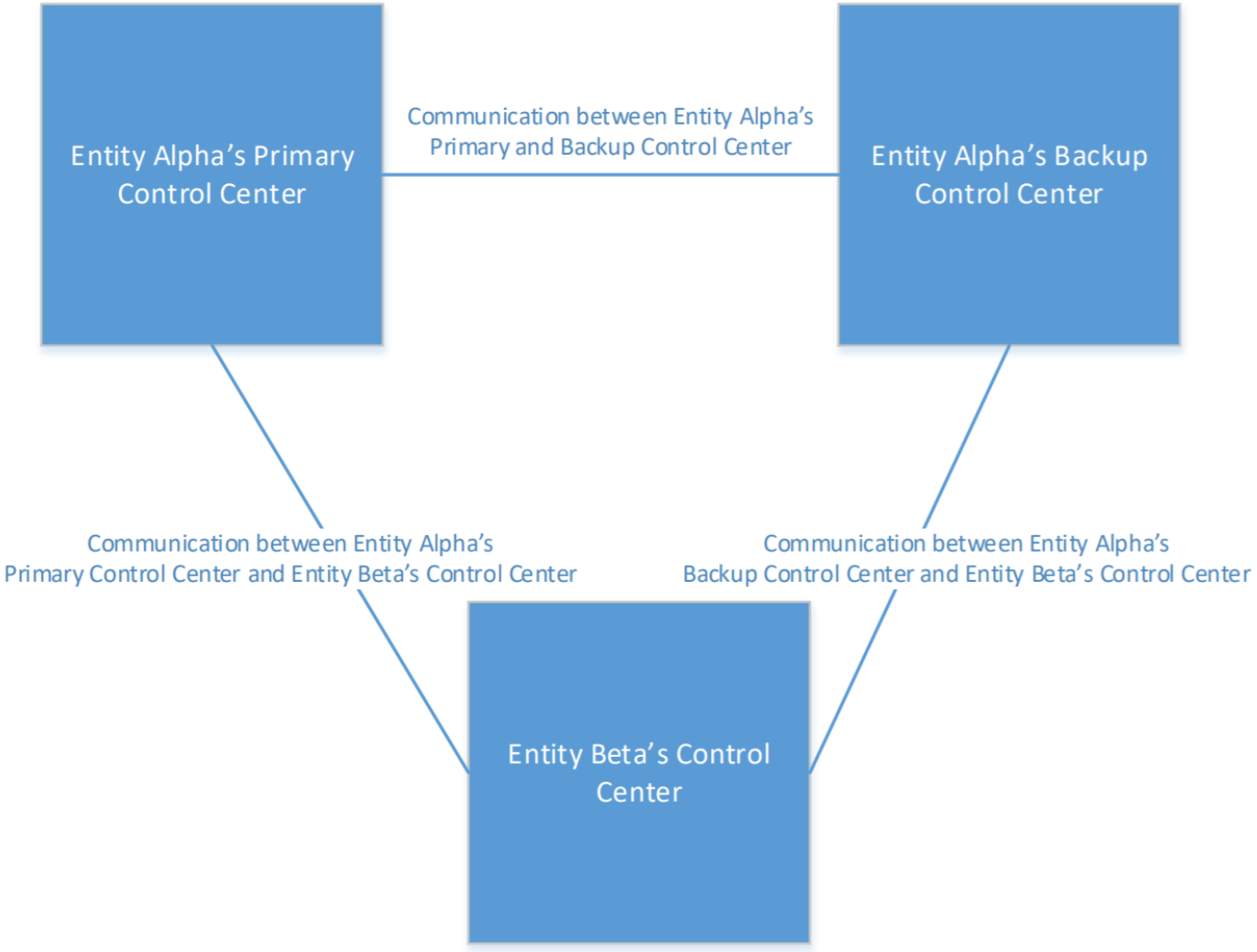
Regions may question risks

- How is the entity protecting from equipment owned by others?
- If only using physical controls, what about logical risks?
- If only using logical controls, what about physical risks?

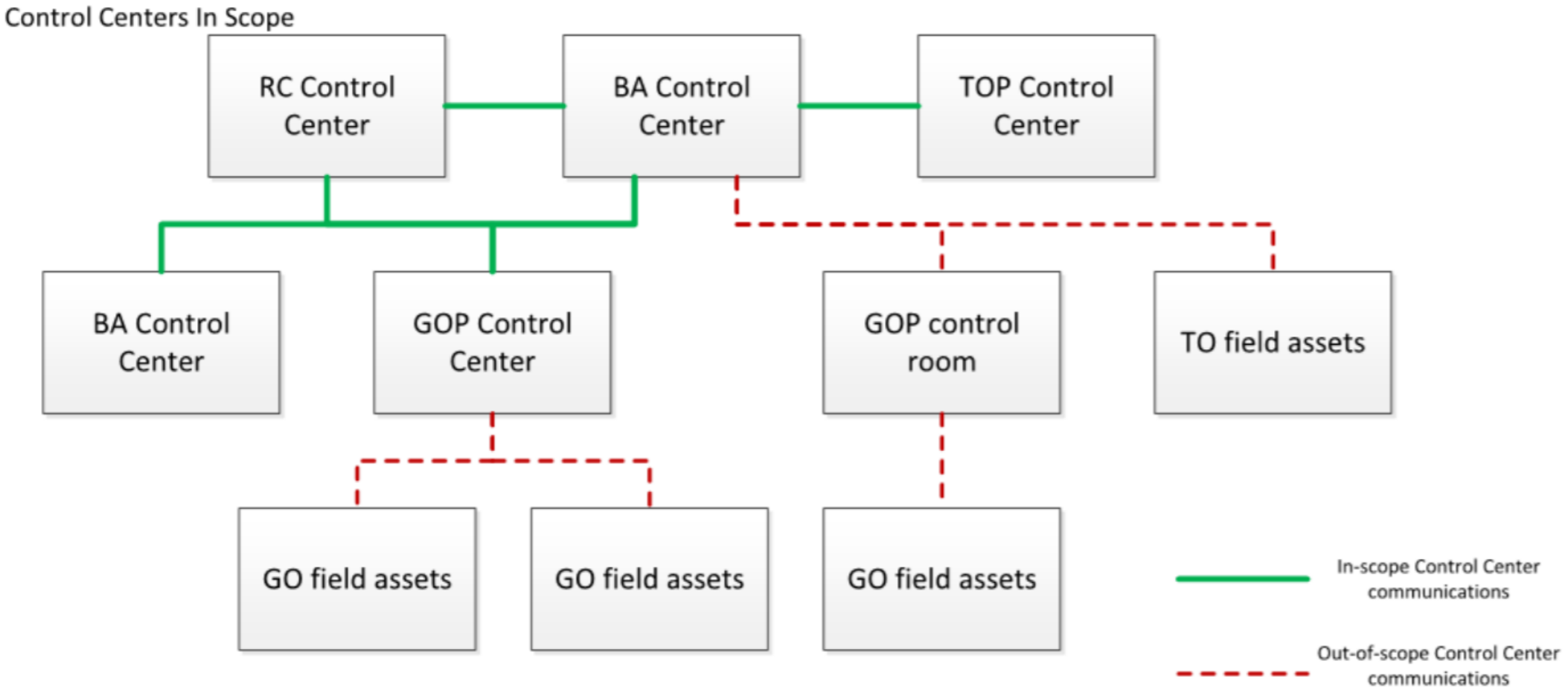
What are some best practices to assist with telling the story?

- **Here are the measures from the standard:**
  - Evidence may include, but is not limited to, documented plan(s) that meet the security objective of Requirement R1 and documentation demonstrating the implementation of the plan(s).

Best Practices



Best Practices



Best Practices

What are some best practices to assist with telling the story?

- Documenting how information shared with others was determined to be applicable to the requirement or not
  - Internal Controls associated with these determinations
- Documenting the controls associated with anything determined to be applicable
  - System generated evidence is always preferred
- Documenting additional controls for devices beyond the identified protections
  - Network switches or additional controls with the corresponding servers

References from the NERC Implementation Guidance Document

- MITRE Common Weakness Enumeration (CWE™) list of software weakness types
  https://cwe.mitre.org/data/definitions/327.html
- Cryptographic Standards and Guidelines
  https://csrc.nist.gov/Projects/Cryptographic-Standards-and-Guidelines
- NIST Special Publication 800-175B - Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms
  http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-175B.pdf
- OWASP Guide to Cryptography
  https://www.owasp.org/index.php/Guide_to_Cryptography#Symmetric_Cryptography

Sli.do (#TXCIP)

Slido Question

What additional information/outreach would be beneficial in helping with CIP-012 compliance?

Critical Infrastructure Protection WORKSHOP

June 3, 2021

Agenda

Intro and Instructions

Supply Chain Compliance Presentation

Supply Chain Security Panel

CIP-012 Compliance Presentation

CIP-012 Security Panel

CIP-008-6 Compliance Presentation

CIP-008-6 Security Panel

E-ISAC Update Presentation

Wrap-Up

TEXAS RE
Ensuring electric reliability for Texans

NPCC, Inc.

CIP-008-6
Cyber Security Incident Reporting and Response Planning

Devin Kitchens, Texas RE
CIP Cyber and Physical Security Analyst

Michael Bilheimer, NPCC
Senior CIP Analyst

Agenda

R1 – R4

- CIP Evidence Request Tool (CERT)
- Important Changes
- Tips, Resources, and Common Issues
- Common Violations

Exercise Improvement Ideas

R1, Part 1.1 Language

R1. Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable requirement parts in *CIP-008-6 Table R1 – Cyber Security Incident Response Plan Specifications.*

Part 1.1 One or more processes to identify, classify, and respond to Cyber Security Incidents.

CIP Evidence Request Tool (CERT)

- Provide each documented plan(s) that addresses the applicable requirement parts in CIP-008 R1
- If reporting of a Cyber Security Incident is prohibited by law, provide evidence of this prohibition

Changes to Applicable Systems

High & Medium

BES Cyber Systems

Associated: EACMS

R1, Part 1.2 Abridged Language

1.2.1 Criteria	• Evaluate and define attempts to compromise
1.2.2 Determine	• Reportable Cyber Security Incident; or • An attempt to compromise per 1.2.1 criteria
1.2.3 Notification	• Notify per Requirement R4

Slido Question

What is an attempt to compromise?

Possible Attempts to Compromise?

Unauthorized

- Vulnerability Scanning
- Port Scanning
- Ping Sweep
- Privilege Escalation
- Electronic or Physical Access
- Login Activity
- Remote Access
- Tunneling
- Baseline Changes
- Usage

Detected

- Malware
- Malicious Communications
- Abnormal Network Traffic

Tips & Resources

Tips

- Use objective criteria with specific thresholds when defining what constitutes an attempt to compromise

Resources

- SANS – Incident Handling Guide
- NIST – Computer Security Incident Handling Guide
- NCCIC – Cyber Incident Scoring System
- NERC – Glossary of Terms

R1, Part 1.3 Language

R1. Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable requirement parts in *CIP-008-6 Table R1 – Cyber Security Incident Response Plan Specifications.*

Part 1.3 The roles and responsibilities of Cyber Security Incident response groups or individuals.

CIP-008-6 Violations in the NPCC Region (R1)

R1, Part 1.3	• Not defining roles and responsibilities of Cyber Security Incident response groups or individuals in its Cyber Security Incident response plan. Individuals were named on a generic Incident Response List.
Mitigation:	• Update Roles and responsibilities to include greater clarity on specific roles in the Incident Response Plan.

Other CIP-008-6 Enforcement Actions

- **Not Performing a detailed enough Cyber Security Drill**
  - Include specific incident response steps.
  - Include all groups/Departments:
    - IT
    - SCADA
    - Substation Protection
    - Physical Security
    - Operations
    - Compliance
    - Communications

Silos should be broken down in Incident Response

R2, Part 2.1 Language

R2. Each Responsible Entity shall implement each of its documented Cyber Security Incident response plans to collectively include each of the applicable requirement parts in *CIP-008-6 Table R2 – Cyber Security Incident Response Plan Implementation and Testing*.

Part 2.1. Test each Cyber Security Incident response plan(s) at least once every 15 calendar months:

- By responding to an actual Reportable Cyber Security Incident;
- With a paper drill or tabletop exercise of a Reportable Cyber Security Incident; or
- With an operational exercise of a Reportable Cyber Security Incident.

CIP Evidence Request Tool (CERT)

- For each Cyber Security Incident response plan provided in the response to CIP-008-R1-L1-01, provide evidence of each test performed during the audit period

Slido Question

What type(s) of injects are you using?

Tips

- Ensure test scenarios stress the plan
- Document lessons learned
- Use preventative controls

Common Issue

- The 15 calendar month testing periodicity is exceeded

CIP-008-6 Violations in the NPCC Region (R2)

R2, Part 2.1

- Not testing Cyber Security Incident response plan(s) to an **actual** Reportable Cyber Security Incident.

Mitigation:

- Perform another drill that is a Reportable Cyber Security Incident to bring entity into compliance.

3.1 No Later than 90 days after completion (test or actual Reportable Cyber Security Incident)

- Document lessons learned
- Update plan(s)
- Notify each person or group with a defined role

CIP-008-6 Violations in the NPCC Region (R3)

R3, Part 3.1

- Failure to document any lessons learned, update the response plan with any lessons learned, or notify each person or group with a defined role in the response plan within 90 days.

Mitigation:

- Create reoccurring reminders to document lessons learned, update response plan, and notify person or group with a defined role in the response plan within 90 days.

4.1 Initial Notifications

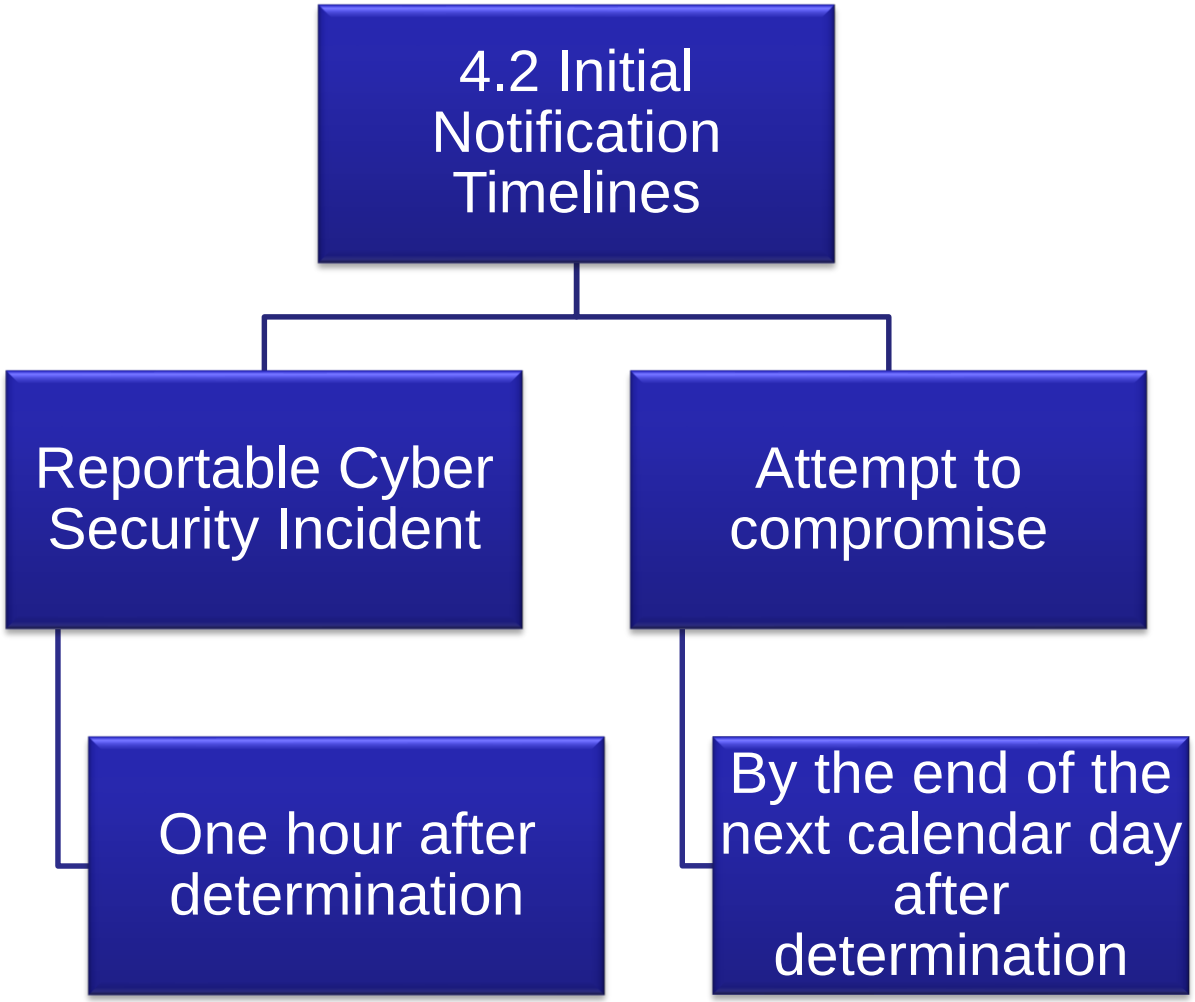
Functional impact	Attack vector used	Level of intrusion (achieved or attempted)

R4 Tips

Part 4.1

- Create a notification template that includes the functional impact, attack vector, level of intrusion, and date/time of notification
- Save notices to E-ISAC and DHS CISA

R4, Part 4.2 Abridged Language



R4 Tips

Part 4.1

- Create a notification template that includes the functional impact, attack vector, level of intrusion, and date/time of notification
- Save notices to E-ISAC and DHS CISA

Part 4.2

- Create a process workflow

R4, Part 4.3 Abridged Language

4.3 Provide updates, if any, within 7 calendar days of determination of new or changed attribute information

Updates to E-ISAC and DHS CISA

R4 Tips

Part 4.1

- Create a notification template that includes the functional impact, attack vector, level of intrusion, and date/time of notification
- Save notices to E-ISAC and DHS CISA

Part 4.2

- Create a process workflow

Part 4.3

- Create notification reminders
- Add checklist items for follow-up actions

The Tabletop Exercise

- **Don’t just focus on IT. Create a multi-department response scenario.**
  - Engage various departments or groups
- **Add various components:**
  - Add Physical components to drills
  - Add internal threats (Disgruntled personnel)
  - Nation State, Supply Chain, Ransomware
  - Drone Attack(s)
  - Third parties getting attacked (SCADA Vendor, Communication Company)
- **Add distraction events**
  - Copper theft in the middle of a cyber event (is part of the attack or not?)

Incident Response Scenarios

- **Relays Firmware update compromise (Stuxnet type attack)**
  - Random breakers opening
- **IT (Select Equipment) Installation Attack (Supply Chain Compromise)**
- **Cyber Attack during a Pandemic**
  - If you need staff on site to mitigate the threat
  - Communication ability
- **Active Shooter (possible Insider Threat)**
  - Incapacitated personnel
- **Unknown device installed at Medium Substation**
- **Vendor Ransomware Infection**
- **Drone Attack on Medium substation or Control Center**

Document, Document, Document

- **Remember to:**
  - Use your plan
  - Push the scenario/injects
    - It’s ok to push into the realm of crazy to stress the plan
  - Involve various departments, groups, individuals
  - Document and implement Lessons Learned
- **Don’t do the incident response drill for compliance, do it for reliability**

Incident Response Resources:

- **GridEX**
  - GridEx Public Reports and Fact Sheet
  - GridEx VI Registration
- **CISA Incident Response**
  - Training and National Incident Response Pan
  - CRR Supplemental Resource Guide
- **NIST:**
  - Computer Security Incident Handling Guide
- **DHS CISA Reporting:**
  - https://us-cert.cisa.gov/forms/report

Critical Infrastructure Protection WORKSHOP

June 3, 2021

Agenda

Intro and Instructions

Supply Chain Compliance Presentation

Supply Chain Security Panel

CIP-012 Compliance Presentation

CIP-012 Security Panel

CIP-008-6 Compliance Presentation

CIP-008-6 Security Panel

E-ISAC Update Presentation

Wrap-Up

A DIVISION OF NERC

E-ISAC

ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER

E-ISAC Update

Threat Landscape, CIP-008-6 Reporting, and GridEx VI

Matthew Duncan, Director, Intelligence

ERO Critical Infrastructure Protection Workshop

June 3, 2021

TLP:WHITE

RELIABILITY | RESILIENCE | SECURITY

Threat Landscape — Supply Chain Compromise

- U.S. Government (USG) officially attributes to Russian Federation
- New malware variants detected and tools released
- No impact to reliability of bulk power system
- E-ISAC/Electricity Subsector Coordinating Council Tiger Teams continue to monitor situation
- Guidance
  - Keep operating systems and enterprise software patches up to date and maintain awareness of latest threats
  - Disable sharing services, or if services are required, use complex passwords or Active Directory authentication
  - Restrict permission to install and run unwanted software applications to administrators
  - Configure firewalls to deny unsolicited connection requests

Threat Landscape — Microsoft Exchange Vulnerability

- Initial disclosure focused on HAFNIUM exploitation of four Zero-Day vulnerabilities for on-premise exchange environments
- USG-required patches to be applied ASAP (CISA ED 21-02)
  - E-ISAC issued All-Purpose Bulletin, and NERC issued a Level 1 Alert
- Microsoft disclosed four additional vulnerabilities for Exchange
  - Two of the vulnerabilities focused on pre-authentication, no login required
  - No known active exploitation at time of disclosure

Threat Landscape — Pulse Secure Vulnerabilities

- Exploitation of vulnerabilities in Pulse Connect Secure (PCS) products (widely used remote access tool)
- USG-required patches to be applied ASAP (CISA ED 21-03)
- Vulnerabilities allow placement of webshells to gain persistent system access
- Patch issued; recommendation to run the Pulse Connect Secure Integrity Tool to detect compromise

Reporting Mechanisms for CIP-008-6

- What to report to E-ISAC and the Department of Homeland Security Cybersecurity Infrastructure and Security Agency (DHS CISA)* (successor of the National Cybersecurity and Communications Integration Center (NCCIC))?
  - A Reportable Cyber Security Incident
  - An attempt to compromise one or more "Applicable Systems" (High and Medium Impact Bulk Electric System (BES) Cyber Systems and their associated Electronic Access Control Monitoring Systems (EACMS))
- Required in the submission (Table R4):
  - 4.1.1 The functional impact
  - 4.1.2 The attack vector used
  - 4.1.3 The level of intrusion that was achieved or attempted
- Please label your submission a "CIP-008 Report" for tracking purposes

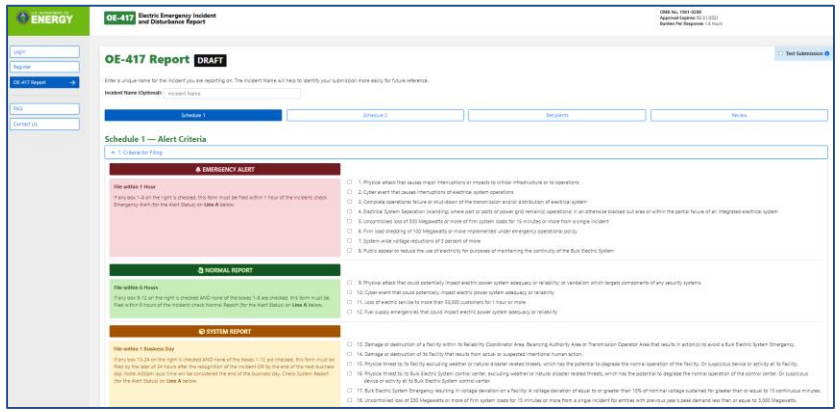
**** The requirement to report to DHS CISA only applies to U.S.-registered entities***

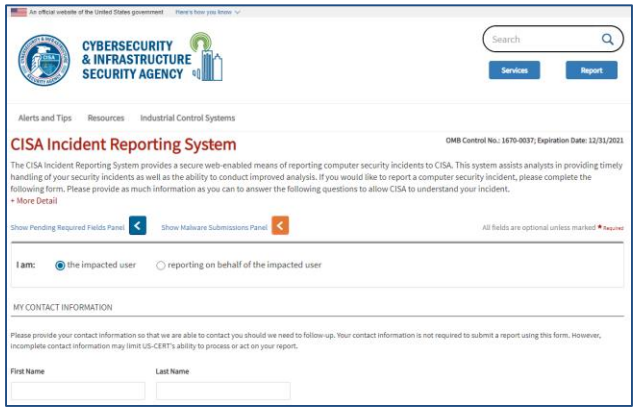
CIP-008-6 Report Requirements

CIP-008-6 Table R4 – Notifications and Reporting for Cyber Security Incidents			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	Initial notifications and updates shall include the following attributes, at a minimum, to the extent known: 4.1.1 The functional impact; 4.1.2 The attack vector used; and 4.1.3 The level of intrusion that was achieved or attempted.	Examples of evidence may include, but are not limited to, dated documentation of initial notifications and updates to the E-ISAC and NCCIC.
4.2	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	After the Responsible Entity's determination made pursuant to documented process(es) in Requirement R1, Part 1.2, provide initial notification within the following timelines: • One hour after the determination of a Reportable Cyber Security Incident. • By the end of the next calendar day after determination that a Cyber Security Incident was an attempt to compromise a system identified in the "Applicable Systems" column for this Part.	Examples of evidence may include, but are not limited to, dated documentation of notices to the E-ISAC and NCCIC.

Reporting Mechanisms for CIP-008-6

- To report a CIP-008 Incident to the E-ISAC you can:
  - Email operations@eisac.com
  - Call the 24/7 E-ISAC Watch at 202-790-6000
  - Post a bulletin to the E-ISAC Portal (www.eisac.com)
  - Submit a copy of a NERC EOP-004 Reliability Standards (nerc.com)
  - Submit a copy of a DOE-417 OE-417 Form (doe.gov)
  - Submit a copy a DHS CISA Reporting Form Incident Reporting System | CISA
- If possible, please label your submission as “CIP-008 Report”





CIP-008-6 Report Requirements

CIP-008-6 Table R4 – Notifications and Reporting for Cyber Security Incidents			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	Initial notifications and updates shall include the following attributes, at a minimum, to the extent known: 4.1.1 The functional impact; 4.1.2 The attack vector used; and 4.1.3 The level of intrusion that was achieved or attempted.	Examples of evidence may include, but are not limited to, dated documentation of initial notifications and updates to the E-ISAC and NCCIC.
4.2	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	After the Responsible Entity's determination made pursuant to documented process(es) in Requirement R1, Part 1.2, provide initial notification within the following timelines: • One hour after the determination of a Reportable Cyber Security Incident. • By the end of the next calendar day after determination that a Cyber Security Incident was an attempt to compromise a system identified in the "Applicable Systems" column for this Part.	Examples of evidence may include, but are not limited to, dated documentation of notices to the E-ISAC and NCCIC.

Sample CIP-008 Submission #1

From: [redacted]
Sent: Monday, May 10, 2021 5:02 PM
To: operations@eisac.com
Subject: Acme Utility Company NCRXXXXX SAMPLE US-CERT Report

US-CERT-Report.pdf
3 MB

As part of the NERC CIP-008- R4.2, we are informing of an attempt to compromise.

As part of patching the Pulse Secure VPN per AA21-110A, five system files were found to be mismatched at approximately 4:50 pm ET on May 10, 2021.
While mitigation is in process, we wanted to provide a notice in accordance with CIP-008-6 R4.2.
There were no known impacts to any systems at this time.

Please contact me for further questions.

- 4.1.1 **Functional Impact** — "no known impacts to any systems"
- 4.1.2 **Attack Vector** — "patching Pulse Secure VPN per AA21-110A"
- 4.1.3 **Level of Intrusion** — **"**five system files were found to be mismatched"

Sample CIP-008 Submission #2

From: [redacted]
Sent: Friday, May 11, 2021 10:11 AM
To: operations@eisac.com
Subject: Acme Utility NCRXXXXX CIP-008 Report

E-ISAC,
We are informing you of an attempt to compromise of our EACMS in a Medium Control Center as part of the NERC CIP-008- R4.2. We also filled out the CISA incident report.

Functional Impact – none noted. Confirmed through analysis of OT Network logs and/or performance.
Attack Vector – Malicious software introduced via a trusted patch source. Investigation is ongoing.
Level of intrusion – At this time, we have identified it as a compromise and have found no indicators of compromise on the DMZ, location of the EACMS that the attempt was detected, or the OT network.

Please contact our SOC for further questions and follow-up.

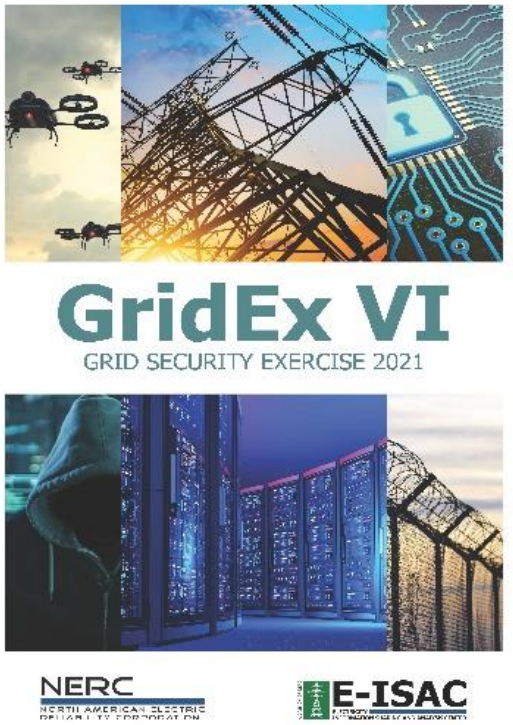
- 4.1.1 **Functional Impact** — "none noted. Confirmed through analysis of OT Network logs and/or performance."
- 4.1.2 **Attack Vector** — "Malicious software introduced via a trusted patch source. Investigation is ongoing."
- 4.1.3 **Level of Intrusion** — "no indicators of compromise on DMZ, location of the EACMS that the attempt was detected, or OT net."

Questions about CIP-008-6 Standards Applicability

For guidance and for specific questions about the revised CIP-008-6 Reliability Standard applicability, please contact NERC's Compliance Assurance or your respective Regional Entity Compliance or Enforcement Staff

GridEx VI

- Objectives
  - Activate incident, operating, and crisis management response plans
  - Enhance coordination with government to facilitate restoration
  - Identify interdependence concerns with natural gas and telecommunications sectors
  - Exercise response to a supply chain-based compromise to critical components
  - Identify common mode and cyber operation concerns across interconnections
- Distributed Play — November 16–17, 2021
- Email GridEx@eisac.com with questions
- Register by August 31 at https://register4gridex.eisac.com



Critical Infrastructure Protection WORKSHOP

June 3, 2021

Agenda

Intro and Instructions

Supply Chain Compliance Presentation

Supply Chain Security Panel

CIP-012 Compliance Presentation

CIP-012 Security Panel

CIP-008-6 Compliance Presentation

CIP-008-6 Security Panel

E-ISAC Update Presentation

Wrap-Up