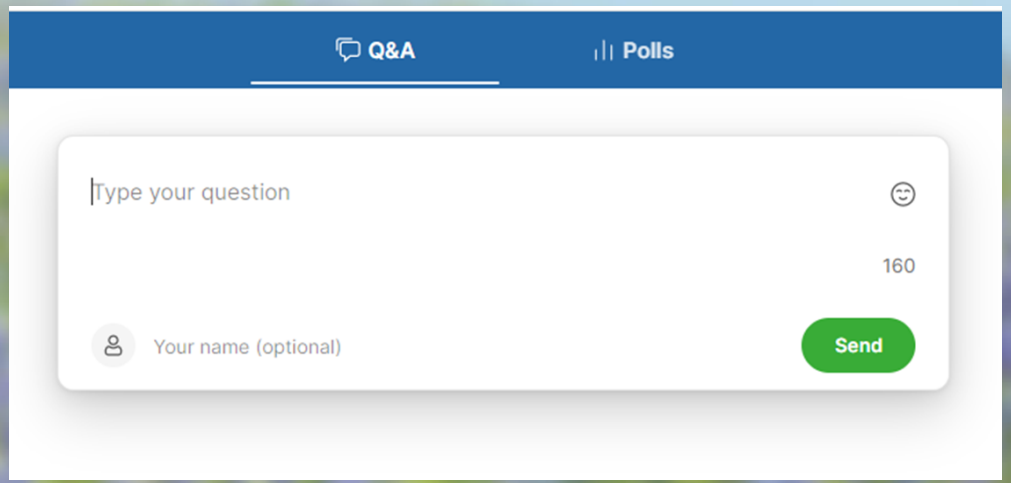
Texas RE Spring Standards, Security, & Reliability Workshop

April 1, 2026

AGENDA

- Aggregation of Control
- CIP-003-9 Low Impact BES Remote Connectivity
- Frequency and Voltage Protection Settings for Generation Resources
- Common Root Cause Codes
- FERC Update
- Large Loads Interconnection in ERCOT
- NERC CIP Drip
- Supply Chain Resilience in a World of Geopolitical Cyber Risk
- AI-Augmented Embedded Security Assessment for BES Resilience

To submit questions during the workshop, please visit **slido.com** and enter today's participant code: **TXRE**



Welcome & Instructions

Matthew Barbour
Texas RE
Manager, Communications & Training

STANDARDS, SECURITY, & RELIABILITY
SPRING WORKSHOP

Antitrust Admonition

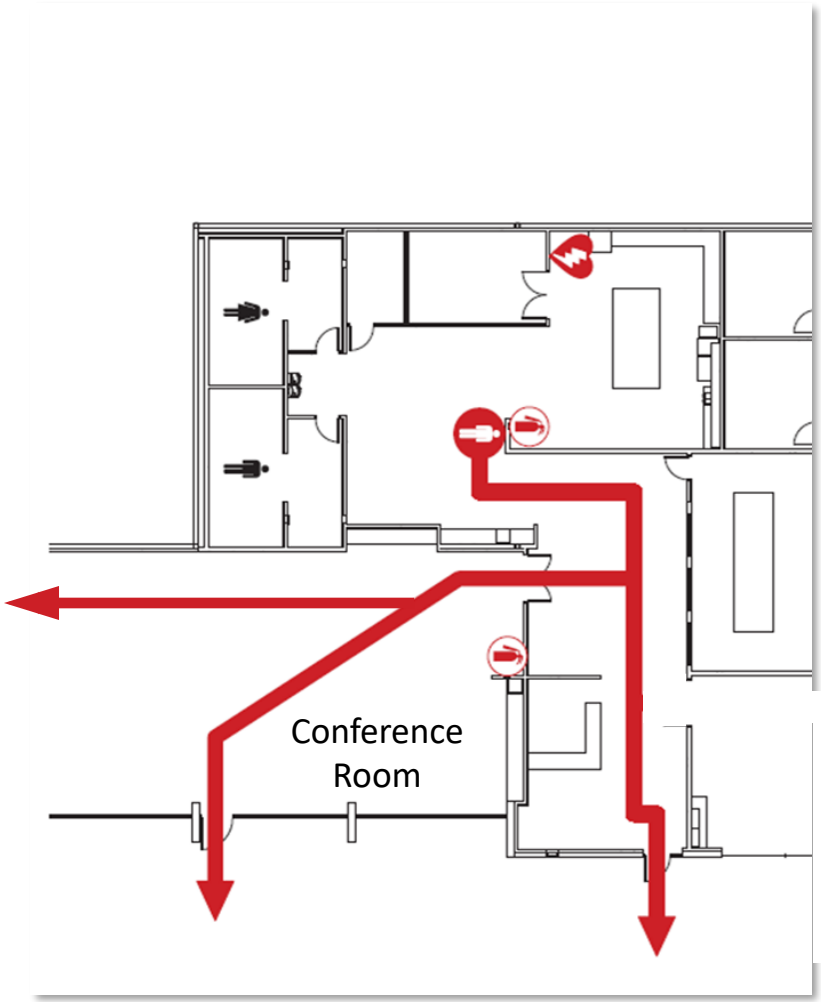
Because this event brings together market participants who may be viewed as actual or potential competitors, we must be mindful to conduct it in a manner that is consistent with the antitrust and competition laws. Participants should not disclose non-public, proprietary, or competitively sensitive information.

Attendees should exercise independent judgment and avoid even the appearance of discussions of agreements or concerted actions that may be viewed as restraining competition. Any questions on Texas RE's Antitrust Compliance Corporate Policy may be directed to Texas RE's General Counsel.

Safety Moment

In case of emergency, evacuate through the nearest door

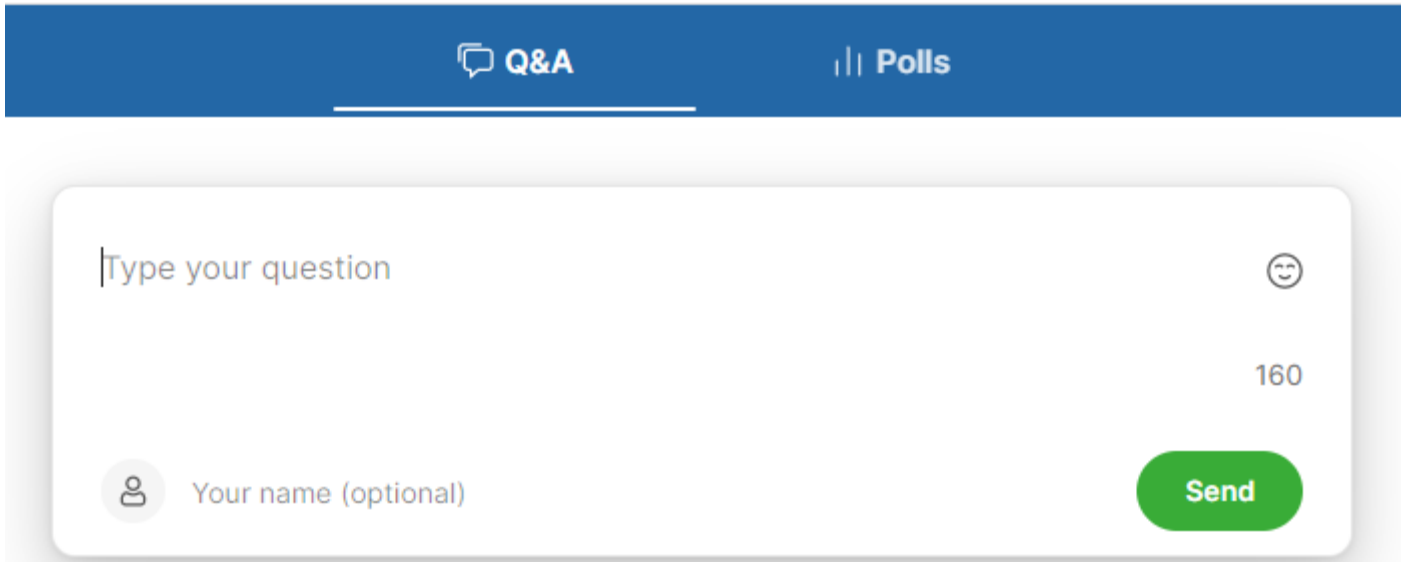
Rally point is in the front parking lot



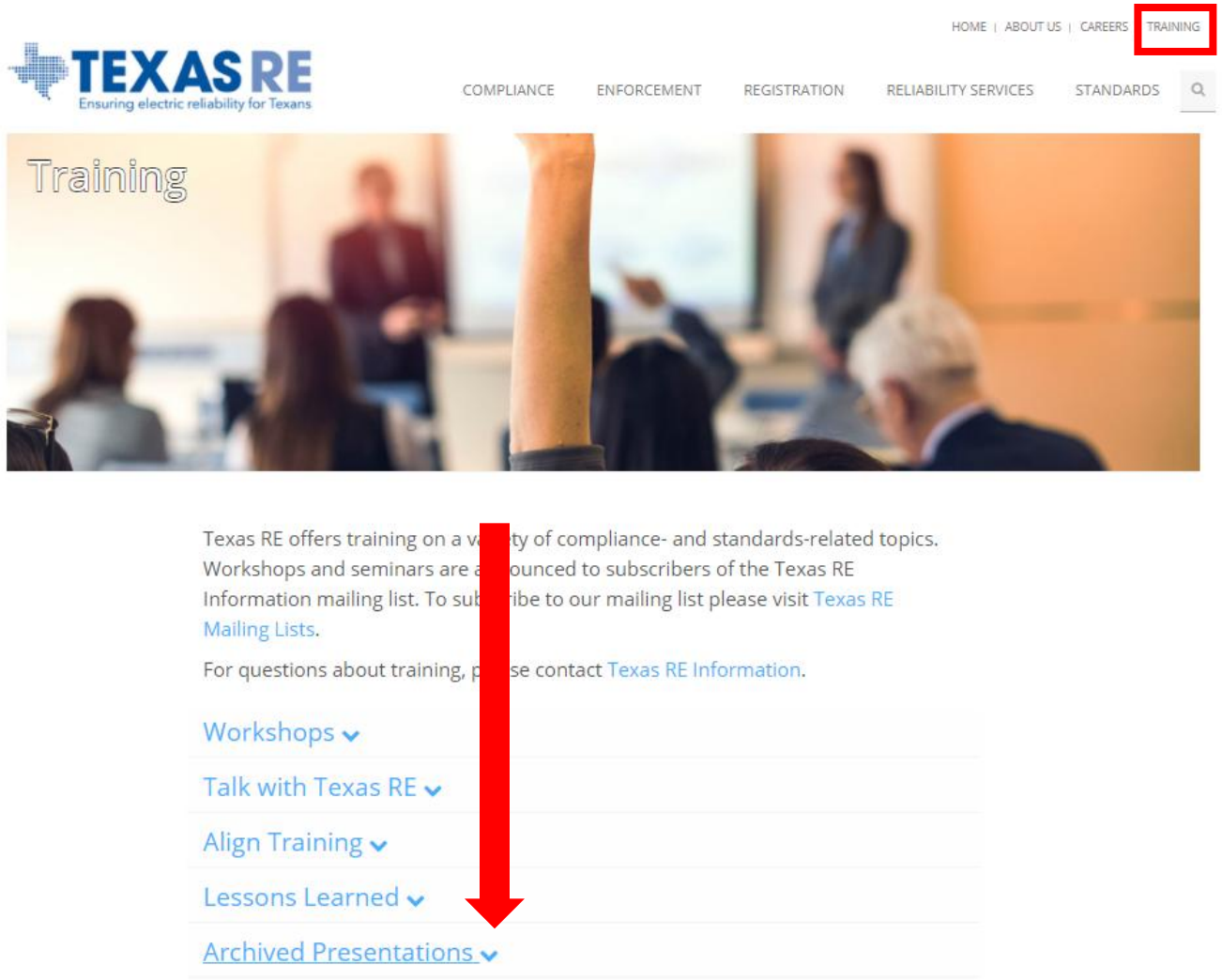
Questions

To submit questions during the workshop, please visit **slido.com** and enter today's participant code: **TXRE**

slido



Training Page



Archived Presentations

All of Texas RE's outreach activities are free and open to the public. Past presentations delivered by Texas RE staff are available here. Please be aware that presentations will not be available indefinitely, and may be removed to comply with Texas RE's document retention policy.

ALIGN

Align Release 1 Training | Recording

Align Release 2 Periodic Data Submittal Training | Recording

Align Release 2 TFE and Self-Certification Training | Recording

Align Release 3 Training | Recording

Align Release 4 & 4.5 Training | Recording

Workshops

Women's Leadership in Grid Reliability and Security Conference | Recording

Understanding New Generator Obligations | Recording

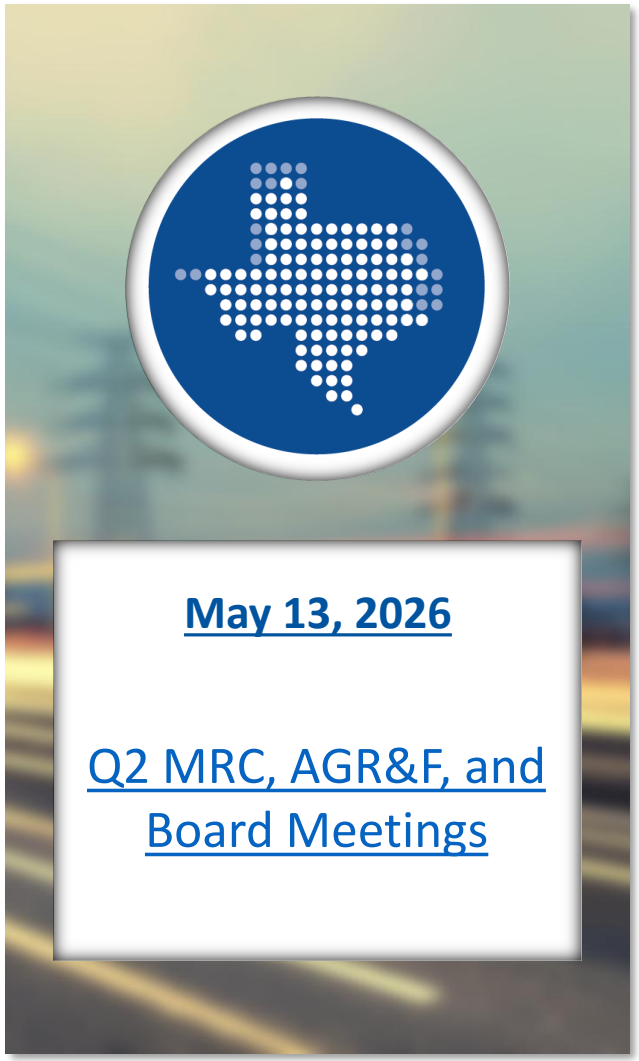
Fall Standards, Security, and Relia

2025 Fall Standards, Security, and Reliability Workshop | Recording

Spring Standards, Security, and Reliability Workshop

2026 Spring Standards, Security, and Reliability Workshop

Upcoming Events at Texas RE



May 13, 2026

Q2 MRC, AGR&F, and Board Meetings

August 19, 2026

Winter Weatherization Workshop

November 4, 2026

Fall Standards, Security, & Reliability Workshop

Social Media

/texas-reliability-entity-inc

@Texas_RE_Inc

/TexasReliabilityEntity

Executive Welcome

Joseph Younger
Texas RE
Senior Vice President & Chief Operating Officer

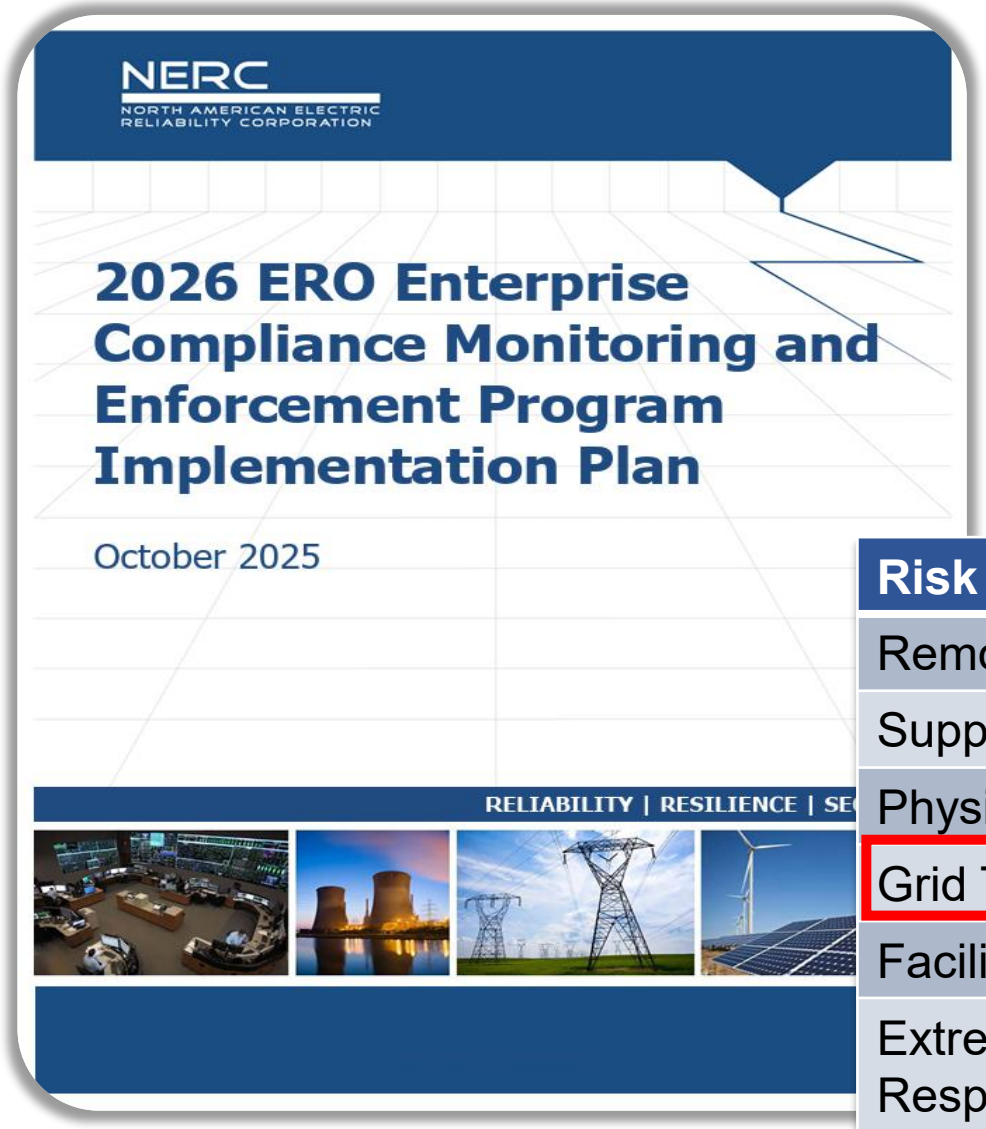
TEXAS RE

Aggregation of Control

Jason Georgoulis
CIP Physical & Cyber Security Analyst

April 1, 2026

Risk Focus & CMEP IP Risk Factors



Risk Elements
Remote Connectivity
Supply Chain
Physical Security
Grid Transformation
Facility Ratings
Extreme Weather Response

2026 CMEP IP – Grid Transformation Risks

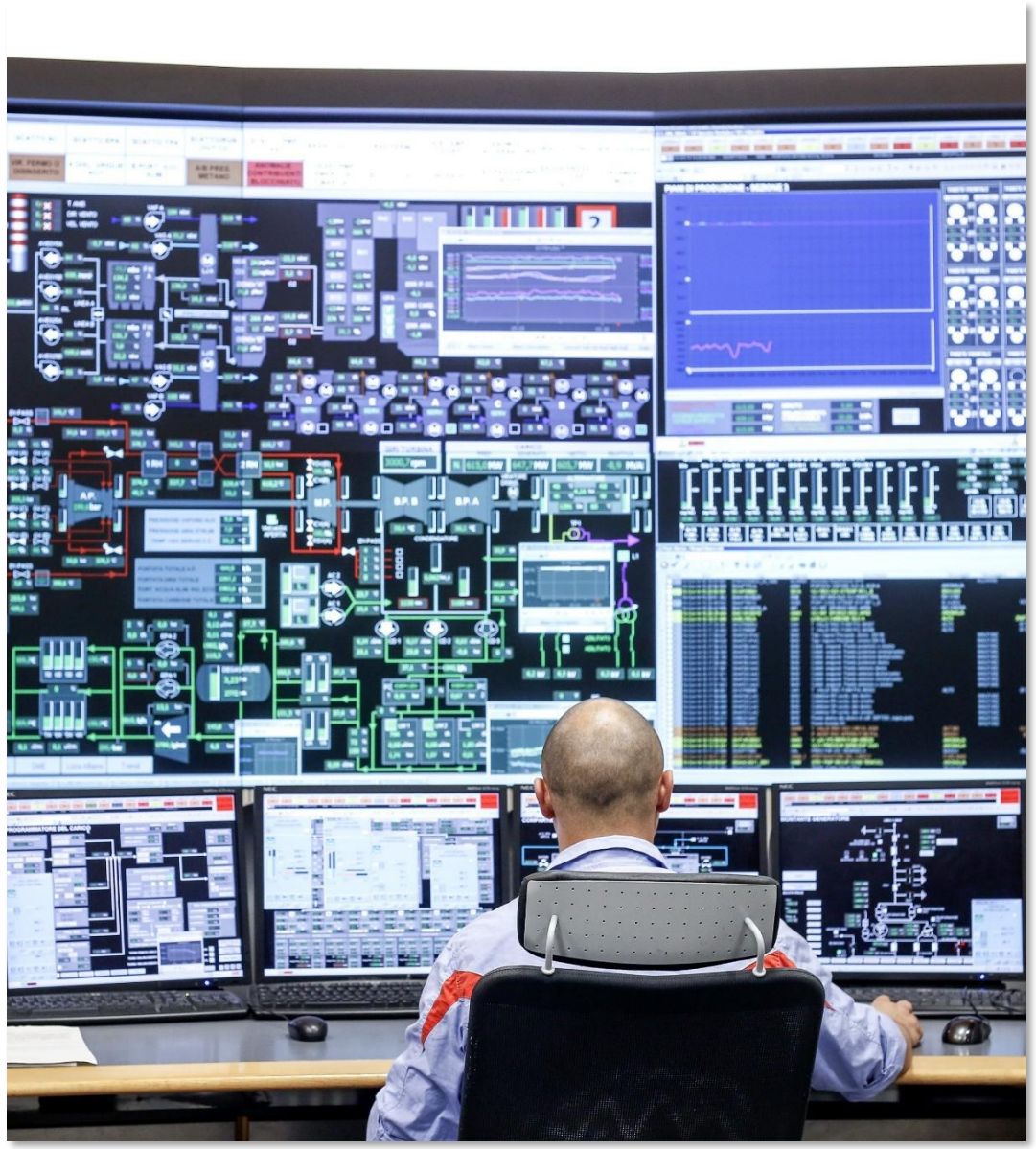
Table 5: Grid Transformation			
Rationale	**Standard**	**Req**	**Entities for Attention**
Address aggregation of control concerns over third parties performing day-to-day operations. Ensure proper identification of Control Centers to afford required security controls.	CIP-002-5.1a	R1	Balancing Authority Distribution Provider Generator Operator Generator Owner Reliability Coordinator Transmission Operator Transmission Owner

Control Center Definition

Control Center

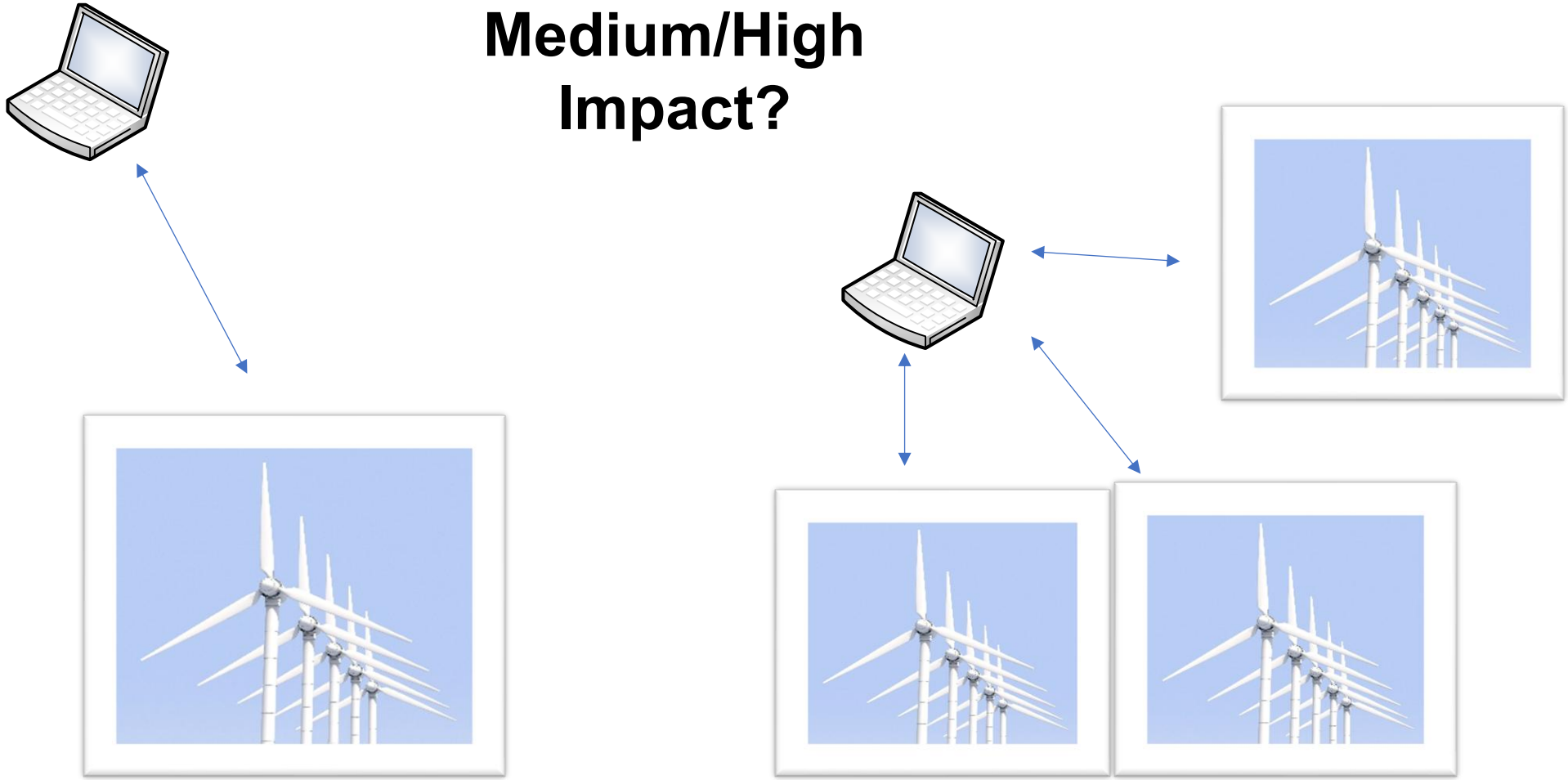
One or more facilities hosting operating personnel that monitor and control the Bulk Electric System (BES) in Real-time to perform the reliability tasks, including their associated data centers of:

1) Reliability Coordinators
2) Balancing Authorities
3) Transmission Operators for transmission Facilities at two or more locations
4) Generator Operators for generation Facilities at two or more locations

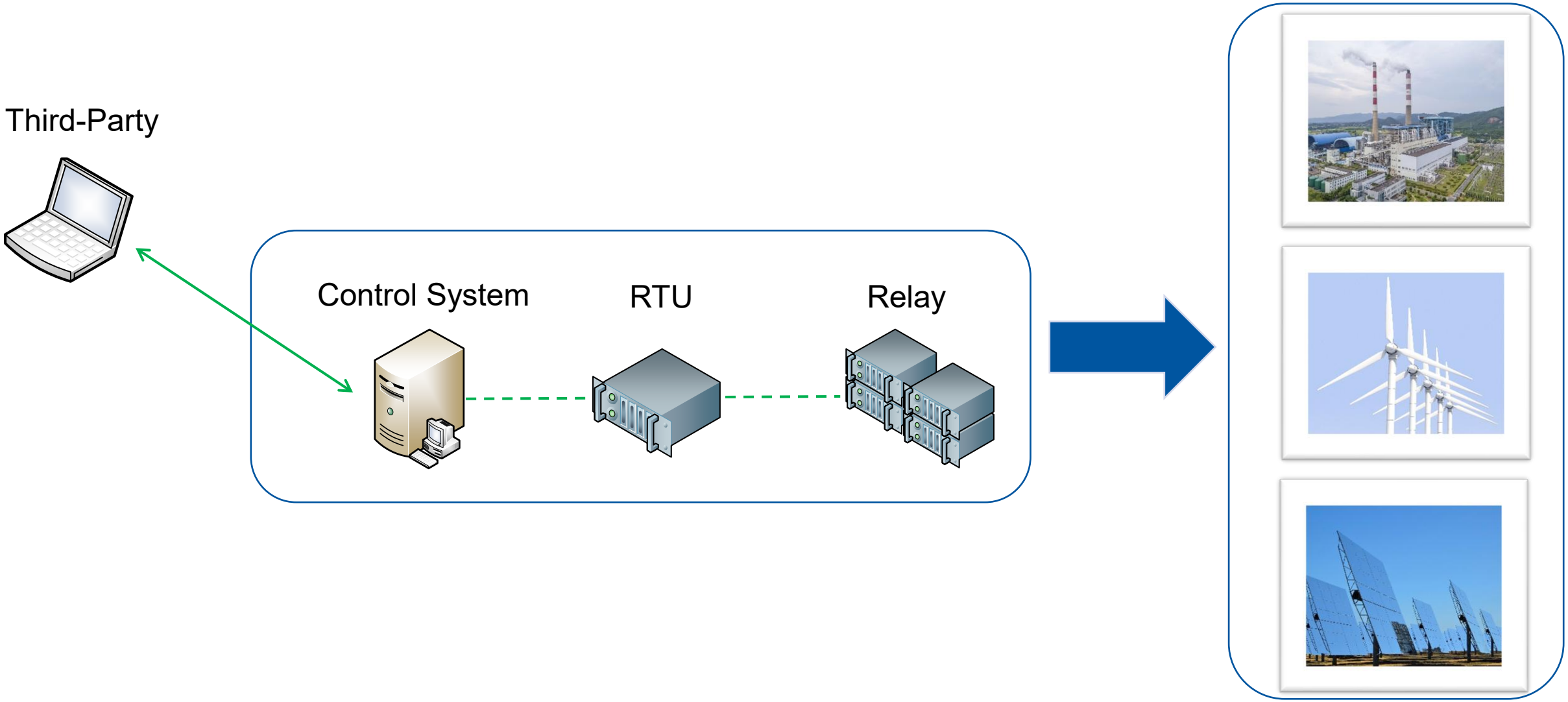


Low vs. High Risk

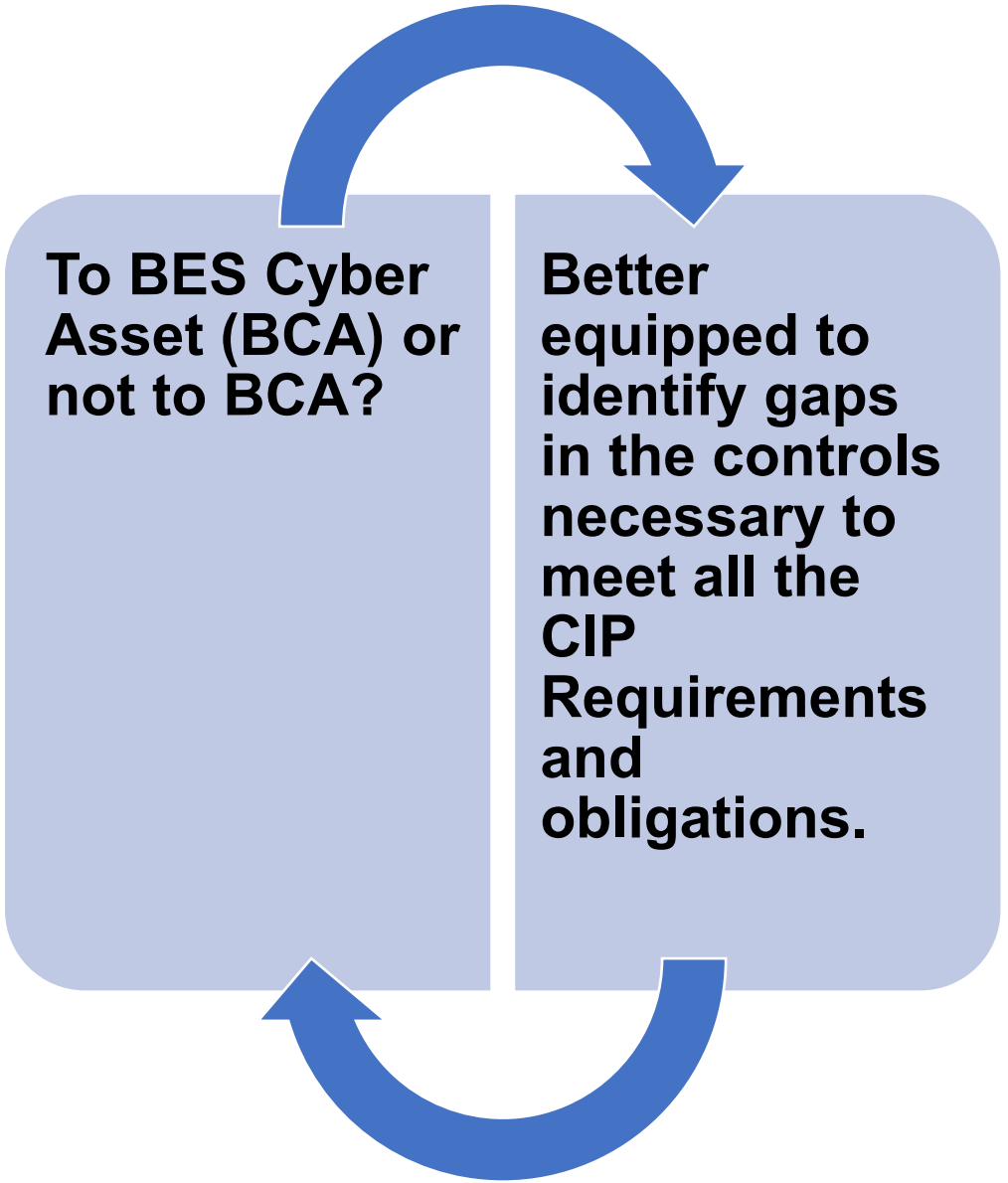
Low or Medium/High Impact?



Third-Party Monitoring or Control



CIP-002 Considerations for Third-Party Cyber Assets



Third-Party Vendor and Device Risks

Risks

- Unauthorized Access
- Exploitation of Device Vulnerabilities
- Introduction of Malware

Controls

- Background Checks/Offboarding
- Device Management Policies
- Cyber Hygiene SCRM

Remote Connection Risks

Location of Third-Party?

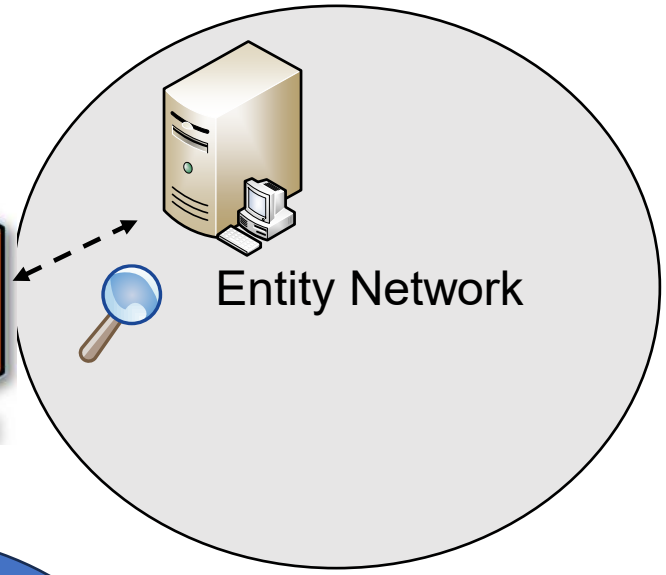
Third-Party

Unauthorized Disclosure? Encryption

Malicious Communications? Monitoring, Logging, Access Control

Unauthorized Access? MFA

Firewall



Privileged Access?

Persistent Connection? No

Detective Controls

Recap Risks vs. Controls

Risks

- Unauthorized disclosure
- Unauthorized access
- Introduction of malicious communications/code
- Lack of visibility

Controls

- Encryption
- MFA, strict ACLs, privileged access policies
- IDS/IPS, SIEM, device management policies, deep pack inspection
- Methods to monitor and terminate sessions

Best Practices

- Understand what technology makes the facility work
- Understand the configuration
- Sufficient training and education

Resources

NERC	2026 ERO Enterprise CMEP Implementation Plan
NERC	2025 NER CIP Roadmap
RF	2024 CIP Themes and Lessons Learned
CISA	2023 Top Routinely Exploited Vulnerabilities | CISA Nation-State Cyber Actors | Cybersecurity and Infrastructure Security Agency CISA
NIST	SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations | CSRC Cryptographic Standards and Guidelines | CSRC

Questions?

TEXAS RE
Ensuring electric reliability for Texans

TEXAS RE

CIP-003-9 Low Impact BES Remote Connectivity

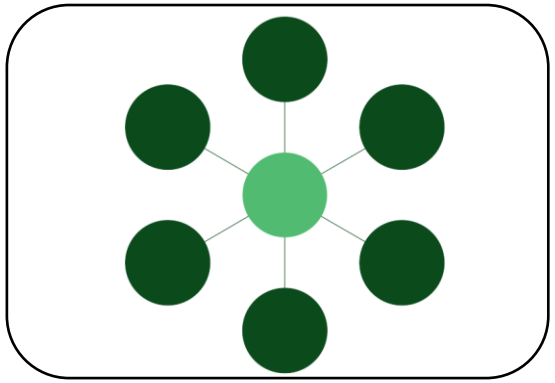
Rebekah Barber
CIP Compliance Team Lead

April 1, 2026

Agenda

- Why CIP-003-9?
- What Does the Standard Say?
- What is Applicable?
- Potential Implementation and Evidence Needed
- Best Practices

Why Are We Talking About This?



Aggregation of Control

Registration of IBRs

CMEP IP

Effective Date

What is CIP-003-9?

Background

What's New?

What Does the Standard Say?

R2

- Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1.

Attachment 1

- Responsible Entities shall include each of the sections provided below in the cyber security plan(s) required under Requirement R2.
- Responsible Entities with multiple-impact BES Cyber Systems ratings can utilize policies, procedures, and processes for their high or medium impact BES Cyber Systems to fulfill the sections for the development of low impact cyber security plan(s). Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets.

Section 6: Vendor Electronic Remote Access Security Controls

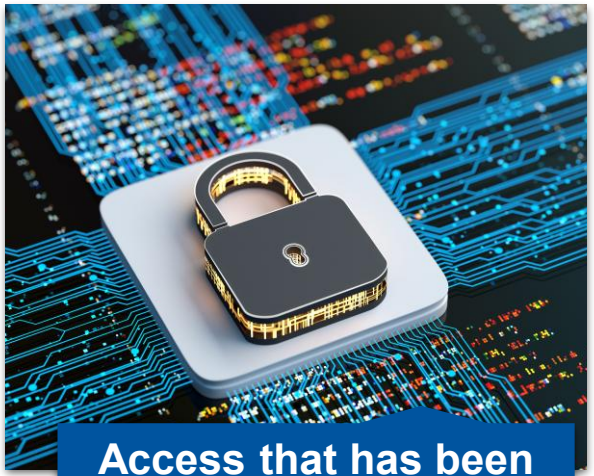
- For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, that allow vendor electronic remote access, the Responsible Entity shall implement a process to mitigate risks associated with vendor electronic remote access, where such access has been established under Section 3.1.
- These processes shall include:
  - 6.1 One or more method(s) for determining vendor electronic remote access;
  - 6.2 One or more method(s) for disabling vendor electronic remote access; and
  - 6.3 One or more method(s) for detecting known or suspected inbound and outbound malicious communications for vendor electronic remote access.

Applicability

Assets containing low impact BES Cyber Systems (BCS)

Vendor

Electronic remote access



Access that has been established under section 3.1

Access Under Section 3.1

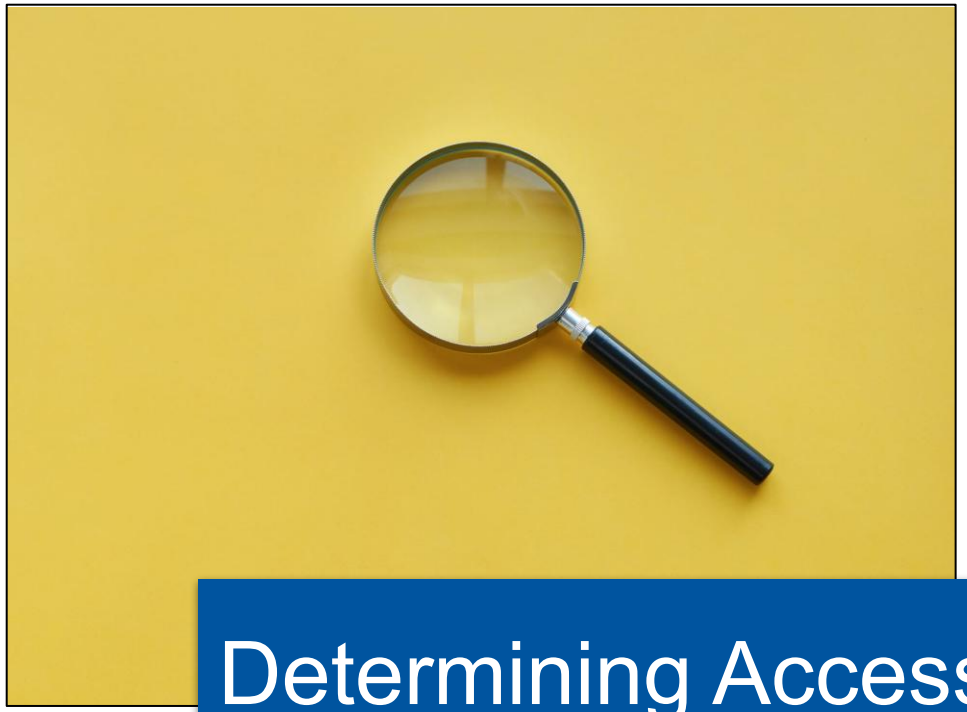
Section 3.1 Permits only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are:

- Between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s)
- Using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s)
- Not used for time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE)

Relationship with CIP-005-7

CIP-003-9	CIP-005-7
6.1 One or more method(s) for determining vendor electronic remote access	**2.4** Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access)
6.2 One or more method(s) for disabling vendor electronic remote access	**2.5** Have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system to-system remote access)
6.3 One or more method(s) for detecting known or suspected inbound and outbound malicious communications for vendor electronic remote access	**1.5** Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications

Implementation Considerations



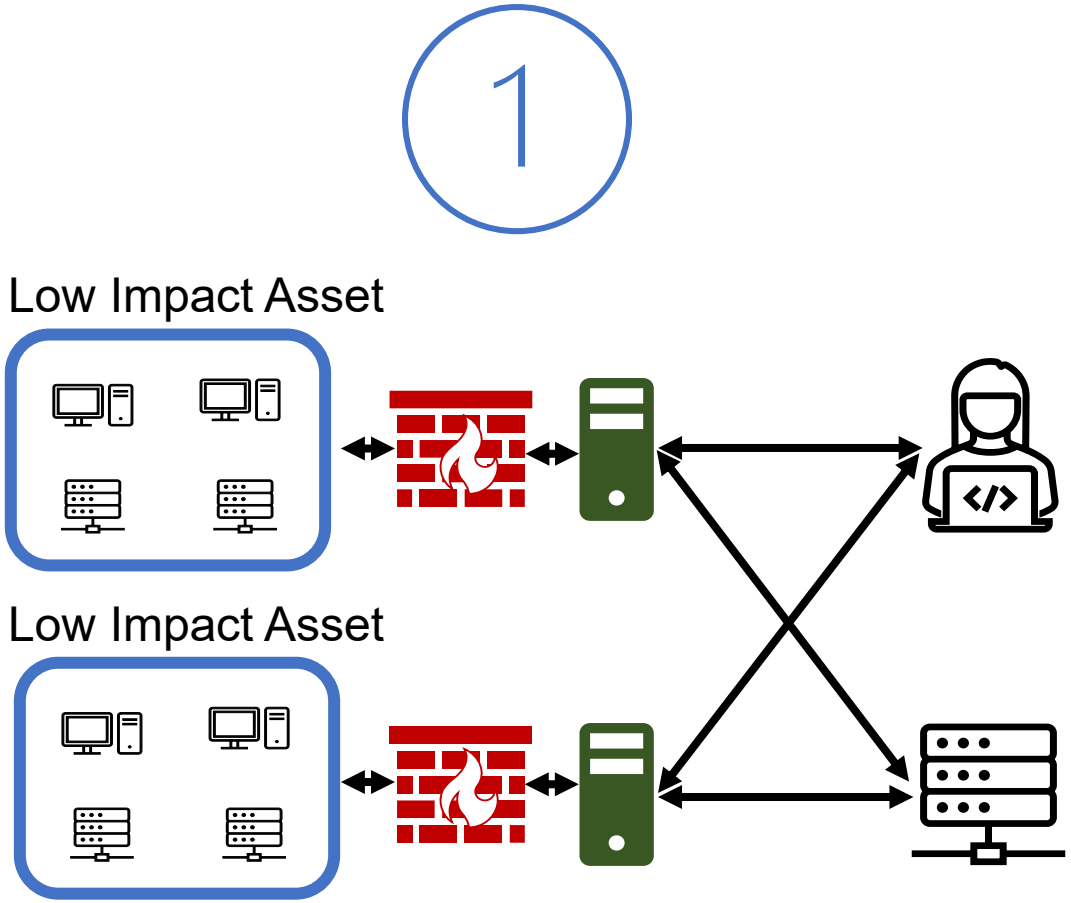
Determining Access

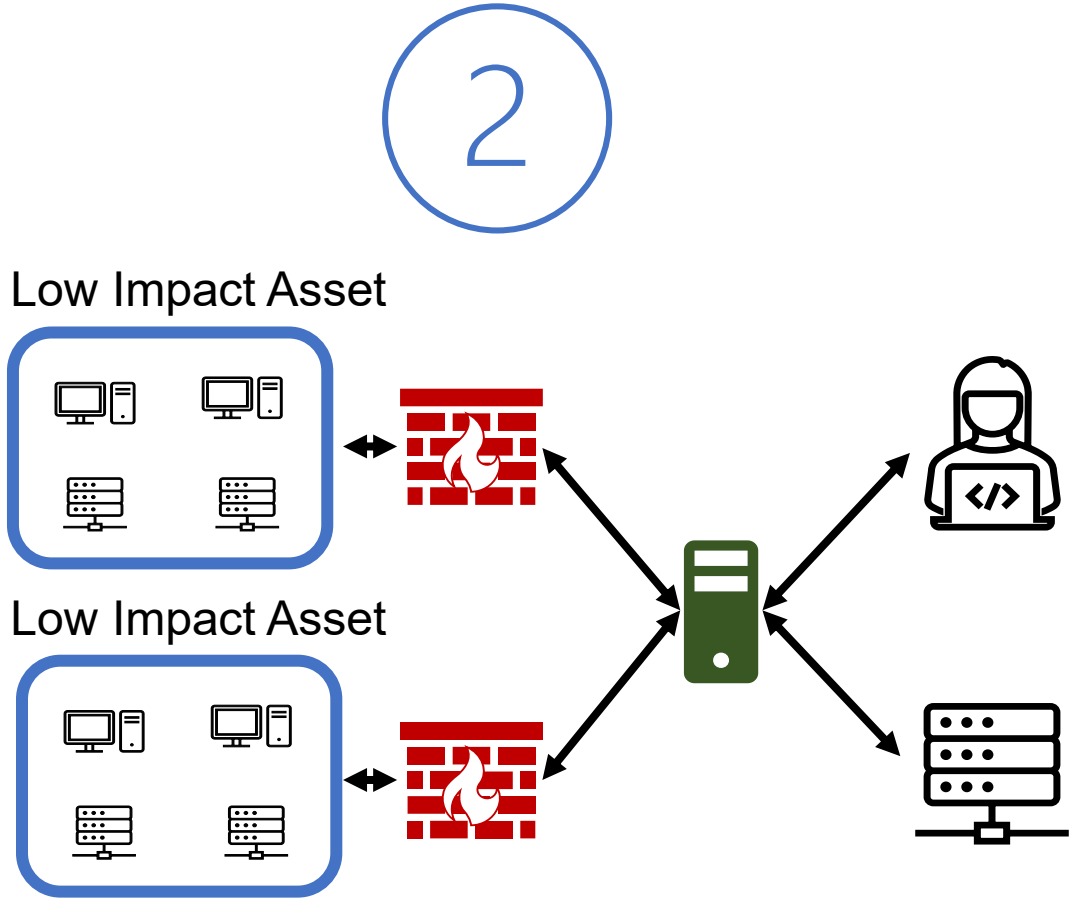
Disabling Access

Implementation Considerations

Detecting Malicious Communications

Example Electronic Access Diagram





Requested Evidence

- Process Documentation
- Firewall Rules
- Screenshots and System Generated Evidence

Best Practices

MFA

Alerting

Zero Trust

Additional Resources

- Guidelines and Technical Basis
- Technical Rational
- Texas RE Outreach
- CIPWG

Just So You Know…

CIP-012-2

July 1, 2026

Questions?

TEXAS RE
Ensuring electric reliability for Texans

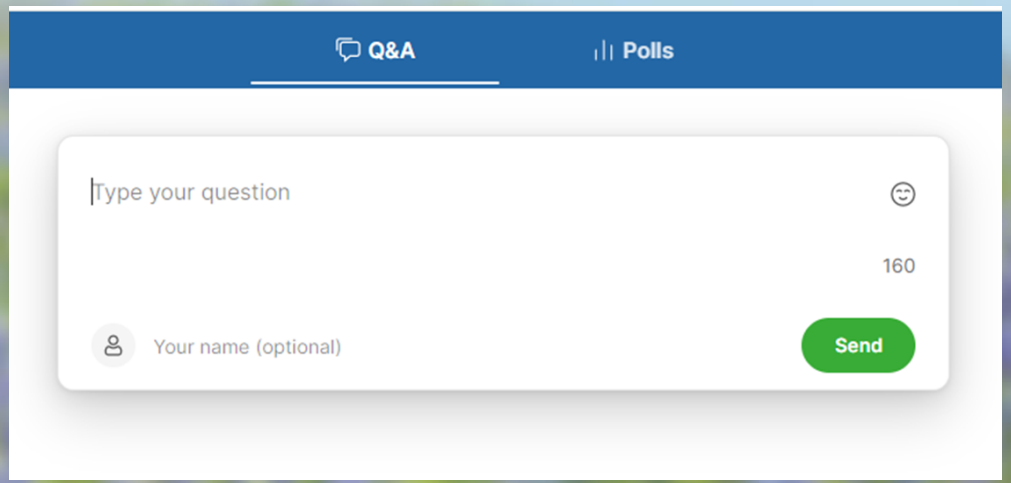
Texas RE Spring Standards, Security, & Reliability Workshop

Return at: 10:25 am

AGENDA

- Aggregation of Control
- CIP-003-9 Low Impact BES Remote Connectivity
- **Frequency and Voltage Protection Settings for Generation Resources**
- Common Root Cause Codes
- FERC Update
- Large Loads Interconnection in ERCOT
- NERC CIP Drip
- Supply Chain Resilience in a World of Geopolitical Cyber Risk
- AI-Augmented Embedded Security Assessment for BES Resilience

To submit questions during the workshop, please visit **slido.com** and enter today's participant code: **TXRE**

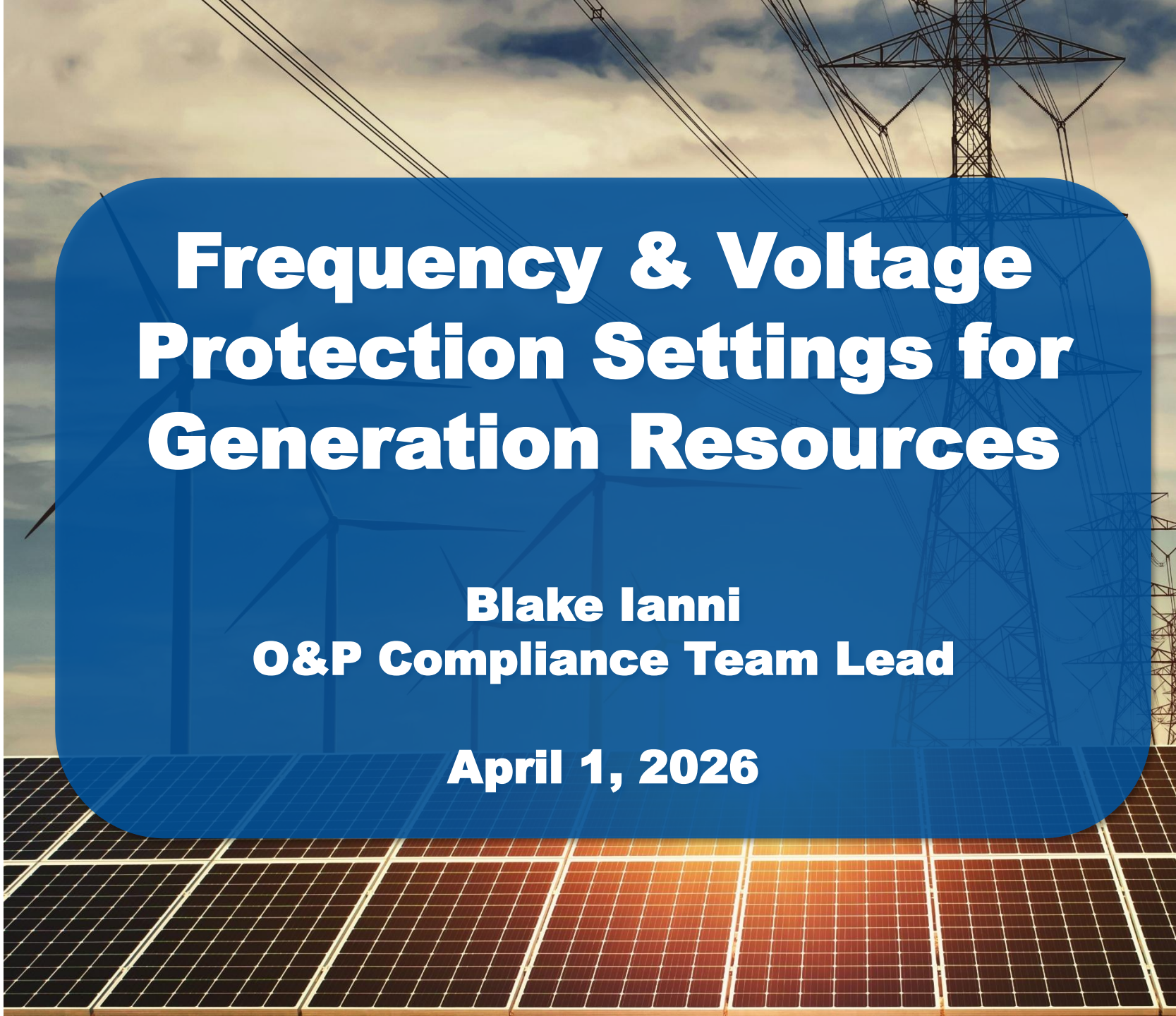


TEXAS RE

Frequency & Voltage Protection Settings for Generation Resources

Blake Ianni
O&P Compliance Team Lead

April 1, 2026



Agenda

PRC-024-4

- Background & Requirements

PRC-028-1 & PRC-029-1

- Background & Implementation Plans

Protection Settings Best Practices & Controls

Comparison to NOGRR245

Periodic Data Submittals (PDS) Process

Sli.do (#TXRE)

Slido Question

What risks do PRC-028-1 & PRC-029-1 address?

Protection Settings Objectives

Ensure settings are properly calculated for applicable frequency & voltage protections

Analyze the effects of frequency & voltage excursions on the system protection

Set frequency & voltage protection to prevent trips & momentary cessation within the “no trip zone”

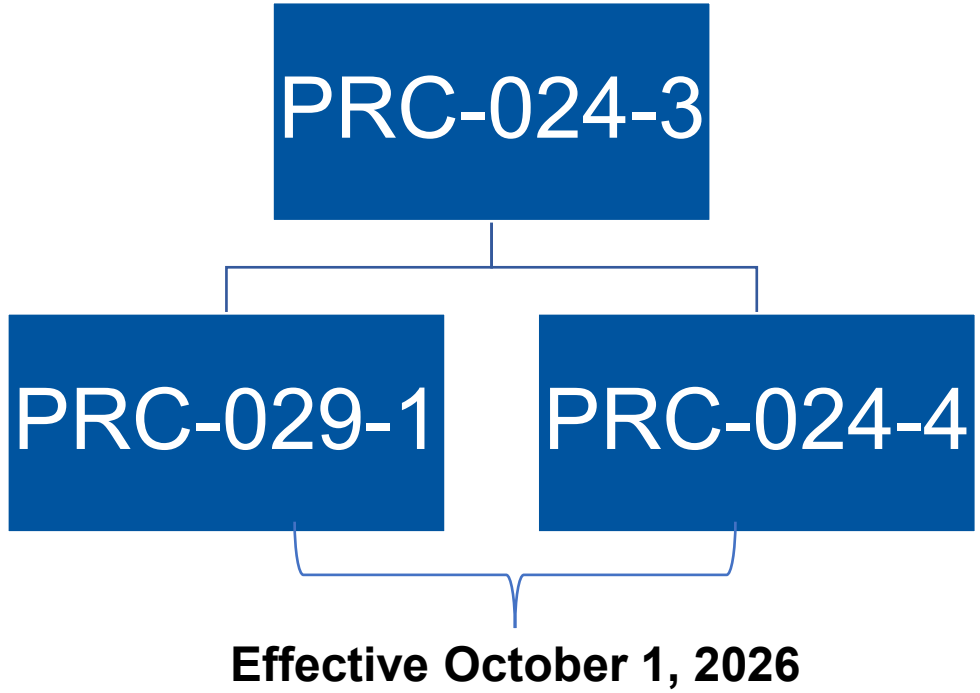
Upcoming Protection Setting Standards

PRC-024-4 Applicability

- Generator Owners (GOs) and Transmission Owners (TOs) that apply protection settings
- Synchronous generators
- Type 1 and Type 2 wind resources
- Synchronous condensers

PRC-029-1 Applicability

- Generator Owner
  - Bulk Electric System (BES) IBRs
  - Non-BES IBRs with:
    - Aggregate nameplate ≥ 20 mVA **and**
    - Connected to common point of connection ≥ 60 kV



PRC-024-4 Requirements Overview

Frequency and Voltage Protection Settings

- GO & TO are responsible for:
  - Setting its frequency protection (R1)
  - Setting its voltage protection (R2)
  - Documenting each known equipment limitation that prevents Facility from meeting protection criteria in R1 or R2 (R3)
  - Providing protection settings to its Planning Coordinator (PC) or Transmission Planner (TP) when requested within 60 days (R4)

Ride-through vs. Protection Settings

- Remain connected during defined frequency and voltage events
- Should be specific to the voltage and frequency protective capabilities
- Outside of the curves is the “may-trip zone”

PRC-024-4 Requirement R1 Attachment 1

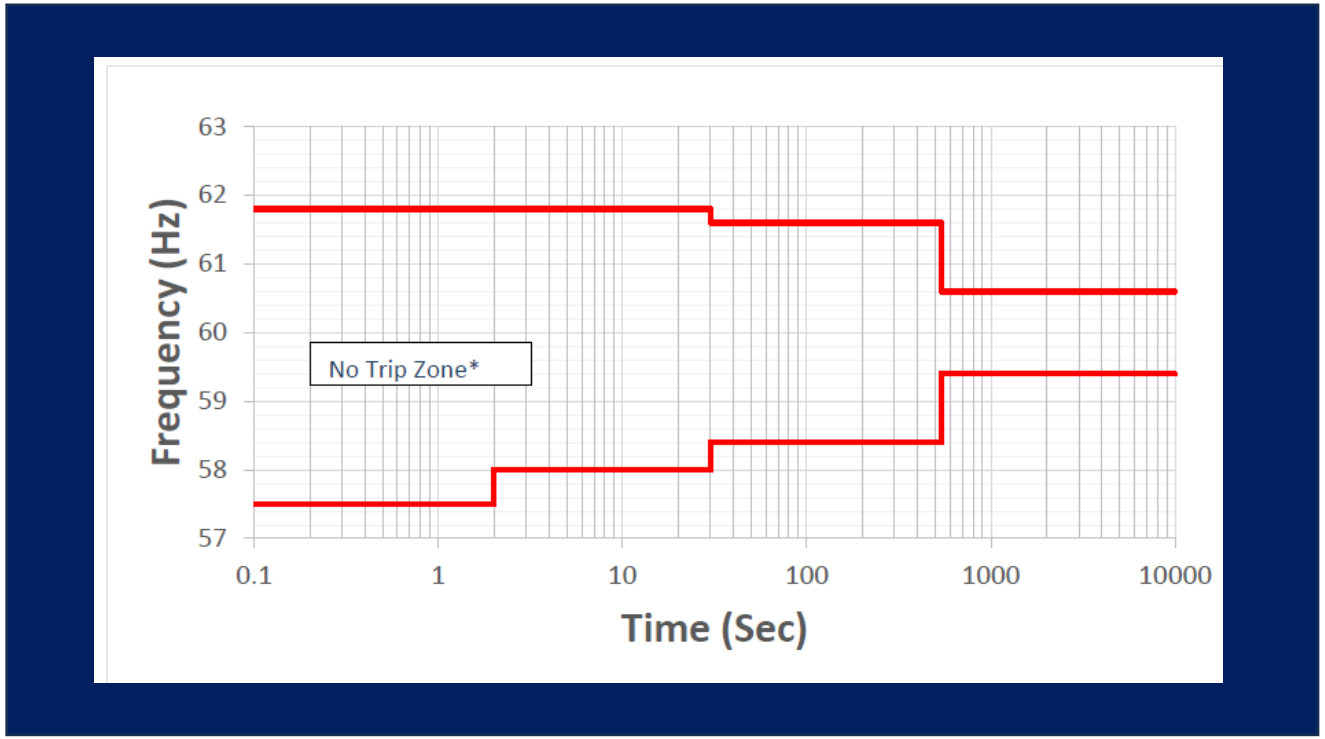


Table 4: Frequency Boundary Data Points – ERCOT Interconnection

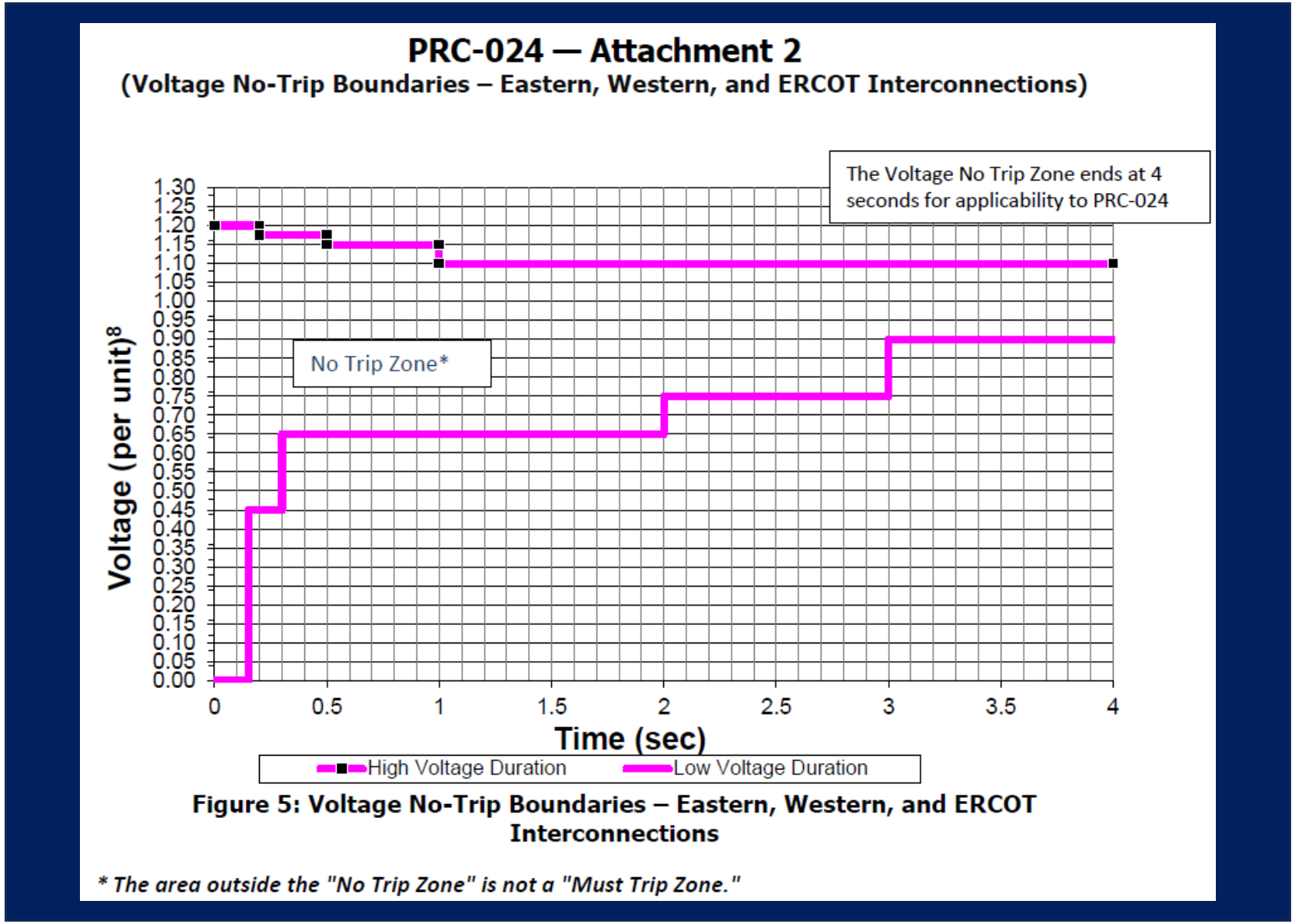
High Frequency Duration		Low Frequency Duration	
Frequency (Hz)	Minimum Time (Sec)	Frequency (Hz)	Minimum Time (sec)
≥61.8	Instantaneous[11]	≤57.5	Instantaneous[11]
≥61.6	30	≤58.0	2
≥60.6	540	≤58.4	30
<60.6	Continuous operation	≤59.4	540
		>59.4	Continuous operation

PRC-024-4 Requirement R2 Attachment 2

Table 5: Voltage Boundary Data Points

High Voltage Duration		Low Voltage Duration	
Voltage (per unit)	Minimum Time (sec)	Voltage (per unit)	Minimum Time (sec)
≥1.200	0.00	<0.45	0.15
≥1.175	0.20	<0.65	0.30
≥1.15	0.50	<0.75	2.00
≥1.10	1.00	<0.90	3.00
<1.10	4.00	≥ 0.90	4.00

PRC-024-4 Requirement R2 Attachment 2



PRC-024-4 Requirements R3 & R4

Document each known regulatory or equipment limitation that prevents the Facility from meeting R1 or R2 protection criteria

- Examples: Study results, experience from an event or manufacturer's advice
- Limitations originating in the *equipment protected by the relay(s)*

R3.1: Communicate limitations to PC and TP

- Within 30 calendar days of: Identifying a limitation, repairing or replacing equipment with limitations, or creating or adjusting limitations caused by consumption of cumulative turbine life-time frequency excursion allowance

R4: Provide protection settings to PC or TP

- Within 60 calendar days of written request
- Within 60 calendar days of change to previously requested settings

Protection Standards for IBRs
PRC-028-1 & PRC-029-1

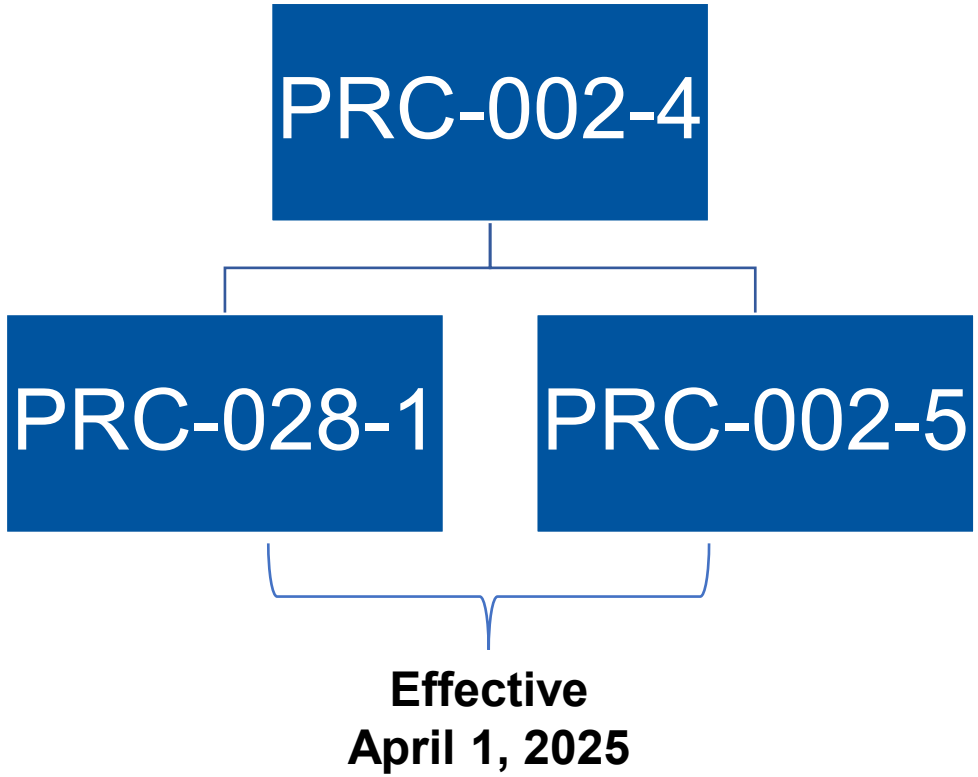
Background of PRC-028-1

PRC-002-5 Applicability

- Reliability Coordinator
- Transmission Owner
- Generator Owner
  excluding inverter-based resources (IBRs)

PRC-028-1 Applicability

- Generator Owner
  - Facilities:
    - Bulk Electric System (BES) IBRs
    - Non-BES IBRs with:
      - Aggregate nameplate ≥ 20 mVA **and**
      - Connected to common point of connection ≥ 60 kV



PRC-028 Disturbance Monitoring and Reporting for IBRs

Purpose

- To have adequate data available from IBRs to evaluate IBR Ride-through performance during system disturbances and to provide data for IBR model validation

Requirements

- R1 – Sequence of event recording (SER) data
- R2 & R3 – Fault recording (FR) data
- R4 & R5 – Dynamic Disturbance Recording (DDR) data
- R6 – Time synchronization
- R7 – Providing data
- R8 – Restoring recording capability

PRC-028-1 Implementation Plan

*BES IBRs

Commercial Operations Date (COD) on/before 4/1/2025

- ❑ 12/31/2028-50% of BES IBRs comply with R1-R7
- ❑ 1/1/2030-100% of BES IBRs comply with R1-R7

COD after 4/1/2025 but within 15 calendar months of Effective Date**

- ❑ 100% of BES IBRs comply with R1-R7 within 15 calendar months

COD after 15 calendar months of Effective Date

- ❑ 100% of BES IBRs comply with R1-R7 by COD

BES IBRs (Regardless of COD)

- ❑ R8—comply by 1/1/2026

Non-BES IBRs (Category 2)

Commercial Operations Date (COD) on/before 5/15/2026

- ❑ 1/1/2030-100% of non-BES IBRs comply with R1-R7

COD after 5/15/2026 but within 15 calendar months of Effective Date**

- ❑ 100% of non-BES IBRs comply within 15 calendar months

COD after 15 calendar months of Effective Date

- ❑ 100% of non-BES IBRs comply with R1-R7 by COD

Non-BES IBRs (Regardless of COD)

- ❑ R8—comply by 4/1/2027

**Effective Date: April 1, 2025*

***Refer to CMEP Practice Guide: Implementation of "Annual" and "Calendar Month(s)"*

PRC-029-1 Frequency and Voltage Ride-through for IBRs

Purpose

- To ensure that IBRs Ride-through to support the Bulk Power System (BPS) during and after defined frequency and voltage excursions

Applicability

- Generator Owner
  - BES IBRs
  - Non-BES IBRs with:
    - Aggregate nameplate ≥ 20 mVA **and**
    - Connected to common point of connection ≥ 60 kV

Requirements

- R1 & R2 – Voltage Ride-through capabilities
- R3 – Frequency Ride-through capabilities
- R4 – Hardware limitations

PRC-029-1 Implementation Plan—Design vs. Operations

The Implementation Plan (IP) for PRC-029 bifurcates the capability-based (design) elements & the performance-based (operation) elements for PRC-029-1 for R1-R3

Design Capabilities for Voltage and Frequency Ride-through

- Entities must demonstrate the *design capability* for each IBR adheres to R1-R3 requirements
- From R1, Measure 1: "Each Generator Owner shall have evidence to demonstrate the design of each IBR will adhere to Ride-through requirements, as specified in Requirement R1."
  - Examples of evidence: dynamic simulations, studies, plant protection settings, and control settings design evaluation.

Operations (Performance-Based) Elements for Voltage and Frequency Ride-through

- Installing and *implementing* the settings in the field
- From R1, Measure 1: "Each Generator Owner shall retain evidence of actual disturbance monitoring (i.e., sequence of event recorder, dynamic disturbance recorder, and fault recorder) to demonstrate that the operation of each IBR did adhere to Ride-through requirements, as specified in Requirement R1."

PRC-029-1 Implementation Plan

*BES IBRs

Commercial Operations Date (COD) on/before Effective Date

- 10/1/2026—100% of BES IBRs comply with R1, R2, & R3 ***design***

COD after Effective Date

- Immediately comply with R1, R2, & R3 ***design*** by COD

BES IBRs (Regardless of COD)

- Comply with R1, R2, and R3 ***operations*** aspect
- Date depends on PRC-028-1 deadlines (when entity establishes DME equipment capabilities under PRC-028-1)
- 10/1/2027—Requirement R4 exemptions due

Non-BES IBRs (Category 2)

- 1/1/2027-100% of non-BES IBRs comply with R1, R2, & R3 ***design***

Non-BES IBRs (Regardless of COD)

- Comply with R1, R2, and R3 ***operations*** aspect
- Date depends on PRC-028-1 deadlines (when entity establishes DME equipment capabilities under PRC-028-1)
- 10/1/2027—Requirement R4 exemptions due

**Upcoming Effective Date: October 1, 2026*

Protection Settings—Best Practices & Controls

- Periodically perform an evaluation of Ride-through capability
- Collaborate closely with equipment manufacturer on settings & any firmware upgrades, or parameter changes needed after installation
- Base settings on equipment capability & leave a buffer zone between trip settings & the must Ride-through zone

PRC-029-1 vs. ERCOT's NOGRR245 Overview

NOGRR245 has Frequency Ride-through (FRT) Requirements for Distribution Generation Resources (DGRs) & Distribution Energy Storage Resources (DESRs), whereas NERC PRC-029-1 does not apply to these resources

NOGRR245 FRT zone is more conservative

PRC-029-1 High Voltage Ride-through (VRT) criteria extends to 1,800 seconds

Voltage Ride-Through Criteria-Wind IBRs

PRC-029-1

Attachment 1: Voltage Ride-Through Criteria

Table 1: Voltage Ride-through Requirements for AC-Connected Wind IBR [13]

Voltage (per unit)[14]	Operation Region	Minimum Ride-Through Time (sec)
> 1.20	N/A[15]	N/A
≥ 1.10	Mandatory Operation Region	1.0
> 1.05	Continuous Operation Region	1800
≤ 1.05 and ≥ 0.90	Continuous Operation Region	Continuous
< 0.90	Mandatory Operation Region	3.00
< 0.70	Mandatory Operation Region	2.50
< 0.50	Mandatory Operation Region	1.20
< 0.25	Mandatory Operation Region	0.16
< 0.10	Permissive Operation Region	0.16

NOGRR245

2.9.1.1 Preferred Voltage Ride-Through Requirements for Transmission-Connected Inverter-Based Resources (IBRs)

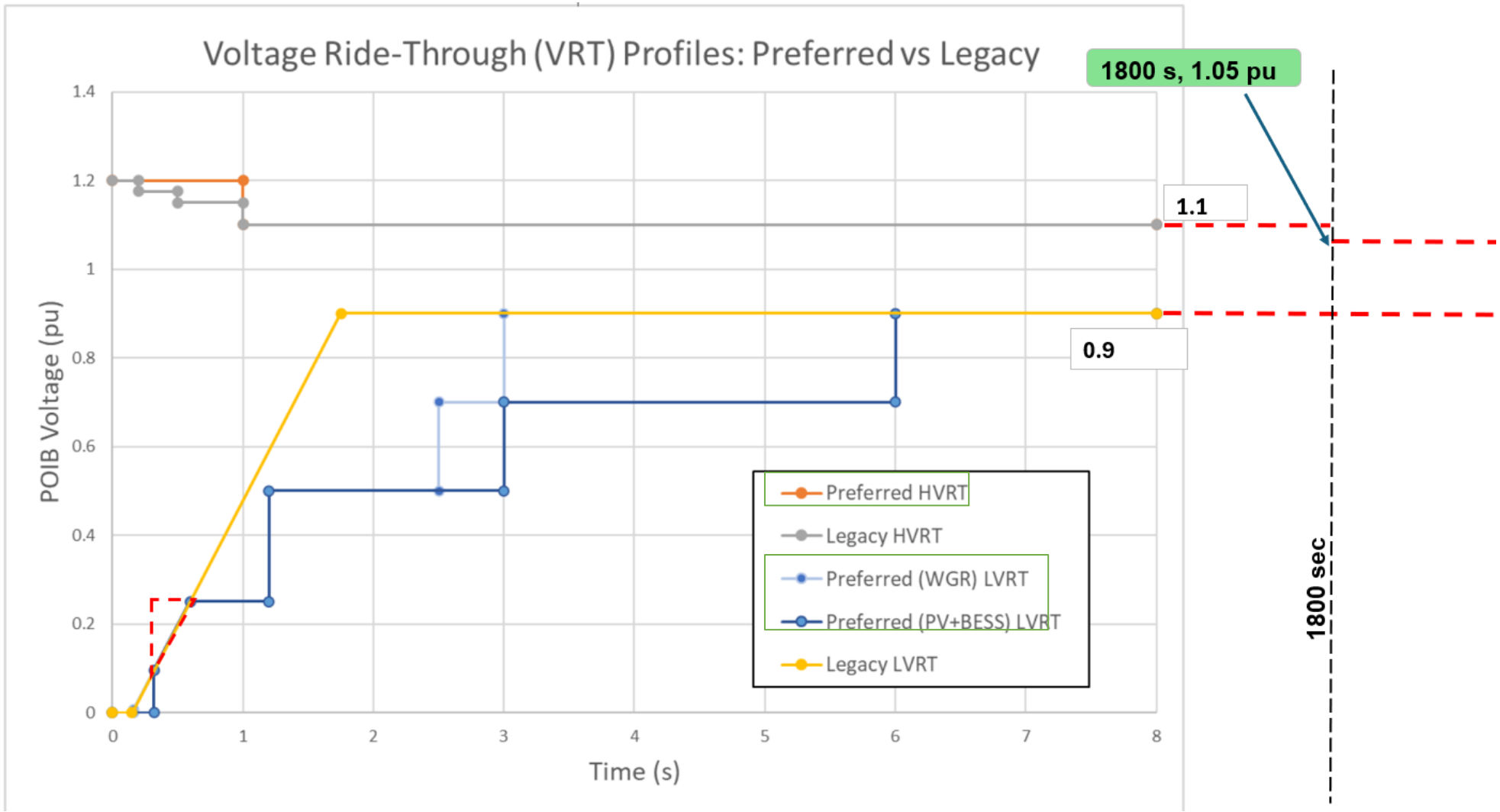
(1) All IBRs subject to this Section shall ride through the root-mean-square voltage conditions in Tables A or B below, as applicable, as measured at the IBR's POIB:

Table A: Applicable to WGR IBRs

Root-Mean-Square Voltage (p.u. of nominal)	Minimum Ride-Through Time (seconds)
V > 1.20	May ride-through or trip
1.10 < V ≤ 1.20	1.0
0.90 ≤ V ≤ 1.10	continuous
0.70 ≤ V < 0.90	3.0
0.50 ≤ V < 0.70	2.5
0.25 ≤ V < 0.50	1.2
0.005625 ≤ V < 0.25	(V+0.084375)/0.5625
V < 0.005625	0.16

ERCOT preserves portion of legacy curve

NOGRR245 vs. PRC-029-1 VRT Curves



Frequency Ride Through (FRT) Criteria for IBRs

PRC-029-1 Attachment 2

Table 3: Frequency Ride-through Capability Requirements

System Frequency (Hz)	Minimum Ride-Through Time (sec)
> 61.8	May trip
> 61.2	299
≤ 61.2 and ≥ 58.8	Continuous
< 58.8	299
< 57.0	May trip

NOGRR245 2.6.2.1 (1)

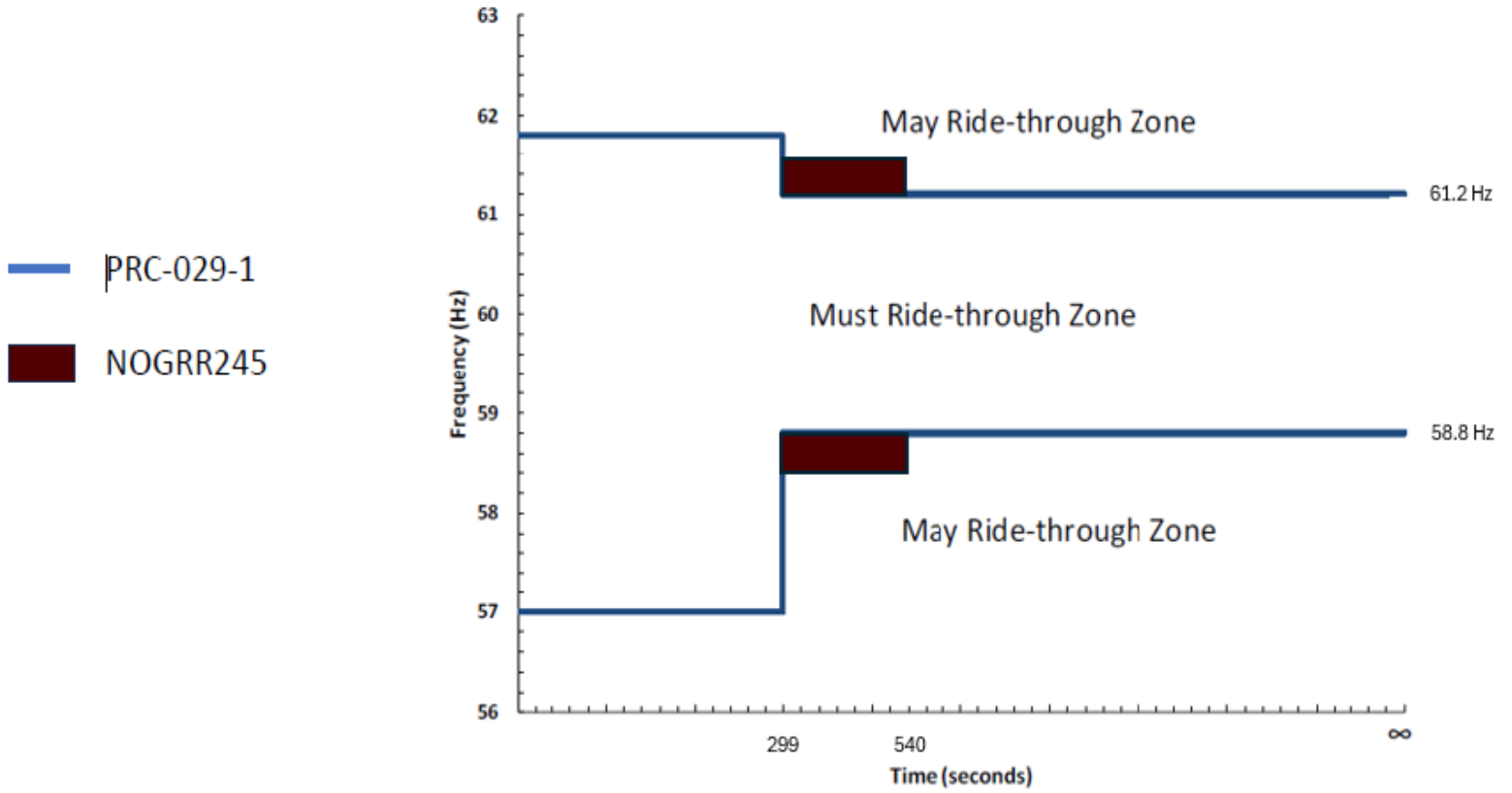
2.6.2.1 Frequency Ride-Through Requirements for Transmission-Connected Inverter-Based Resources (IBRs), Type 1 Wind-Powered Generation Resources (WGRs) and Type 2 WGRs

(1) This Section applies to all IBRs, Type 1 Wind-powered Generation Resources (WGRs) and Type 2 WGRs connected to the ERCOT Transmission Grid. Such Resources shall ride through the frequency conditions at the Resource's Point of Interconnection Bus (POIB) specified in the following table:

Frequency (f) in (Hz)	Minimum Ride-Through Time (seconds)
f > 61.8	May ride-through or trip
61.6 < f ≤ 61.8	299
61.2 < f ≤ 61.6	540
58.8 ≤ f ≤ 61.2	continuous
58.4 ≤ f < 58.8	540
57.0 ≤ f < 58.4	299
f < 57.0	May ride-through or trip

NOGRR245 vs. PRC-029-1 FRT Curves

NOGRR245 Must Ride-through zone is larger than PRC-029-1



PRC-029-1 vs. NOGRR245—Key Takeaways

NOGRR245 - Permits exemptions <u>for software and hardware limitations</u>

- Applies to Distribution Resources
- Generally has broader Ride-through zones

PRC-029-1 R4 - Permits exemptions <u>only for hardware limitations</u>

Periodic Data Submittals (PDSs) for PRC-028-1 & PRC-029-1

Periodic Data Submittal (PDS) Overview

PDSs for PRC-028-1

- R8-Corrective Action Plan (CAP) after failure of recording capability
- R1 through R8—Requesting extension of compliance dates (upcoming PDS)

PDS for PRC-029-1

- Upcoming PDS: R4-Hardware Limitations (Exemption from Ride-through criteria)

PRC-028-1 R8 Event-driven PDS for CAP

R8. Each Generator Owner shall, upon the discovery of a failure of the recording capability for the SER, FR, or DDR data: *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

- Restore the recording capability within 90 calendar days, or
- Submit a Corrective Action Plan (CAP) to the Regional Entity within 90 calendar days and then implement it according to CAP timeline.

❑PRC-028-1 R8 CAP Process

- Will submit within 90 calendar days through Align Period Data Submittal section
- Submit supporting documentation via ERO Secure Evidence Locker (SEL)
  - Include the CAP itself & evidence of implementation per CAP timeline
- Evidence can include:
  - Dated reports of discovery of a failure
  - Documentation with the date the data recording was restored
  - SCADA records
  - Dated CAP
- Able to submit within Align currently

PRC-028-1 PDS for Compliance Date Extension

Overview of PRC-028-1 Compliance Date Extension

- Based on the Implementation Plan for PRC-028-1
- GOs may request an extension from the compliance dates for Requirements R1-R8
- For IBRs that were COD before the April 1, 2025, effective date
- For circumstances beyond GO's control that prevent installation of Disturbance Monitoring Equipment on its IBRs
- Due at least three months prior to compliance date for which extension is being requested

PRC-028-1 PDS for Compliance Date Extension (Cont.)

PDS extension request module is being developed in Align

Will include a spreadsheet to download, complete, and upload to SEL

Must contain the info listed on pg.4 of IP

- **1.1.** Identification of the inverter-based resource(s) for which the entity requests the extension
- **1.2.** A plan for installing the Disturbance Monitoring Equipment and a timetable for completion
- **1.3.** A description of the circumstances precluding the timely installation of Disturbance Monitoring Equipment and how those circumstances are beyond the control of the entity
- **1.4.** Any other information the entity deems relevant to the Compliance Enforcement Authority's (CEA) consideration of its request

PRC-029-1 R4 Hardware Limitation PDS

PDS is currently being developed by ERO Enterprise

Due 12 months after effective date of Standard (October 1, 2027)

Align PDS and accompanying spreadsheet & evidence to SEL

Evidence should include all information in R4.1.1 through 4.1.5

- IBR info, which specific aspects of Ride-through requirements IBR is unable to meet
- ID the hardware piece(s) with limitation, relevant technical documentation
- Any plans to remedy limitation

R4.2-Provide copy of R4.1 information to associated entities

R4.3-Communicate replacement of hardware limitation

Acceptance of PDS

- Texas RE verifies GO submits all information in sub-Requirements of R4.1 (footnote 12 of PRC-029-1)

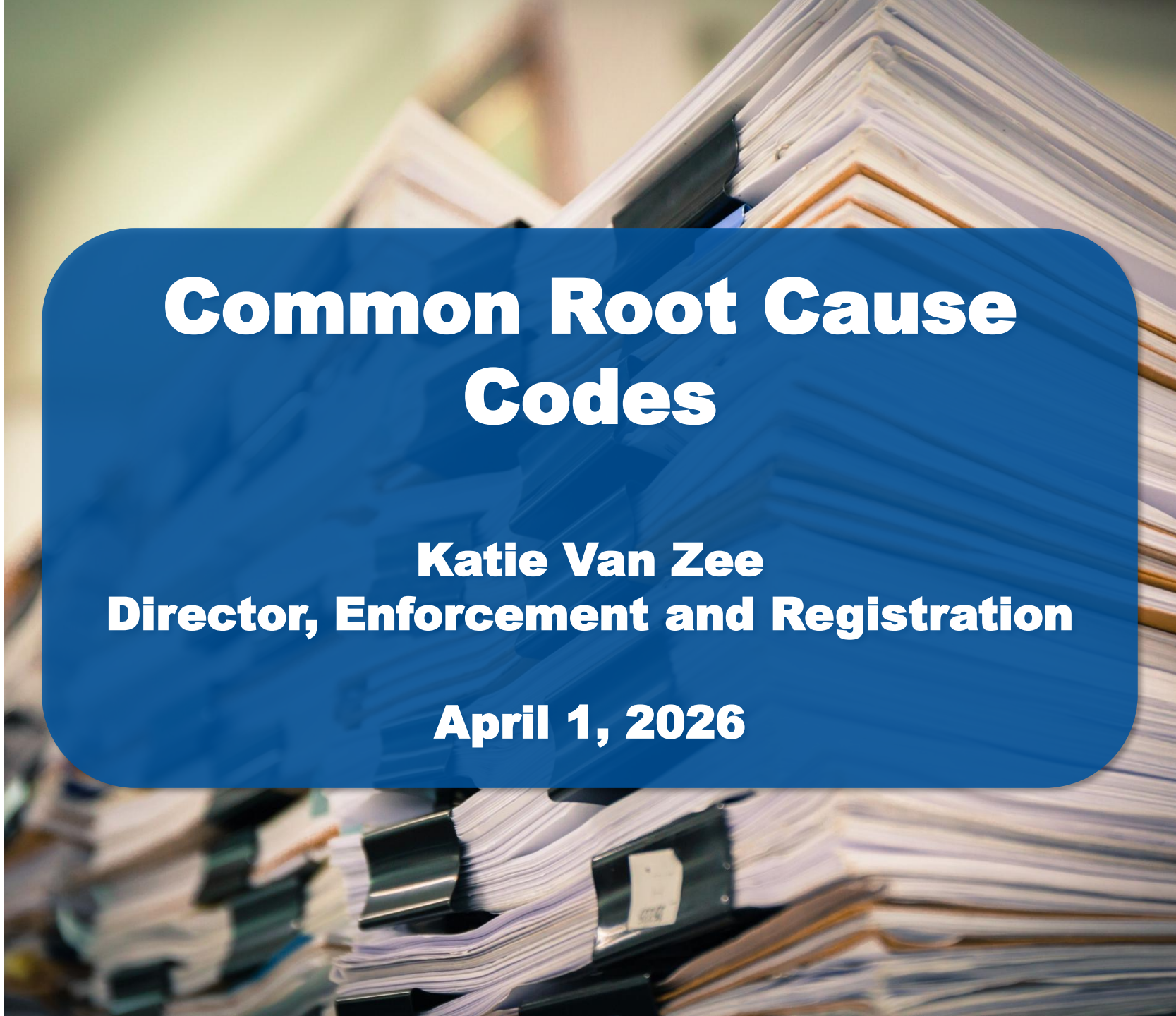
Resources

- PRC-024-4 Standard
- PRC-028-1 Standard
- PRC-028-1 RSAW
- PRC-029-1 Standard
- PRC-028-1 Implementation Plan
- PRC-024-4 & PRC-029-1 Implementation Plan
- CMEP Practice Guide on Annual & Calendar Months
- **NOGRR245 Info**
  - 245NOGRR-PUCT Report
  - PRC-029-1 & NOGRR245 Category 2 Registration Practice Guide
  - PRC-028 vs IEEE 2800-2022 vs NOGRR255
- **Project Pages**
  - 2020-02 Modifications to PRC-024 (Generator Ride-through)
  - 2021-04 Modifications to PRC-002 - Phase II
- **Technical Rationale**
  - PRC-024-4 Technical Rationale
  - PRC-028-1 Technical Rationale
  - PRC-029-1 Technical Rationale
- **Proposed Implementation Guidance**
  - PRC-029-1 Requirement R4

Questions?

TEXAS RE
Ensuring electric reliability for Texans

TEXAS RE



Common Root Cause Codes

Katie Van Zee
Director, Enforcement and Registration

April 1, 2026

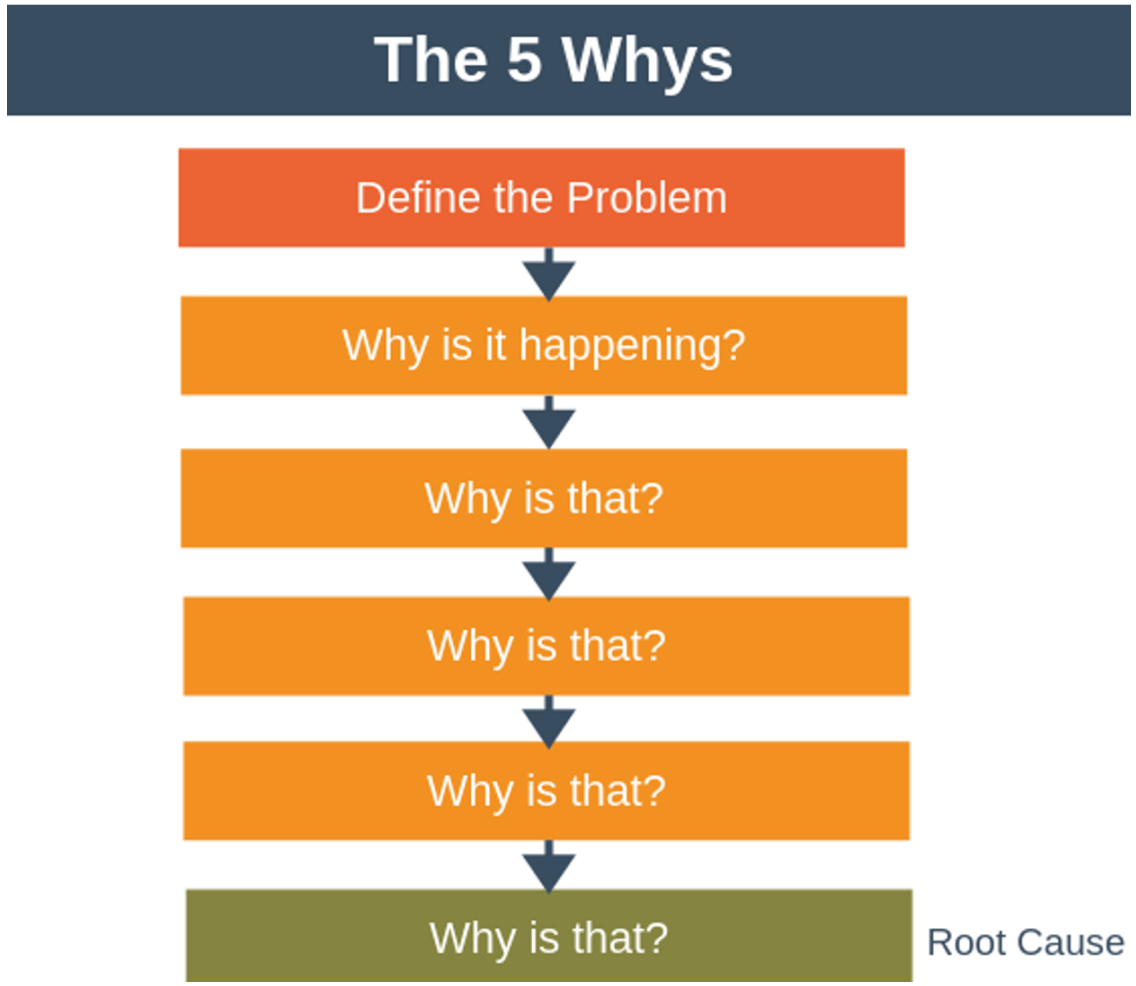
Roadmap

- Importance of Root Cause
- Align Root Cause Codes
- Most Common Root Cause Codes
- Best Practices to address Common Root Causes

Importance of Root Cause

Required analysis for disposition of Potential Non-compliance (PNC)

- Necessary to determine appropriate prevention of reoccurrence mitigation
- Help identify potential risks and best practices



Root Cause Codes Development

Q4 2023

Root Cause Codes introduced to Align for Regional users

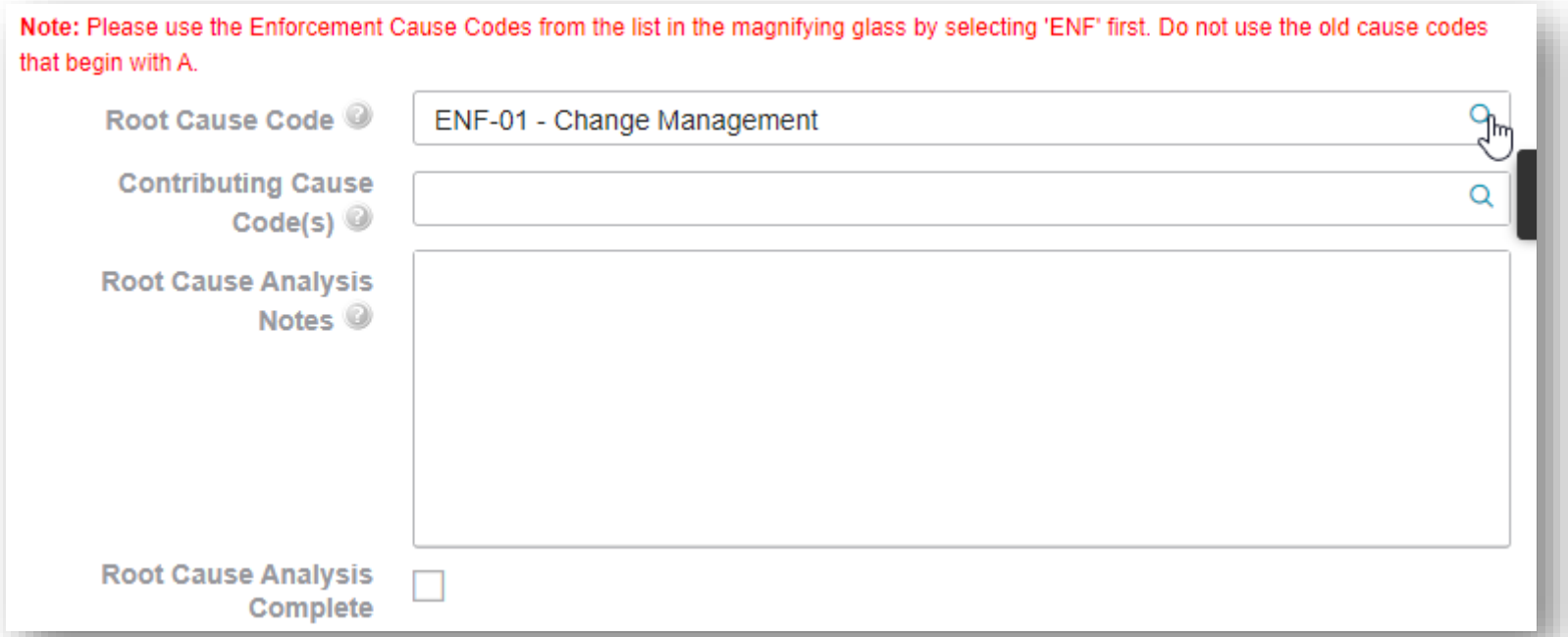
Q3 2025

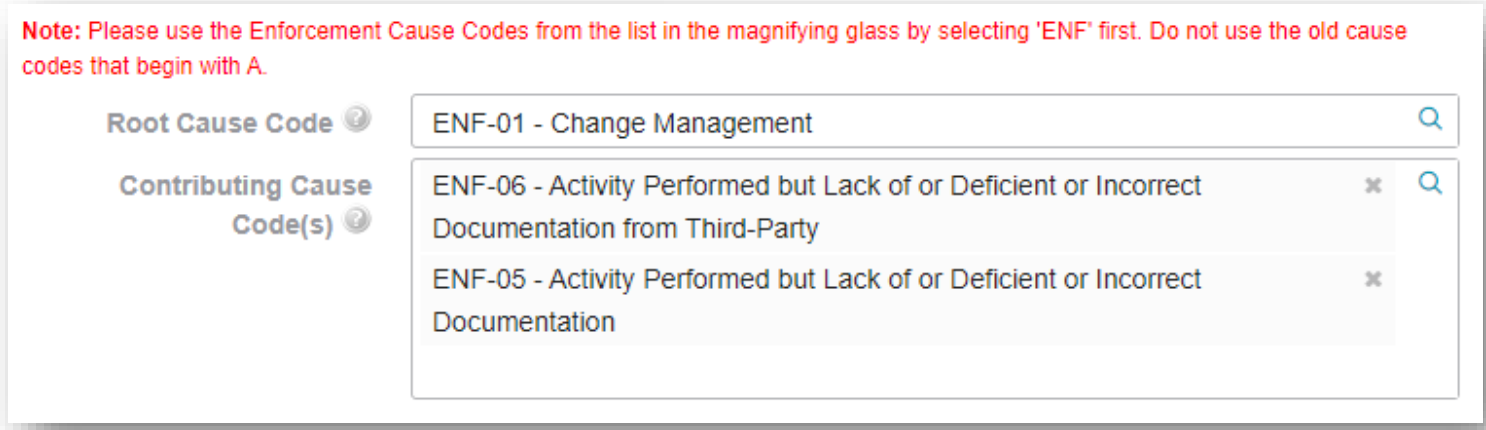
Available for registered entities to select on self-reported PNCs in 2025

Dec. 2024

NERC Cause Code User Guide in December 2024

Root Cause Code Selection in Align

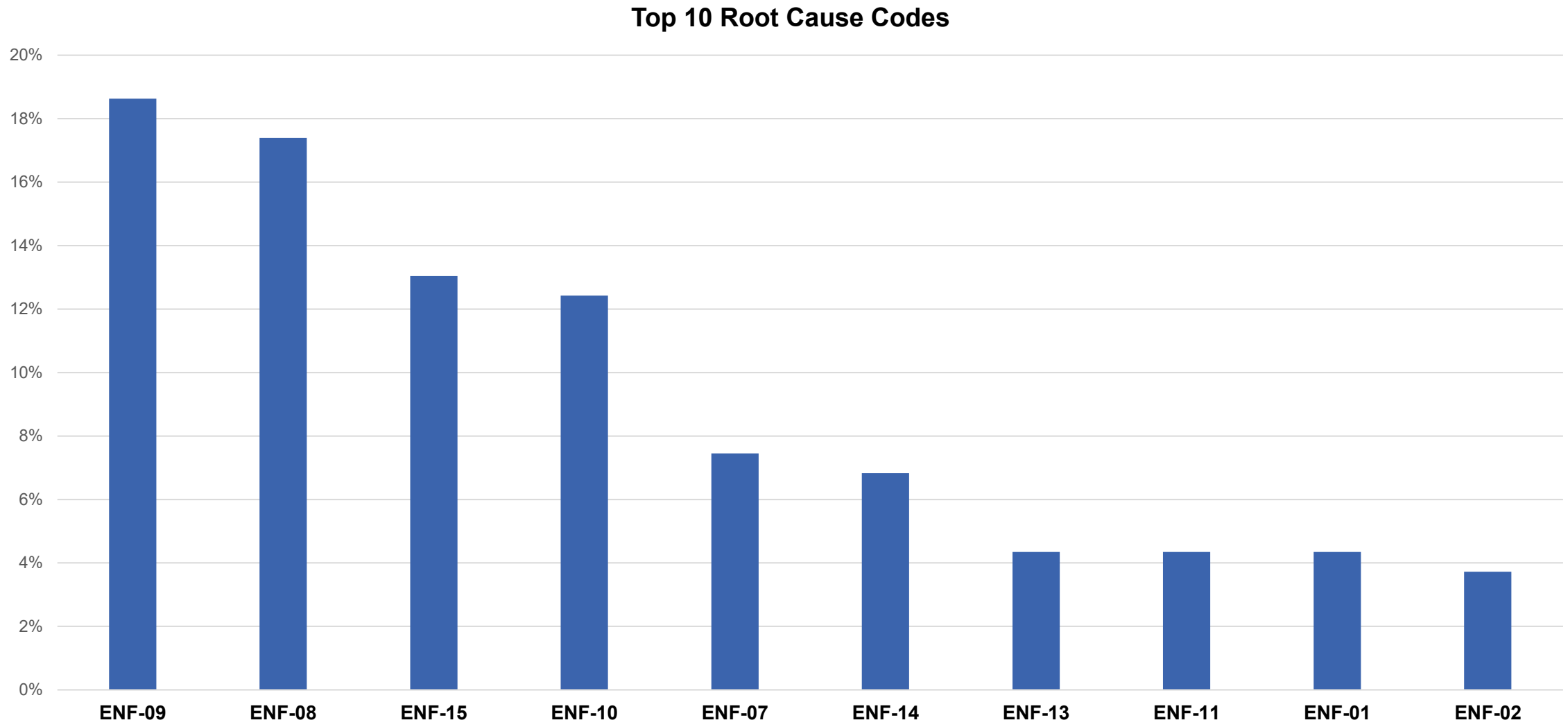




Root Cause Code Choices

ENF-01 Change Management	ENF-02 Communication/Coordination Internal	ENF-03 Communication/Coordination External	ENF-04 - Design - Ineffective Process Flow or System Design or Failure of System/Technology	ENF-05 - Lack of/Deficient Documented Evidence
ENF-06 - Lack of/Deficient Documented Evidence - Third Party/Vendor	ENF-07 - Lack of/Deficient Policy/Procedure - Company Wide	ENF-08 - Lack of/Deficient Policy/Procedure - Department/Business Level	ENF-09 - Ineffective Preventive Controls	ENF-10 - Ineffective Validation/Detective Controls
ENF-11 - Additional Training Needed	ENF-12 - Lack of/Deficient Training Materials and Content	ENF-13 - Lack of Understanding or Lack of Compliance Awareness	ENF-14 - Ineffective Organizational Methods	ENF-15 - Ineffective Resource or Project Planning
	ENF-16 - Exceptional Circumstances	ENF-17 - Human Performance Failure	ENF-18 - Other	

Texas RE's Most Used Root Cause Codes



NERC Guidance

"Lack of or ineffective internal controls designed to prevent noncompliance. Detective controls were implemented but there was an ineffective or lack of preventative control (e.g., checklist, secondary reviewer, workflow, or a backup or a redundant control)."

Examples of Ineffective Preventive Controls

MOD-026 R2

- Missed MOD-026 R2 deadline
- No compliance task reminders
- No compliance tracking software
- No automated reminders

CIP-003 R2

- Personnel did not complete the process for mitigating the introduction of malicious code when connecting a transient cyber asset to a low impact BES cyber system
- No checklist
- No reminder of the steps included in the procedure

CIP-010 R1

- Failed to maintain correct baseline
- Process made it possible for newly added assets to be overlooked
- Baseline needed to be manually compared to asset production status data
- No secondary review

Effective Mitigation for Ineffective Preventive Controls

MOD-026 R1

- Added MOD-026 to compliance tracking software
- Set up automated reminders
- Periodic meeting to review compliance obligations and tasks

CIP-003 R2

- Periodic training
- Labeled BCAs to remind personnel of procedures for Transient Cyber Assets (TCAs) and Removable Media

CIP-010 R1

- Automated review
- Added secondary review
- Added step that requires new assets to be added to baseline prior to being placed into production

NERC Guidance

"Ineffective business-level procedure/process – Standard Operating Procedure, Instructions, department-based. Needs new policy/procedure/process (did not exist) or was deficient."

Examples of Lack of or Deficient Procedure

VAR-002 R2

- Failed to provide timely notifications when Facility deviated from voltage schedule
- Had a procedure for voltage and reactive control settings and performance
- However, procedure did not include specific instructions relating to the notification timeframes for deviations

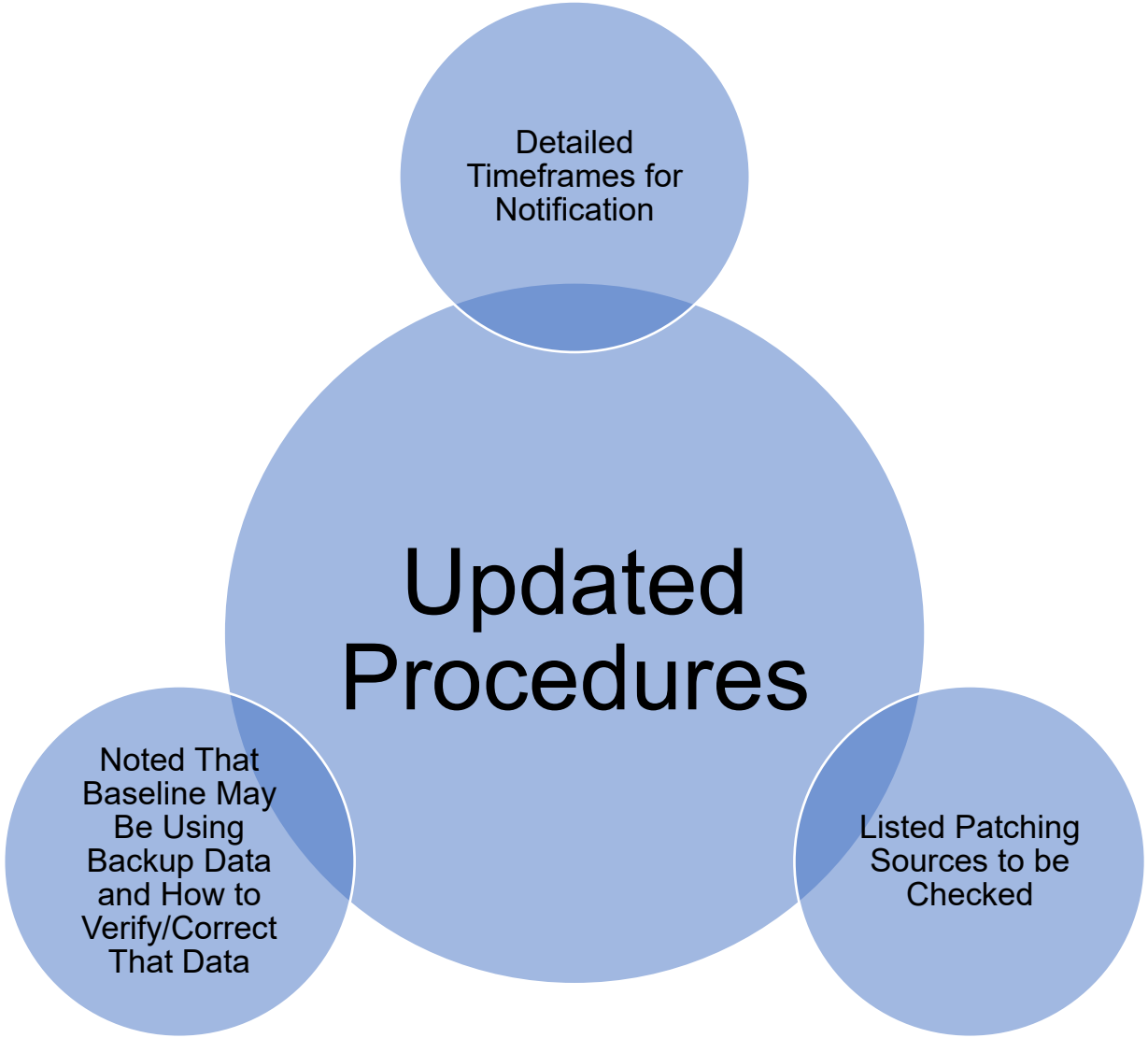
CIP-007 R2

- Failed to evaluate and apply security patches
- Aware of requirement to evaluate and apply security patches for the software at issue
- Personnel mistakenly believed it was evaluating all relevant security patches
- However, personnel failed to check at least one patching source

CIP-010 R1

- Failed to maintain accurate baseline
- Procedure/automated program allowed for device backups to be used if most recent information could not be pulled
- Program did not flag baselined items where backups were used

Effective Mitigation for Lack of or Deficient Procedure



ENF-15 Ineffective Resource or Project Planning

NERC Guidance:

"There was improper allocation of resources and/or improper scoping of project, including:

(i) insufficient supervisory resources to provide necessary supervision;

(ii) insufficient workforce or and equipment/tools to support identified compliance-related goals/objectives/tasks, including allotting sufficient time to complete tasks, train, or to implement quality procedures or controls;

(iii) work planning did not account for potential interruptions and/or special circumstances; and/or

(iv) work planning did not include coordination with all departments or business units involved in completing the tasks."

Examples of Ineffective Resource or Project Planning

MOD-026 R2

- Missed deadline
- Entity used compliance task tracking tools
- However, the tracking process did not ensure sufficient lead time to finalize report after testing
- The verification testing was performed before the required deadline
- The report was not completed until after the deadline to provide the verified model data to the TP

CIP-002 R2

- Failed to review R1 identifications at least once every 15 months and have CIP senior manager or delegate approve the identifications
- Compliance team had high rate of turnover
- Team members with little or no onboarding training
- Resulted in only one CIP team member for a significant period with no other compliance personnel to support the CIP tasks

Effective Mitigation for Ineffective Resource or Project Planning

MOD-026 R2

- Programed compliance tracking software to trigger a planning meeting
- Built out longer timeline in both tracking software and deadlines in procedure

CIP-002 R2

- Added additional team members
- Hired CIP consultant
  - Training
  - Verification/detective control

NERC Guidance

"Lack of or an ineffective validation/detective control. Preventative controls were implemented but there was an ineffective or lack of a validation/detective control after completion of the task."

Examples of Ineffective Validation/Detective Controls

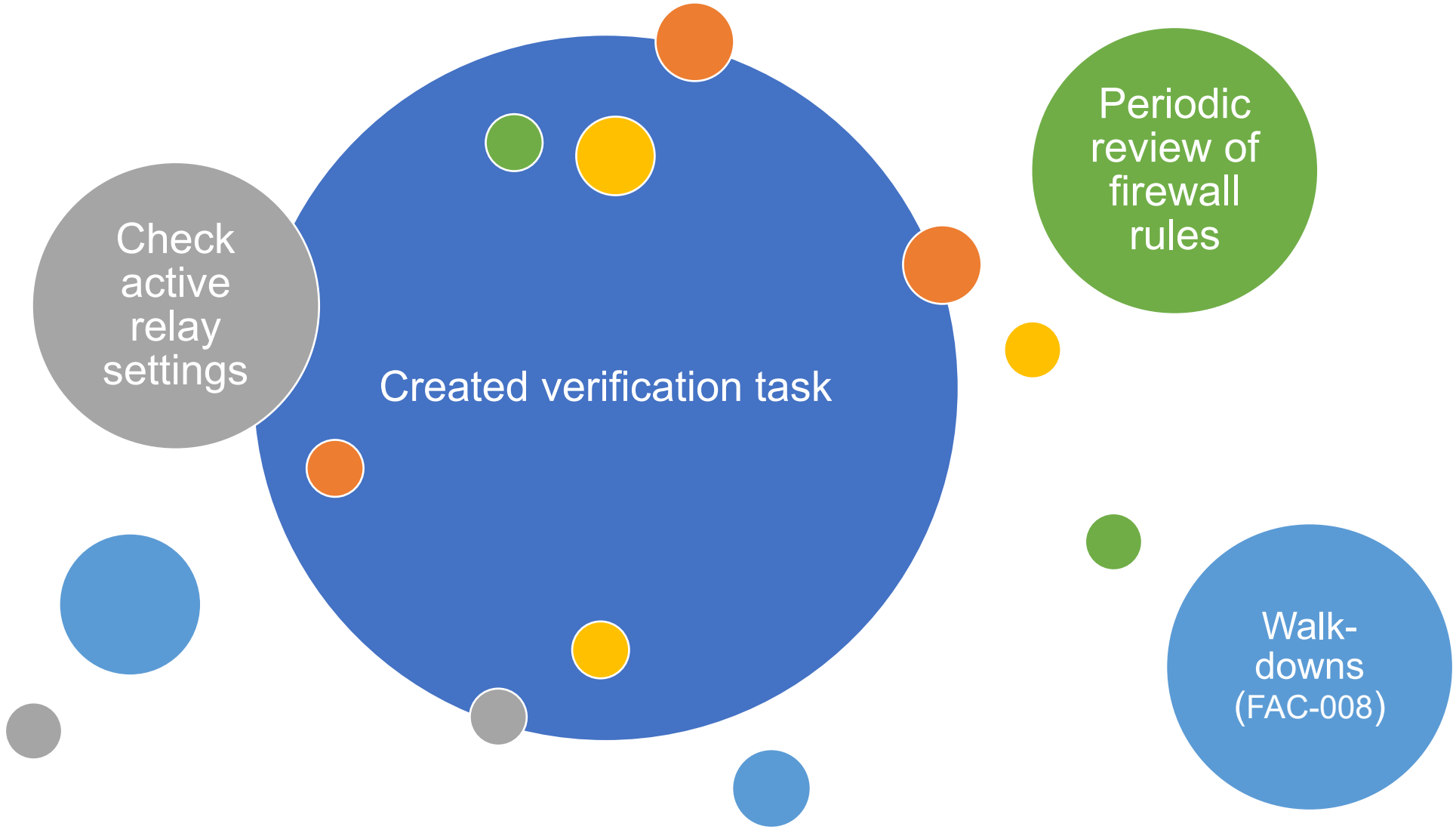
PRC-025 R1

- Entity had incorrect relay settings
- Entity determined that relay settings should be changed
- Work order created to implement
- Employee incorrectly marked the associated work orders as complete when the required relay setting changes had not been completed in the field

CIP-003 R2

- Failed to permit only necessary inbound and outbound electronic access
- Created a list of all firewall rules
- Never reviewed active firewall rules

Effective Mitigation for Ineffective Validation/Detective Controls



NERC Guidance

- "Ineffective management policy–high level, company wide issue. Needs new policy/procedure/process (did not exist) or was deficient."

Examples of Lack of Deficient Policy/Procedure Company Wide

PRC-005

- Failure to document testing
- Failure to get records when acquiring Facility so could not demonstrate compliance

VAR-002

- Failure to monitor voltage at correct location
- Energy Management System (EMS) was set to monitor at the wrong location

CIP-003 R2

- Failure to implement and review physical access controls
- Historically, entity allowed for each Facility to manage physical access at the site level without centralized standards or periodic oversight

Effective Mitigation for Lack of Deficient Policy/Procedure Company Wide

PRC-005

- New compliance software for better record management
- Training for corporate/legal/acquisitions team on NERC compliance requirements

VAR-002

- Corrected procedure to note the correct location at which to monitor voltage
- Corrected Energy Management System to monitor at the correct location

CIP-003 R2

- Established a centralized procedure:
  - Periodic training on the procedure
  - Assigned personnel to perform review

Questions?

TEXAS RE
Ensuring electric reliability for Texans

FERC and the Office of Electric Reliability

Priorities and Current Focus Areas

Deepak Ramlatchan,
Deputy Director, Office of Electric Reliability
Federal Energy Regulatory Commission

Texas RE Spring Workshop April 2026

Overview

- Intro and OER Key Focus Areas
- Challenges and Solution Opportunities
  - Evolving BPS
  - Extreme Weather
  - Cyber Security
  - Load Growth: Large Loads

Office of Electric Reliability

Responsible for protecting and improving the reliability of the Bulk Power System

Oversight of NERC Reliability Standards development and enforcement

Engineering support for other FERC filings and rules

Leadership Team

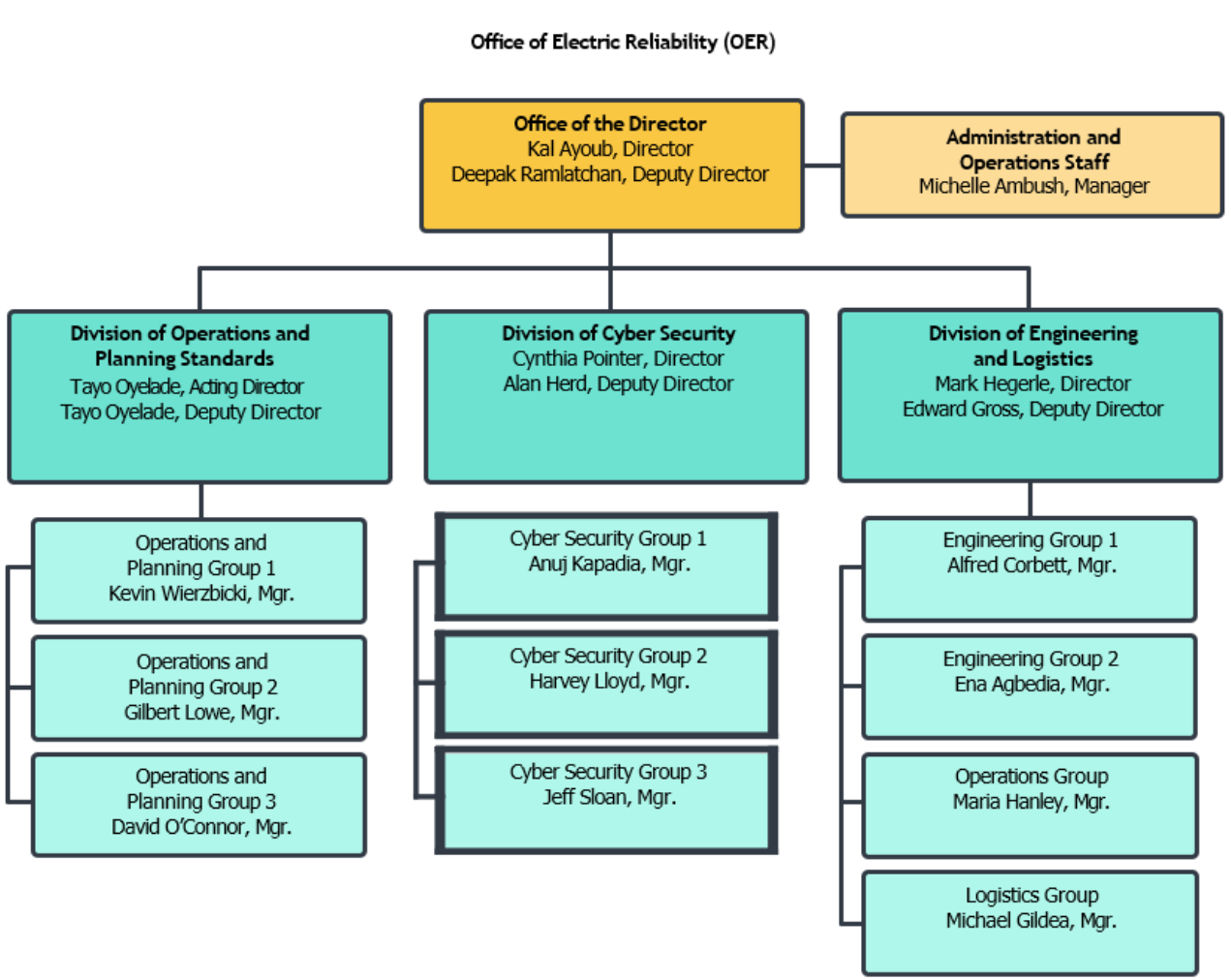
Kal Ayoub

Director

Deepak Ramlatchan

Dep. Director

All opinions are my own and do not reflect the views of the Commission or any individual Commissioner



Office of Electric Reliability

FEDERAL ENERGY REGULATORY COMMISSION

OER Functions and Responsibilities

- Review NERC-proposed penalties
- Provide technical support on tariff filings and rulemakings, focusing on system engineering and reliability impacts
  - Review over 500 FPA section 205/206 filings per year
- Analyze and issue reports on blackouts and major grid events with recommendations to mitigate recurrence
- Monitor the bulk-power system 24/7 to ensure the Commission is informed of major and evolving system events
- Perform seasonal energy market and electric reliability assessment

OER Priorities

Cyber and Physical Security

Supply Chain Compromise
Protections for Low Impact Assets
Physical Security

Resource Transition

Inverter Based Resources (IBR)
Resource/Energy Adequacy, Load Growth
Priority System Attributes (e.g., quick start, ramping)

Extreme Weather

Asset Hardening (e.g., generator freeze protection)
System Planning and Design

Office of Electric Reliability

OER is the Commission's lead reliability office under section 215 of the FPA. OER performs the oversight role for electric reliability, approving and enforcing reliability standards developed by NERC

- Advise on whether to approve, remand or require changes to reliability standards proposed by NERC
  - Monitor or process 10-30 new or revised reliability standards per year
- Oversee compliance with approved standards by users, owners, and operators of the Bulk-Power System (BPS)

NERC RISK Priorities Report, 2025

- Grid Transformation (including demand growth and large loads)
- Resilience to Extreme Events
- Critical Infrastructure Interdependencies
- Security
- Energy Policy

https://www.nerc.com/comm/RISC/Related%20Files%20DL/2025_RISC_ERO_Priorities_Report.pdf

Actions to Address Reliability Challenges

- Resource Transition
  - Order No. 901 – directives for new or revised reliability standards covering IBR data sharing, model validation, planning and operational studies, and performance requirements
  - IBR Registration Orders (RD22-4, RR24-2) – Issued June 2024, requires NERC to determine which IBRs are required to comply with relevant reliability standards by May 2026

Actions to Address Reliability Challenges

- Order 901
  - Three batches of standards due November 2024, 2025, and 2026
  - Second batch November 4, 2025: Data sharing, data and model validation for registered IBRs, unregistered IBRs, and IBR-DERs in the aggregate. Approved February 2026
  - Third batch November 2026: Planning and operational studies for registered IBRs, unregistered IBRs, and IBR-DERs in the aggregate.
  - Effective Date of New or Revised Standards: all new or modified IBR-related Reliability Standards must be effective and enforceable "well in advance of 2030."

Actions to Address Reliability Challenges

- Cybersecurity

- **Summer 2025**
  - **Internal Network Security Monitoring**: issued Order No. 907 (June 2025) and Order No. 907-A (August 2025) approving Reliability Standard CIP-015-1 that requires INSM inside an entity's electronic security perimeter and directing modifications to extend protections to access control systems outside of the electronic security perimeter (RM24-7).

- **March 2026:**
  - **Final Rule on Virtualization Reliability Standards, Docket No. RM24-8-000**
    - secure use of virtualization technologies
  - **Final Rule on CIP Reliability Standard CIP-003-11, Docket No. RM25-8-000**
    - baseline cybersecurity for low impact bulk electric system (BES) Cyber Systems

Actions to Address Reliability Challenges

- Extreme Weather
- TPL-008-1 (Transmission System Planning Performance Requirements for Extreme Temperature Events), filed in response to Order No. 896, approved February 2025
- EOP-012-3 (Extreme Cold Weather Preparedness and Operations), the revised generator winterization reliability standard, effective October 2025
  - Commission previously accepted and directed further revisions to address concerns pertaining to generator cold weather constraints and corrective action implementation

Large Loads

CHAIRMAN SWETT

Top Priority:

"Connect and power …as quickly and durably as possible…"

Large Loads

NERC

- Large Load Working Group
  - Whitepapers, Guidelines, Alerts
- Project 2026-02 "Computational Loads"
  - SAR comment period, SDT

FERC Proceedings

DOE ANOPR

Industry Whitepapers etc.

Large Load Issues

Resource Adequacy

Unexpected, simultaneous loss

Protection System Failures (co-located)

- Sudden appearance of load
- Sudden appearance of the generator

Oscillations

- Sub-synchronous
- Forced

Power Quality Issues

- Harmonics

Load Growth: Large Loads

- Forced Oscillations: the rapid, synchronized power demands of AI workloads (like GPU clusters) create fluctuating loads that can resonate with the power grid's natural frequencies, potentially causing widespread instability, equipment damage (like turbines), and blackouts. These rapid fluctuations (tens to hundreds of MW in milliseconds) act as "forcing signals," unlike steady industrial loads, demanding new grid management strategies for grid operators to maintain stability.
- Sub-synchronous Oscillations: These oscillations are usually caused by the load's own fast-acting control systems interacting with grid impedance or nearby generators.

Megapack

"Today's problem is dealing with extreme power jitter…

We are having some power fluctuation issues, when you do synchronized training it's like having an orchestra and it can go loud to quiet very quickly, at the sub-second level. The electrical system freak out about that – with 10-20 MW shifts several times per second."

- Elon Musk
  August 2024 in conversation with Lex Fridman about xAI Memphis data center

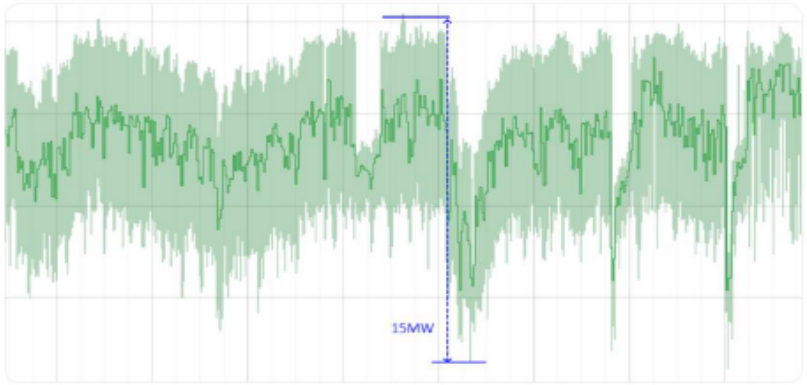


Fig. 1. Large power fluctuations observed on cluster level with large-scale synchronized ML workloads

"In our latest batch-synchronous ML workloads running on dedicated ML clusters, we observed power fluctuations in the tens of megawatts"

- Google Technical Lead Manager and VP, Engineering
  February 2025, Blog Post

Large Load Issues: Power Swings

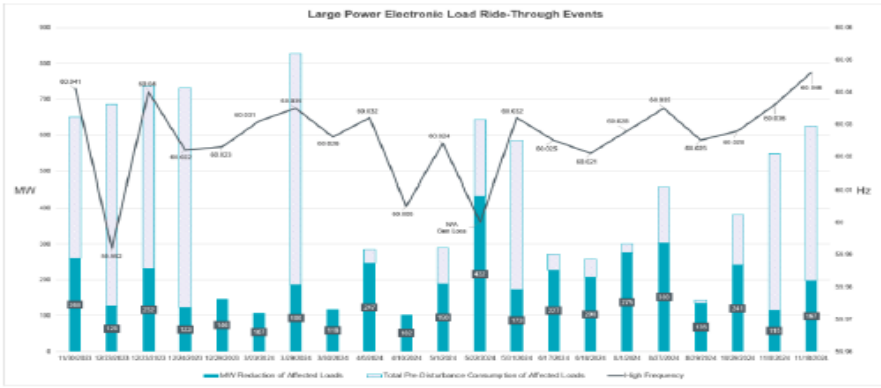
Megapack

Challenge: Low Voltage Ride Through (LVRT) of data centers

Dominion: 1.5 GWs across 60 data centers

July 2024 – due to reclosing attempts on faulted 230 kV system

ERCOT: Many events of 100s of MWs



Grid Operator Perspective

- Challenging to manage load drops at this scale
- Over frequency and voltage concerns

Data Center Perspective

- UPS systems working as intended
- Protecting our expensive and reliability critical equipment from utility system faults

Large Load Issues: sudden loss

Questions

- FERC and OER Priorities and Focus Areas

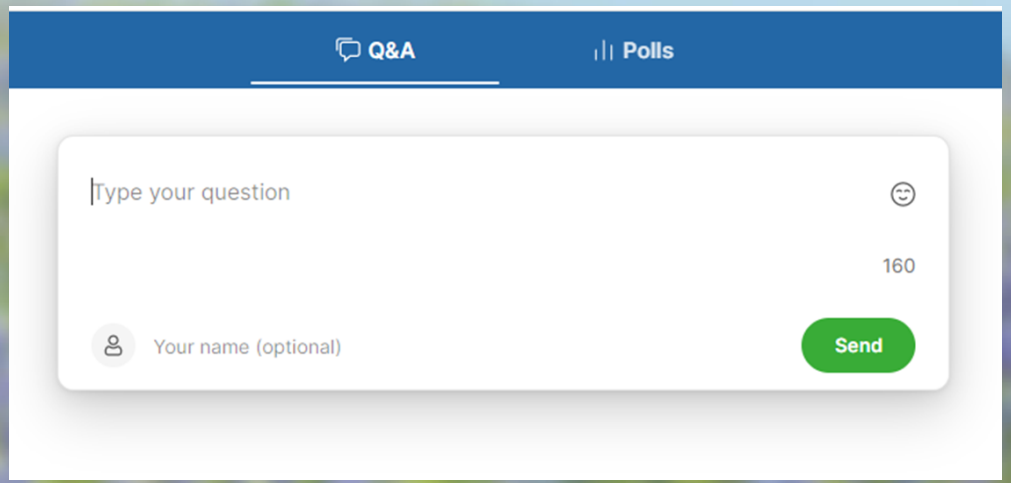
Texas RE Spring Standards, Security, & Reliability Workshop

AGENDA

- Aggregation of Control
- CIP-003-9 Low Impact BES Remote Connectivity
- Frequency and Voltage Protection Settings for Generation Resources
- Common Root Cause Codes
- FERC Update
- **Large Loads Interconnection in ERCOT**
- NERC CIP Drip
- Supply Chain Resilience in a World of Geopolitical Cyber Risk
- AI-Augmented Embedded Security Assessment for BES Resilience

Return at: 12:55 pm

To submit questions during the workshop, please visit **slido.com** and enter today's participant code: **TXRE**



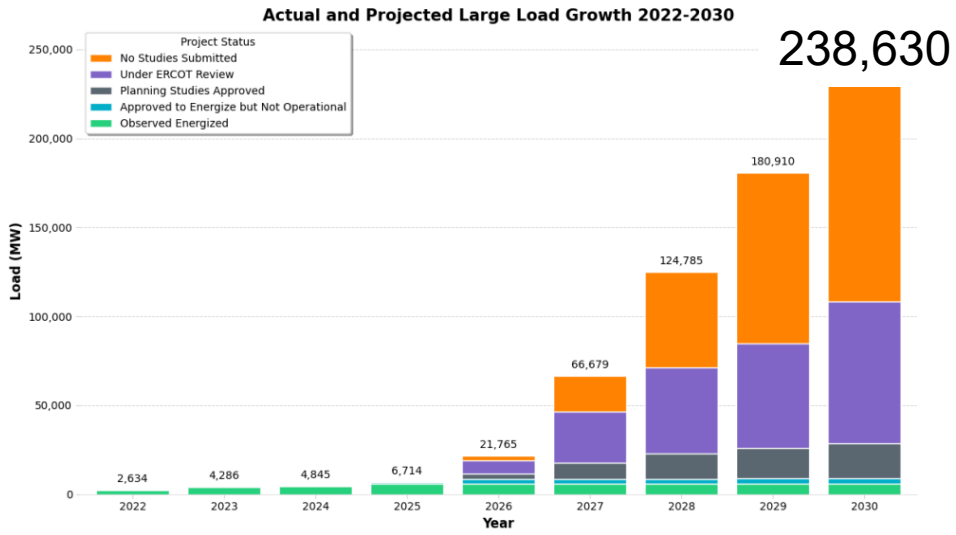
Large Load Interconnection in ERCOT

Harsh Naik

04/01/2026

ERCOT Interconnection Queue

Current Large Load Interconnection Queue



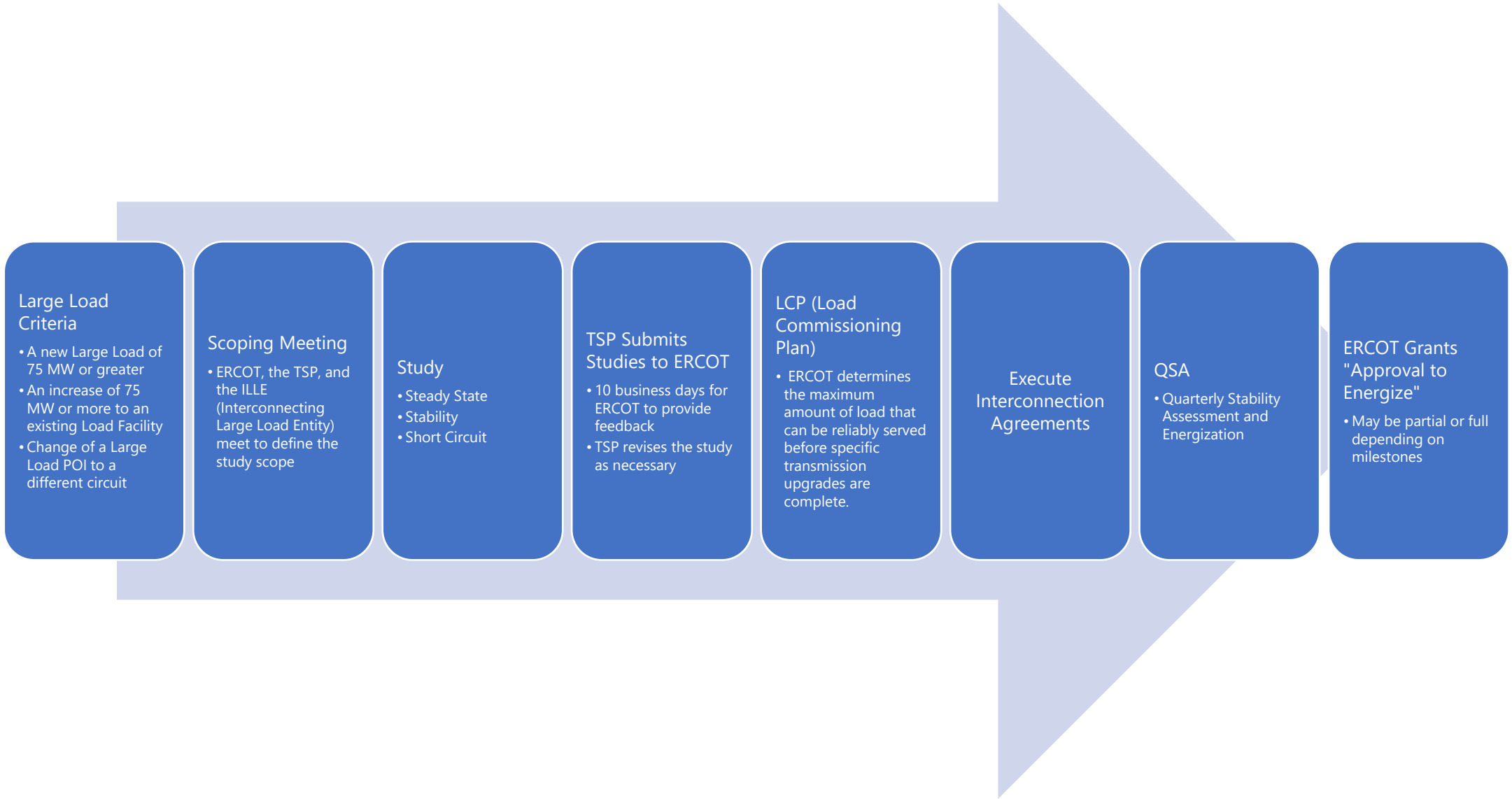
Project Status	2022	2023	2024	2025	2026	2027	2028	2029	2030
No Studies Submitted	0	0	0	0	2,704	20,341	53,546	95,879	130,303
Under ERCOT Review	0	0	0	0	7,353	28,454	48,171	58,831	79,825
Planning Studies Approved	0	0	0	0	3,181	9,164	14,348	17,180	19,482
Approved to Energize but Not Operational	0	0	0	946	2,759	2,952	2,952	3,252	3,252
Observed Energized	2,634	4,286	4,845	5,768	5,768	5,768	5,768	5,768	5,768
Total (MW)	**2,634**	**4,286**	**4,845**	**6,714**	**21,765**	**66,679**	**124,785**	**180,910**	**238,630**

- **Observed Energized –** Projects that have received Approval to Energize from ERCOT Operations and are fully operational. Represented by all time non-simultaneous peak load consumption.
- **Approved to Energize but Not Operational –** Projects that have received Approval to Energize from ERCOT Operations but are not observed to be operational.
- **Planning Studies Approved –** Projects that have received ERCOT approval of required interconnection studies. Any MWs that were not approved are reclassified as No Studies Submitted.
- **Under ERCOT Review –** Projects that have studies under review by ERCOT.
- **No Studies Submitted –** Projects that are tracked by ERCOT but that have not yet provided sufficient information for ERCOT to begin review. Additionally, MWs that were not approved by ERCOT after review of planning studies are included in this category until a path to interconnect these MWs is identified, or the customer cancels the interconnection request.

ERCOT has recently received 137 new LLI submissions. Preliminary review indicates these total approximately 140,000 MW of new Large Load by 2036. ERCOT is still processing these submissions, and they will be reflected in future reports.

Source: ERCOT Update at March 2026 LLWG

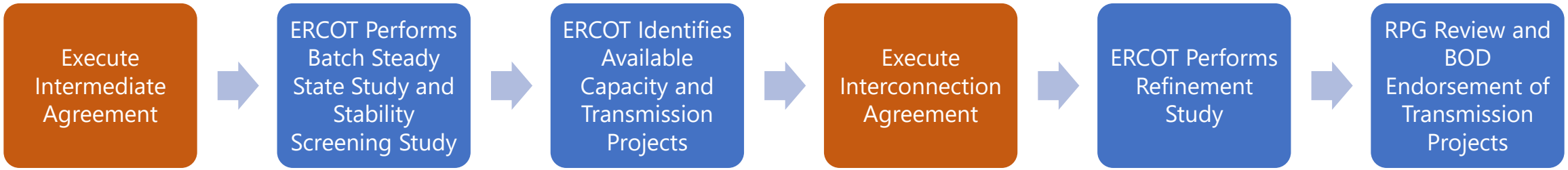
Current Large Load Interconnection Process



Current Large Load Interconnection Challenges

- The Volume Storm – The process was built to handle a smaller stream of requests. Instead, it faced a 277% increase in the queue, exploding from **63 GW in late 2024 to over 238 GW in 2026.**
- Structural Limitations of the Current LLIS Process – The existing individual-study approach strains both TSPs and ERCOT, resulting in:
  - Multiple load studies can be moving in parallel resulting in repeated restudies for overlapping projects
  - Inconsistent assumptions across TSPs
  - Increased coordination challenges
  - A growing study backlog
  - These issues create long delays and uncertainty for all parties.
- Need for a System-Wide, Coordinated Approach – Large Loads often affect multiple transmission areas

Proposed Batch Study



Interconnection Agreement Requirements

Intermediate Agreement (Pre-Study Requirements)

- Demonstrates project viability through: Site control (lease, deed, or option).
  - Disclosure of substantially similar interconnection requests.
  - Submission of site-related studies, permitting plans, and energization schedule (quarter/year).
  - Disclosure of backup generation, power supply plans, and controllable load capability.
- Financial Obligations:
  - Study Fee: ≥$100k (75–250 MW) or ≥$300k (≥250 MW).
  - Financial Security: $50,000 per MW of requested load.
  - Optional security for long-lead equipment (≥6-month lead time).

Interconnection Agreement (Post-Study Requirements)

- Executed within 30 days after ERCOT completes the interconnection study.
- Confirms readiness to proceed to construction:
  - Updated site control, permitting, engineering, and energization schedule (month/year).
  - Continued disclosure of similar interconnection requests and backup generation plans.
- Financial Obligations:
  - Interconnection Fee: $50,000 per MW (non-refundable).
  - Financial Security for Significant Equipment/Services (mandatory before procurement).
  - CIAC: Customer pays 100% of direct interconnection costs (non-refundable).
  - Financial Security for System Upgrades (cash, guaranty, or LOC).

ERCOT Batch Study Implementation Roadmap

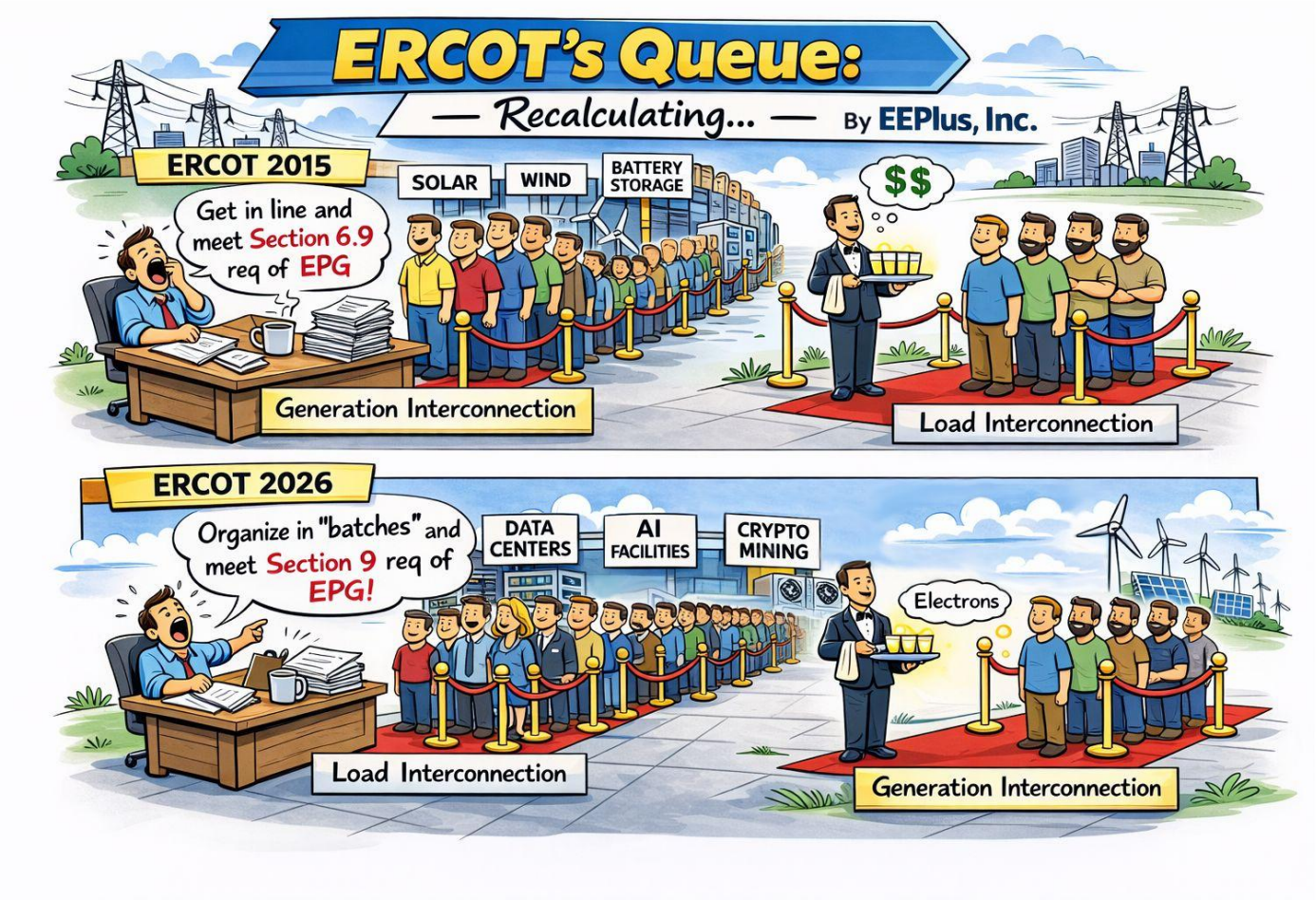
Moving from Individual to System-Wide Study

- Strategic Transition: Establishes "Batch Zero" to shift from the legacy individual study-based approach (LLIS) to a system-wide "Batch Study" process.
- Backlog Resolution: Designed to manage the "unprecedented volume" of Large Load requests that caused coordination issues, repeated restudies, and backlogs.
- Resource Allocation: Focuses on allocating available transmission capacity and planning future capacity through an actionable transmission plan while maintaining grid reliability.

The Future Landscape: Post-Batch Zero

- Permanent Batch Cycles: ERCOT plans to submit a future revision request to establish an ongoing, permanent batch study process.
- Stricter Eligibility: Loads failing to meet Batch Zero criteria will be ineligible for "Initial Energization" until a future study process is established.
- Regulatory Alignment: Implementation of Public Utility Commission (PUCT) Project No. 58481 standards to minimize stranded costs and support Texas business development.

Questions?


ERCOT's Queue:
— Recalculating... —
By EEPlus, Inc.
ERCOT 2015
Get in line and meet Section 6.9 req of EPG
SOLAR
WIND
BATTERY STORAGE
$$
Generation Interconnection
Load Interconnection
ERCOT 2026
Organize in "batches" and meet Section 9 req of EPG!
DATA CENTERS
AI FACILITIES
CRYPTO MINING
Electrons
Load Interconnection
Generation Interconnection

NOVASYNC

Brent Castagnetto, CISSP

Co-Founder & VP Business Development

Nick Santora, CISSP, CISA

VP of Growth

NOVASYNC

Agenda

* Welcome & introductions
* Intro to the CIP Drip
* Why CIP Drips matter
* Strategies to identify CIP Drips
* People, Process, & Technology Drips
* Closing Q&A

NOVASYNC

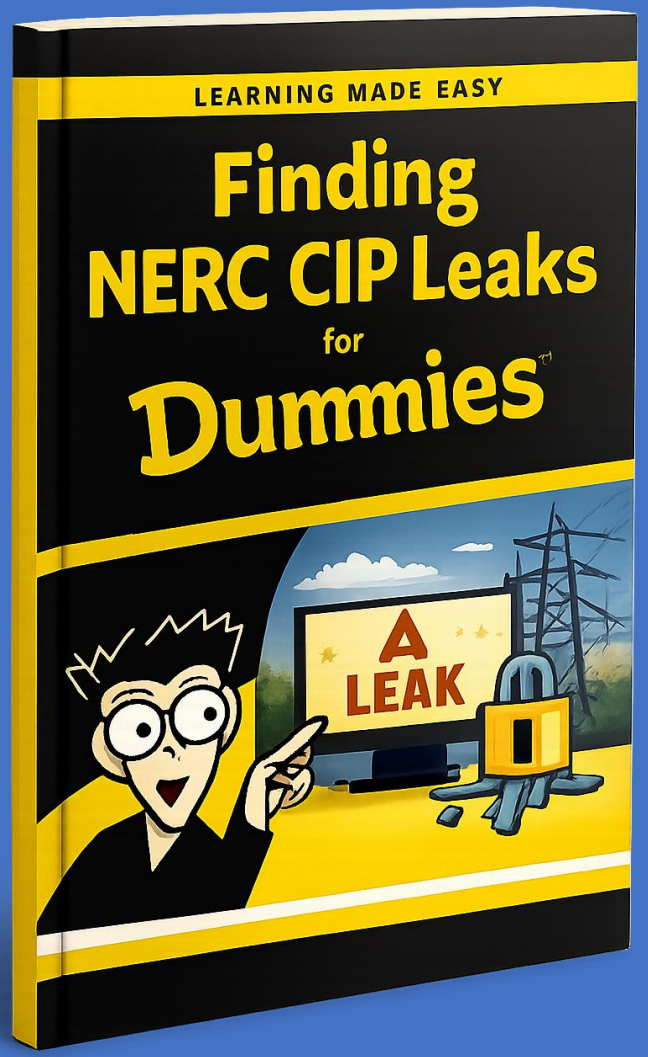
CIP DRIP

NOVASYNC

Why it matters?

NOVASYNC

How to identify CIP drips?



NOVASYNC


People

NERC CIP Training and Awareness

NOVASYNC

Reply | Reply All | Forward

From: **CIP Manager** <cip.manager@utility.com>

To: CIP Staff

Subject: Q1 NERC CIP Quarterly Awareness (checking the box!)

Hello,

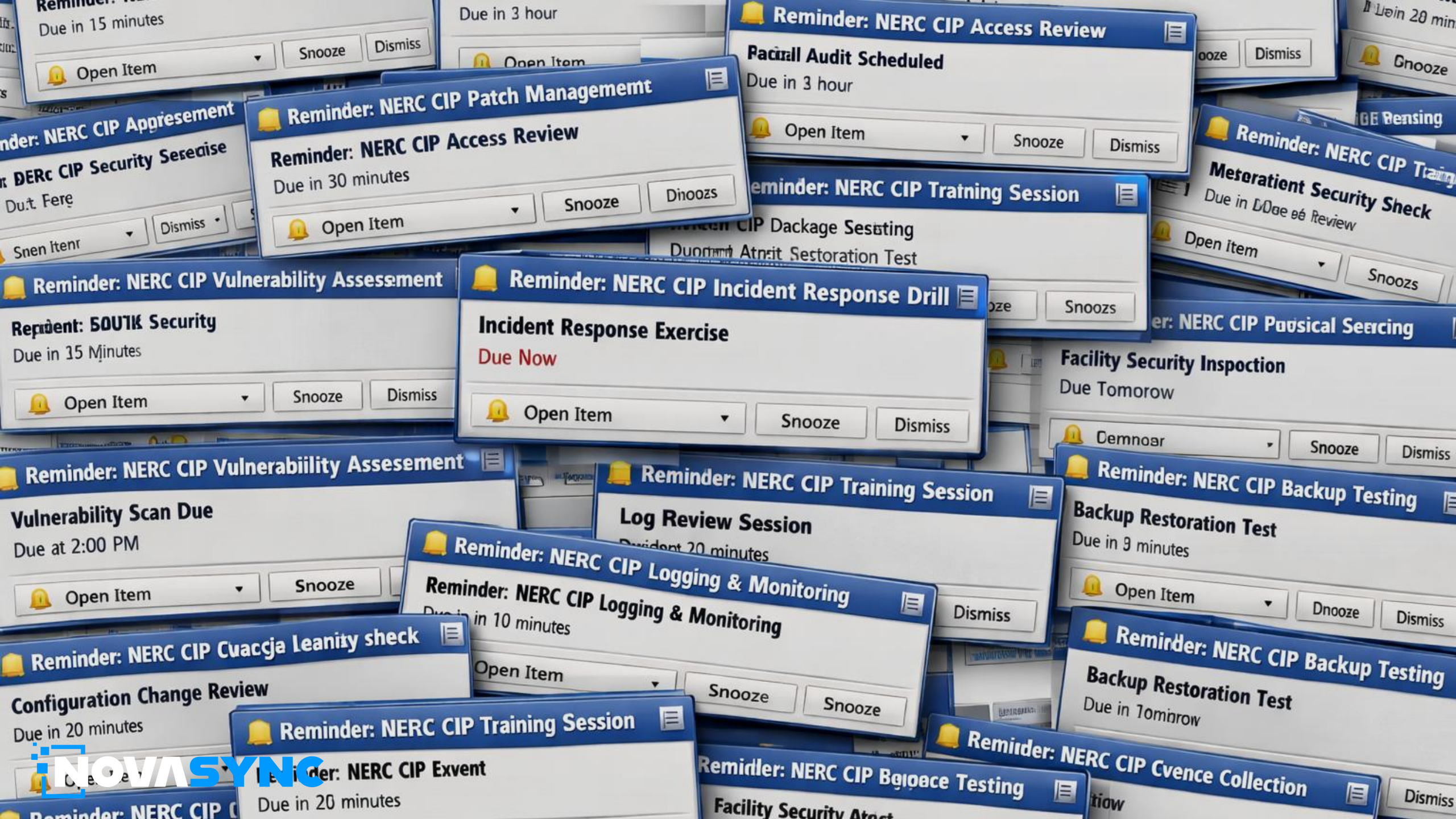
Please don't get hacked this quarter.

Thank you for participating in our NERC CIP awareness program.

Best regards,
CIP Manager

NOVASYNC

NOVASYNC


Reminder: NERC CIP Access Review
Due in 3 hour
Open Item
Snooze
Dismiss
Reminder: NERC CIP Patch Management
Reminder: NERC CIP Access Review
Due in 30 minutes
Open Item
Snooze
Reminder: NERC CIP Vulnerability Assessment
Due in 15 Minutes
Open Item
Snooze
Dismiss
Reminder: NERC CIP Incident Response Drill
Incident Response Exercise
Due Now
Open Item
Snooze
Dismiss
Reminder: NERC CIP Training Session
Log Review Session
Reminder: NERC CIP Logging & Monitoring
Reminder: NERC CIP Logging & Monitoring
Due in 10 minutes
Open Item
Snooze
Reminder: NERC CIP Backup Testing
Backup Restoration Test
Due in Tomorrow
Reminder: NERC CIP Training Session
Due in 20 minutes
Facility Security Inspection
Due Tomorow
Snooze
Dismiss

Review Your Buying Process

NOVASYNC

Laptop Farmville USA!

(Let’s prevent this)

NOVASYNC

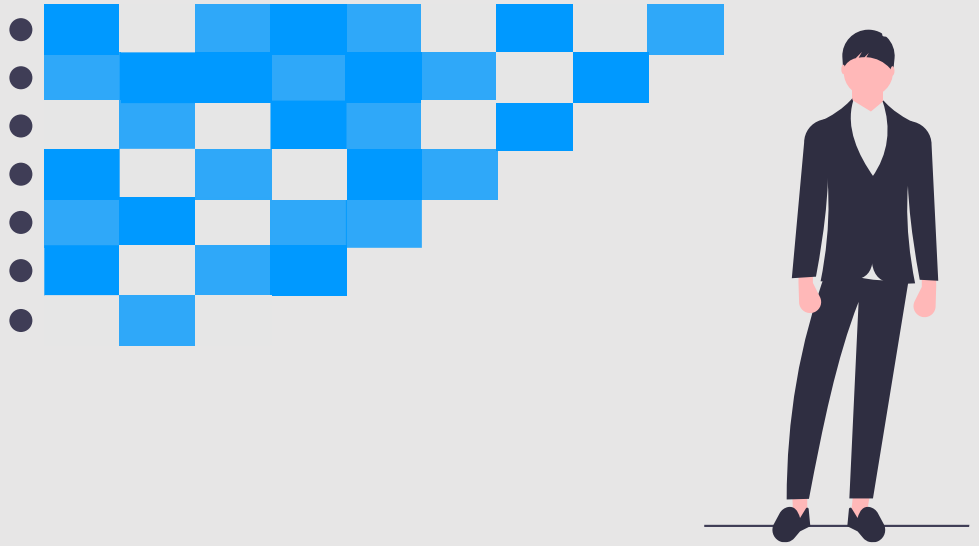
Technology

NOVASYNC

Technology Choices

NOVASYNC

Creating Internal Champions



NOVASYNC

Patch Management
Change Management
Access Management
Asset management

NOVASYNC

Connecting systems to compliance outcomes

NOVASYNC

www.NovaSync.io

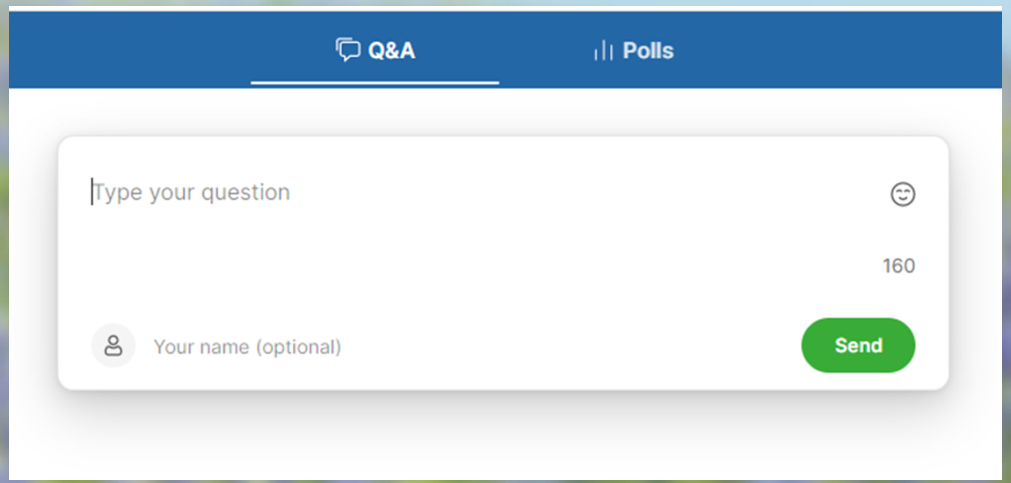
Texas RE Spring Standards, Security, & Reliability Workshop

AGENDA

- Aggregation of Control
- CIP-003-9 Low Impact BES Remote Connectivity
- Frequency and Voltage Protection Settings for Generation Resources
- Common Root Cause Codes
- FERC Update
- Large Loads Interconnection in ERCOT
- NERC CIP Drip
- **Supply Chain Resilience in a World of Geopolitical Cyber Risk**
- AI-Augmented Embedded Security Assessment for BES Resilience

Return at: 2:05 pm

To submit questions during the workshop, please visit **slido.com** and enter today's participant code: **TXRE**



Supply Chain Resilience in a World of Geopolitical and Cyber Risk

Texas RE

Austin, TX

April 01, 2026

Resilience in a World of Geopolitical and Cyber Risk

Booz Allen

Booz Allen Overview

U.S. Defense and Intelligence

Civil Government Agencies

Law Enforcement

Global Commercial:

- ***Energy & Utilities***
- ***Financial Services***
- ***Health and Life Sciences***
- ***Manufacturing***
- ***Software and High Tech***
- ***Transportation***

Leading with Tech + Tradecraft for Security Advantage

Footprint

23
Major Business Centers

17
Manufacturing / R&D Centers

>35,000 Employees

22,00
technologists

8,000
cyber professionals

6,000
software engineers

2,500
AI practitioners

Key Facts

$9.3B
revenue in FY23

1914
Booz Allen founded

- **Leading AI provider** to the federal government
- **Invested ~$3B** over last decade through R&D, Ventures, M&A, and co-creation
- Scaled businesses in **Defense Tech, Space, and Digital Transformation** and a leading position in Quantum

12,000+ Cyber Certifications

70% Hold Security Clearances

2 NSA Accreditations

4 CREST Certifications

1,000+ Annual IR Engagements

Global Commercial

Where Innovation Meets Impact: **Commercial Solutions**

Advanced Cyber Defense & Resilience

- Cyber Resilience
- Cyber Transformation
- Post-Quantum Cryptography (PQC)

Artificial Intelligence (AI)

- AI Governance
- AI Red Teaming
- AI Security
- Cyber AI

Operational Technology & Enterprise Security

- Cloud Security
- Enterprise Security Architecture
- Operational Technology (OT)
- Product Security
- Smart Manufacturing

Governance, Risk, Compliance (GRC)

- Compliance & Certification Readiness
- Cyber Risk & Analytics
- Cyber Strategy

Incident Response & Threat Management

- Forensic Investigations
- NextGen Threat Intelligence
- Ransomware Negotiations
- Rapid Response & Recovery
- Security Testing
- Wargames & Exercises

Strategic Security Solution: **Leveraging Advanced Technology**

We integrate best-of-breed security technologies with our advanced technology solution expertise to help you navigate the evolving threat landscape.

red canary, ARMIS, Microsoft, HIDDENLAYER, CYVATAR.AI, splunk>, ThreatModeler, BLACKDUCK, SAFE, NETRISE, SentinelOne, halcyon, aws

Resilience in a World of Geopolitical and Cyber Risk

Local operations, global dependencies

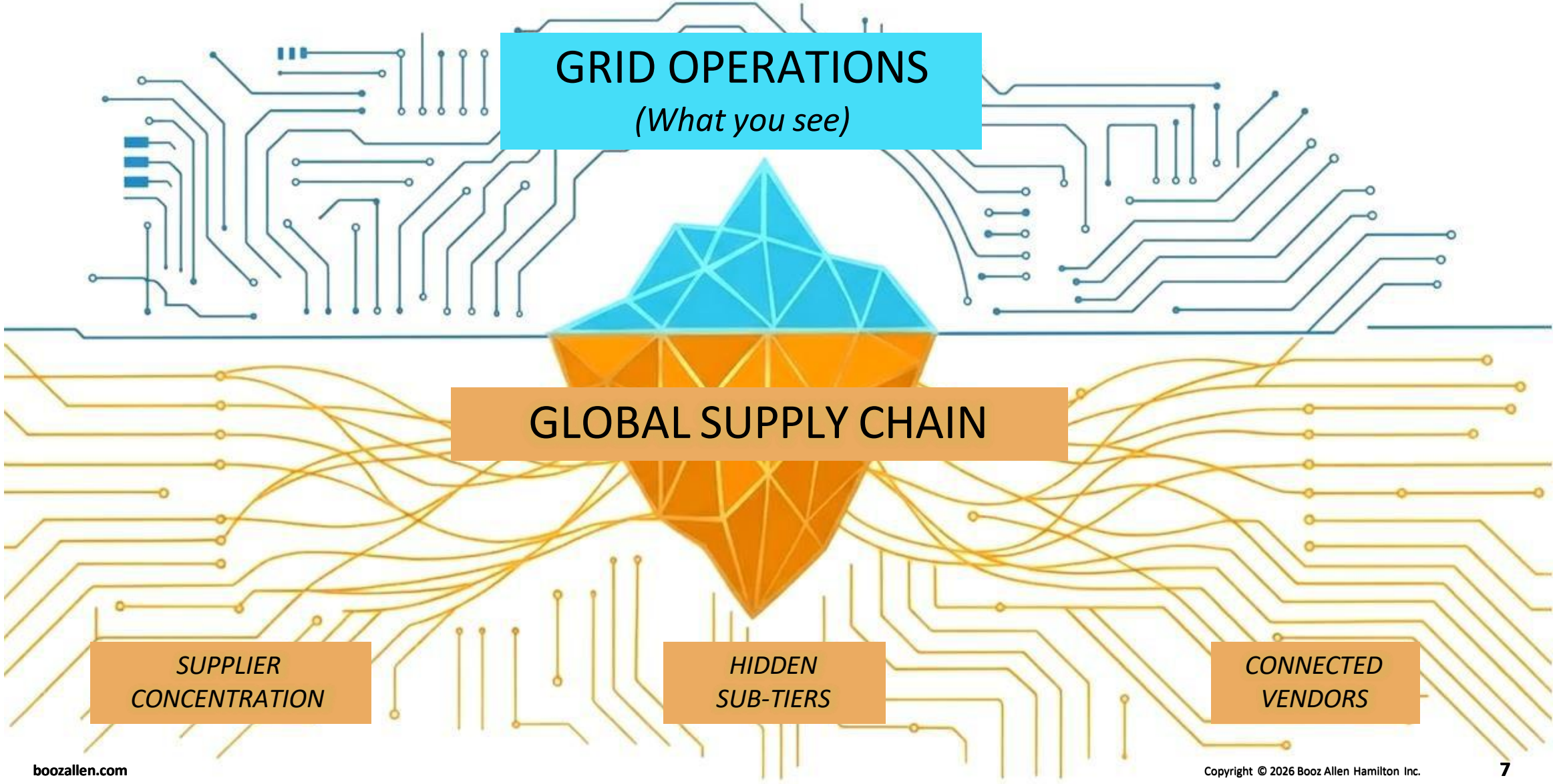
Texas reliability depends on outside equipment, software, and support

The three dependencies behind reliability

The essential pillars supporting day-to-day operations

Pressure starts below the waterline

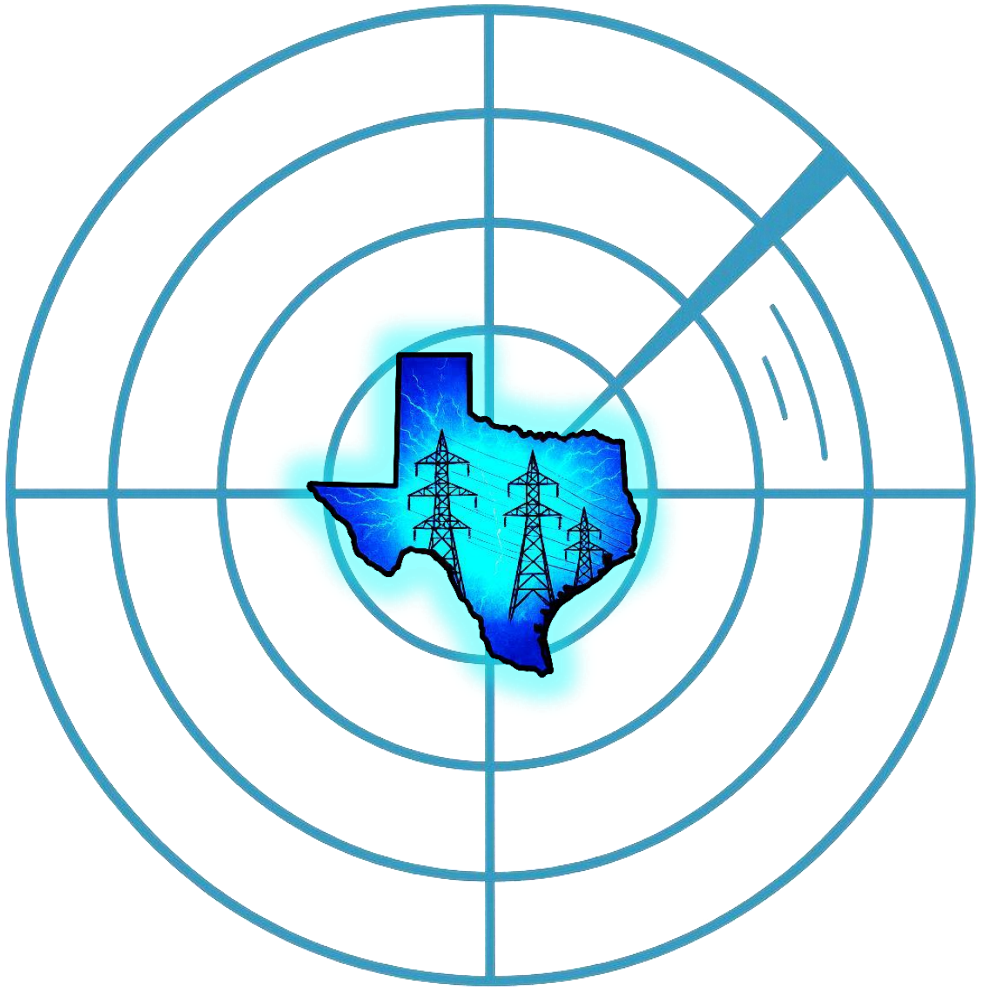
Global challenges create local operating risk



Where reliability is exposed

Four areas reliability leaders need visibility

- ☑ Critical assets
- ☑ Vendor concentration
- ☑ Supply-chain visibility
- ☑ First points of impact



Energy Infrastructure Supply Chains: A High-Impact Attack Path

The Energy Sector Supply Chain is a large and highly interconnected ecosystem of operational technology (OT) vendors and suppliers across the globe providing:

- Industrial Control Systems (ICS) and SCADA platforms
- Substation and T&D automation equipment
- Generation plant monitoring and turbine control systems
- Grid analytics, forecasting, and energy market platforms
- Field service contractors with remote operational access

This ecosystem creates **multiple indirect pathways into critical operational environments.**

KEY THREAT SCENARIOS

Compromise of OT / Grid Management Software
Attackers insert malicious code or exploit vulnerabilities in widely used versions of grid management software.

Vendor Remote-Access Exploitation
Third-party engineers and maintenance providers maintain privileged access into plant and transmission infrastructure.

Hardware and Firmware Supply Chain Risks
Grid equipment sourced globally introduces risk of compromised firmware or vulnerable embedded systems.

Software Dependency Attacks
Energy market platforms and monitoring systems rely heavily on open-source components that can introduce vulnerabilities at scale.

Potential Impacts to Utilities and Energy Service Providers

Regulatory exposure under NERC CIP and evolving federal requirements

Disruption to energy generation or transmission operations

Cascading grid instability or regional outages

Safety and environmental risks to personnel and infrastructure

Potentially material financial loss / exposure

Building Supply Chain Resilience for Grid Reliability

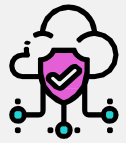
To meet regulatory requirements and ensure long-term grid security & availability, energy providers and utilities must work collaboratively to mitigate supply chain risks as a core element of operational resilience.

Identify & Prioritize Critical Supplier Relationships

- Focus on vendors supporting generation, transmission, and distribution
- Identify suppliers tied to EMS, SCADA, and substation control systems
- Prioritize vendors and partners with remote access

Harden Software & Firmware Supply Chain Assurance

- Require vendors to provide SBOMs for critical platforms & power electronics
- Enforce vulnerability disclosure and patch management processes
- Ensure firmware updates are secure for OT equipment



Map Key Dependencies Before a Crisis Event

- Understand supply chain impact across critical grid assets
- Identify single points of failure across suppliers and key components
- Identify & validate critical fourth-party partner dependencies

Diversify Mission-Critical Component Suppliers

- Build redundancy across mission-critical supply chains
- Reduce reliance on single-source suppliers for critical components
- Pre-qualify alternates and maintain inventory for high-risk components

Foundational Cybersecurity Priorities for Energy Sector Resilience

Strong cybersecurity practices are critical to ensuring reliability, redundancy, and resilience.

01 IDENTITY & ACCESS MANAGEMENT

Secure Remote Access for Critical Systems & Secured Environments

02 NETWORK SEGMENTATION

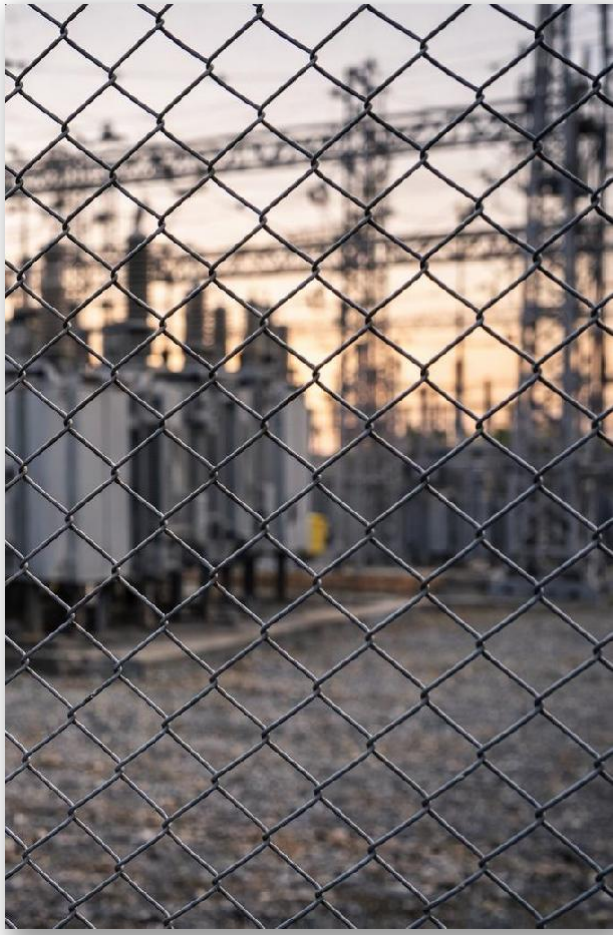
Segment IT and OT Environments to Prevent Lateral Movement

03 ASSET MANAGEMENT / CMDB

Establish Full Visibility into Critical IT & OT Technology Assets

04 ATTACK SURFACE MANAGEMENT

Proactively Manage Vulnerabilities in Critical OT Environments



KEY TAKEAWAYS

Nation-state sponsored threat **actors** are actively **pre-positioning in** U.S. critical infrastructure.

Cyber **attacks** impacting the **availability** of energy control systems are **no longer theoretical.**

The energy sector in Texas is a **high-priority target** for nation-state and ransomware actors.

Resilience in a World of Geopolitical and Cyber Risk

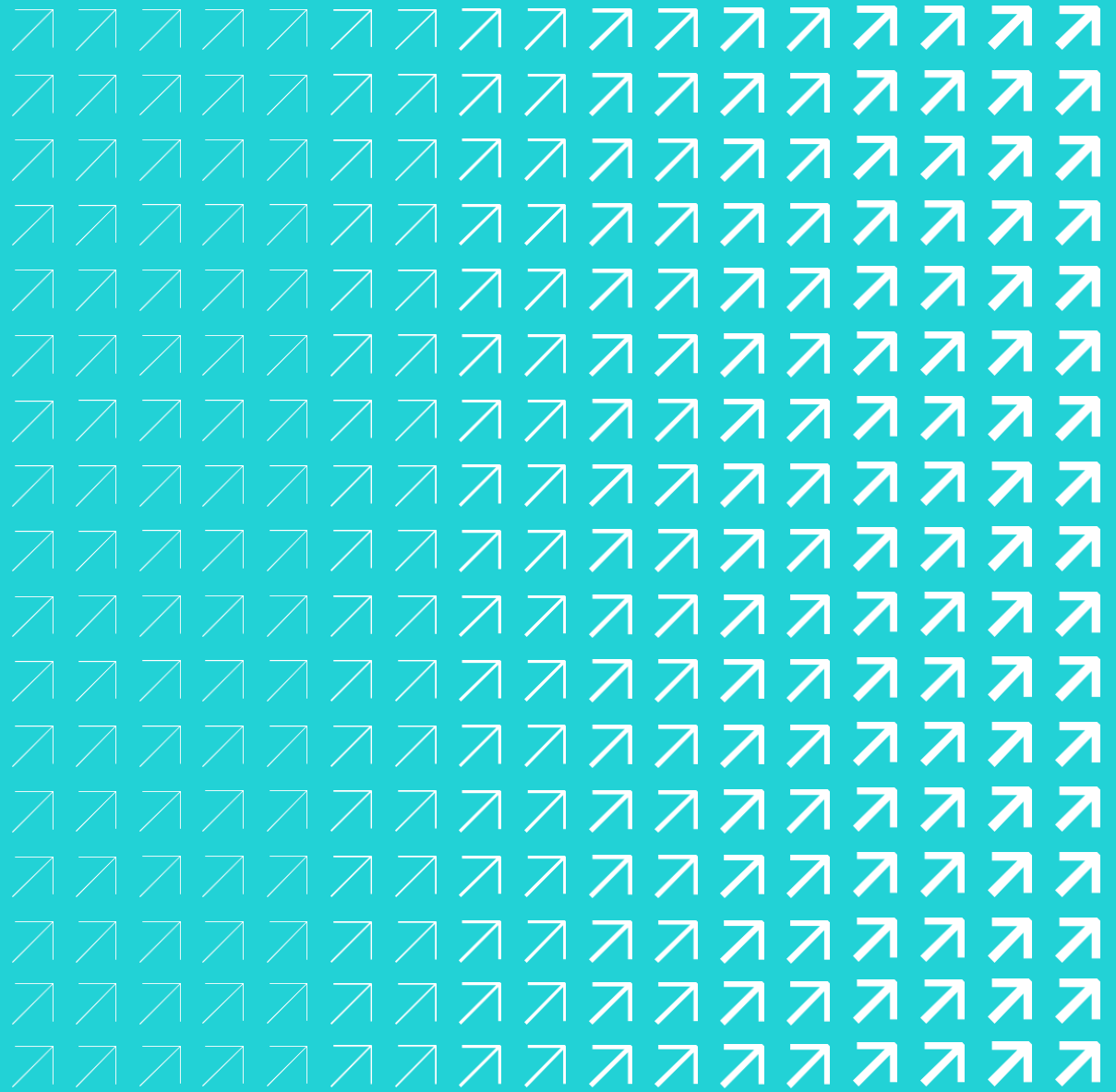
01 BOOZ ALLEN - GENERAL OVERVIEW

02 GEOPOLITICS AND SUPPLY CHAIN RISK

03 QUESTIONS / OPEN DISCUSSION

04 GridEx

Questions/Discussion



Resilience in a World of Geopolitical and Cyber Risk

01 BOOZ ALLEN - GENERAL OVERVIEW

02 GEOPOLITICS AND SUPPLY CHAIN RISK

03 QUESTIONS / OPEN DISCUSSION

04 GridEx

GridEx Planning and Execution Support

For organizations considering GridEx for the first time—or looking to get more from the next exercise, we help plan, design, delivery, and document your exercise, so you get the most value possible.

We help you turn your GridEx participation into a right-sized, expertly structured exercise that exposes critical gaps, strengthens coordination, and creates the conditions for performance improvement where it matters most.

SUPPORT OPTIONS ALIGNED TO THE RIGHT LEVEL OF CHALLENGE

GridEx Tabletop | Structured, decision-forcing discussion

Best when: Roles, escalation, communications, and cross-functional coordination need clarity and conceptual evaluation.

GridEx-in-a-Box | Focused functional validation with right-sized rigor

Best when: Your goal is to validate plans, playbooks and capabilities, but need a narrower scope and planning lift than a full operations-based exercise.

Standard GridEx | Broad operations-based testing across teams

Best when: Plans are established, participants know their roles, and your teams are ready for integrated multi-team play to fully test your organization's ability to respond.

FLEXIBLE SUPPORT OPTIONS

Targeted support • Co-delivery • Full-service

- **Targeted Support**: We fill critical gaps in planning, design, facilitation, evaluation, or after-action analysis to strengthen the value of your GridEx participation where it matters most.
- **Co-Delivery**: We partner with your internal team to shape and execute a right-sized GridEx experience that builds capability while creating stronger learning and outcomes.
- **Full-Service**: End-to-end support from participation strategy through after-action reporting so your organization can focus on the exercise while we drive a structured, improvement-oriented experience.

SUPPORT CAN FLEX ACROSS THE LIFECYCLE

From fit assessment and design through facilitation, evaluation, and after-action reporting.

Independent support services for organizations participating in GridEx; not affiliated with NERC or the E-ISAC.

Booz Allen Contacts:

Eric Reddel

Reddel_Eric@bah.com

Nate Beach-Westmoreland

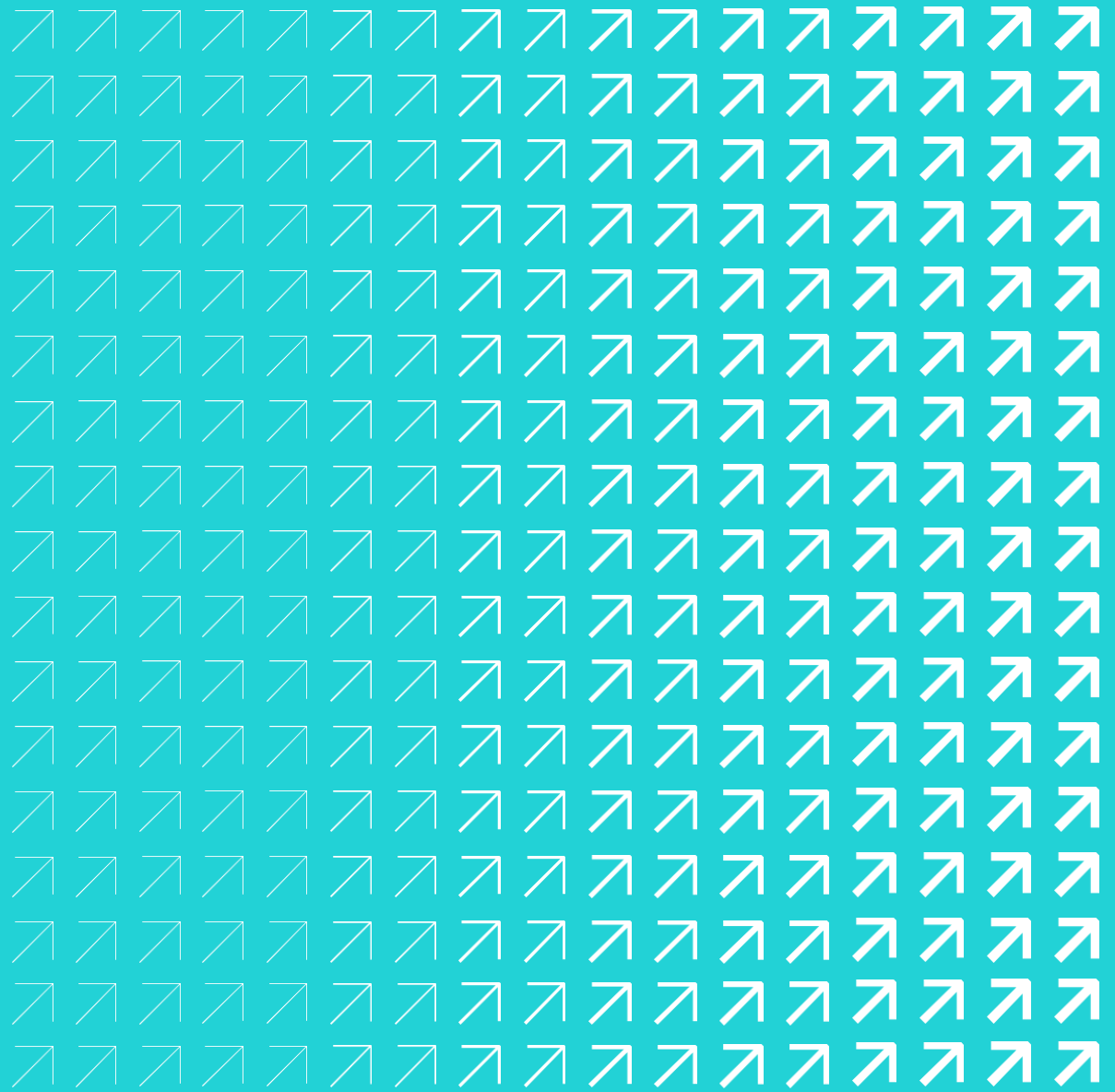
Beach-Westmoreland_Nathaniel@bah.com

Talmo Martins

Martins_Talmo@bah.com

Erin Wehlage

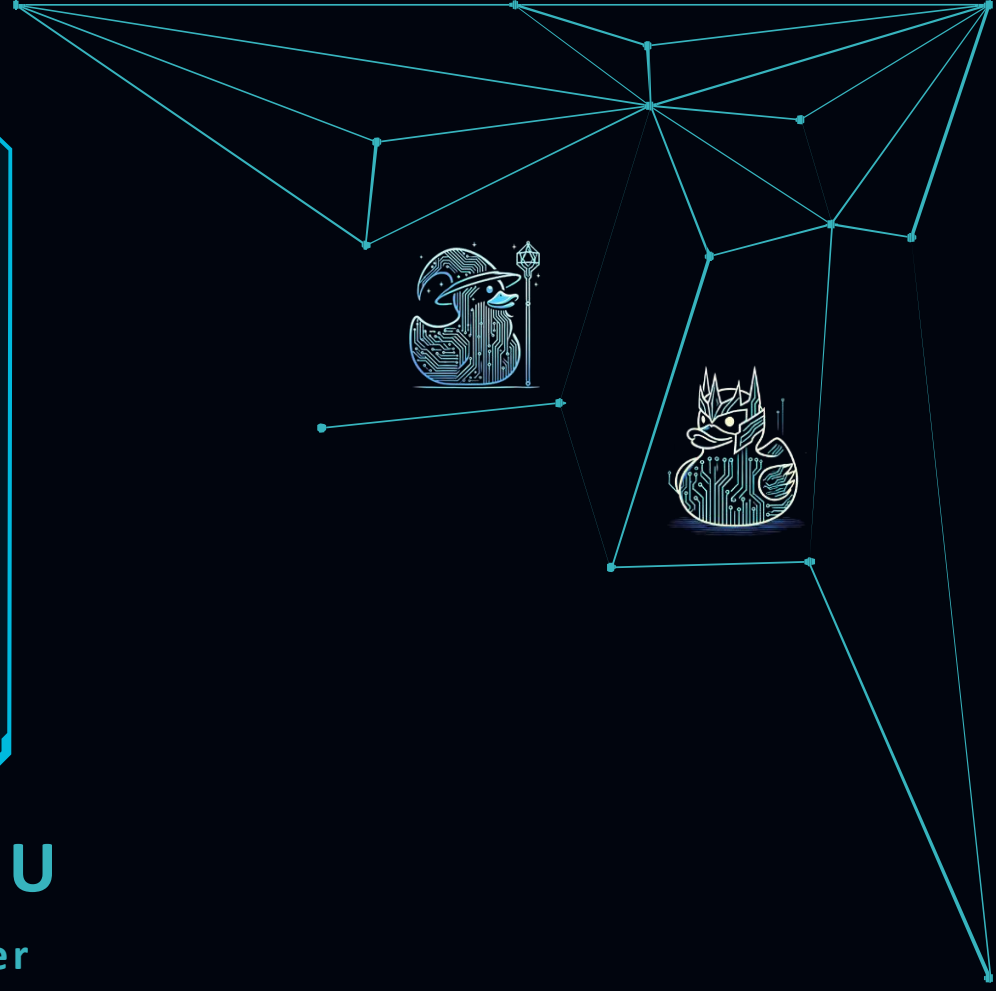
Davis_Erin@bah.com



AI-Augmented Embedded Security Assessment for Bulk Electric System Resilience

By Matthew Prater & Jake Brandau

AXE.AI



MATTHEW PRATER

DOO / Senior Penetration Tester

JAKE BRANDAU

Senior Penetration Tester

GIAC PENETRATION TESTER GPEN · GIAC CERTIFIED INCIDENT HANDLER GCIH · GIAC SECURITY ESSENTIALS CERTIFICATION GSEC · GIAC FOUNDATIONAL CYBERSECURITY TECHNOLOGIES GFACT · eJPT · CompTIA Security+ CERTIFIED · Microsoft CERTIFIED AZURE FUNDAMENTALS

Etc.....

AXE.AI

WHY THIS MATTERS

CIP focuses heavily on networks and access control

Many BES devices are embedded systems

Hardware interfaces are often overlooked

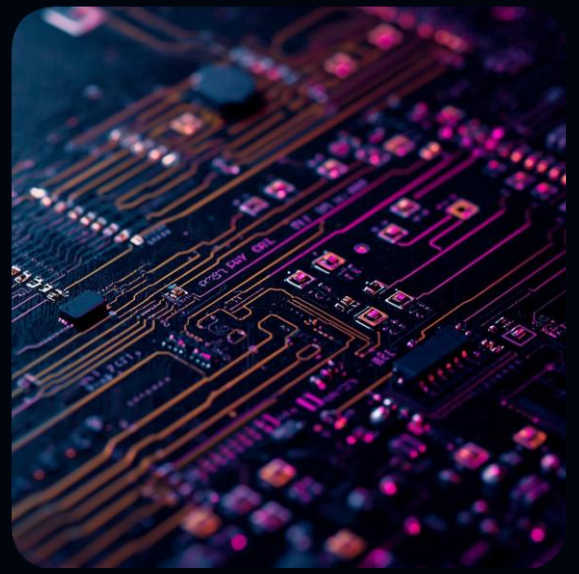
- Relays
- RTUs
- Serial Gateways
- PLCs
- Network Appliances

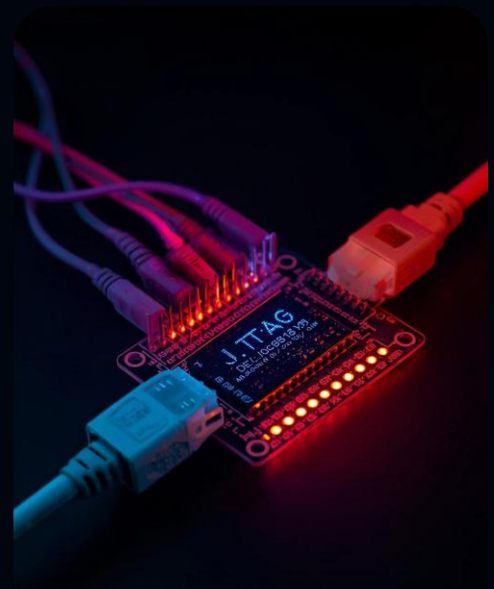
AXE.AI

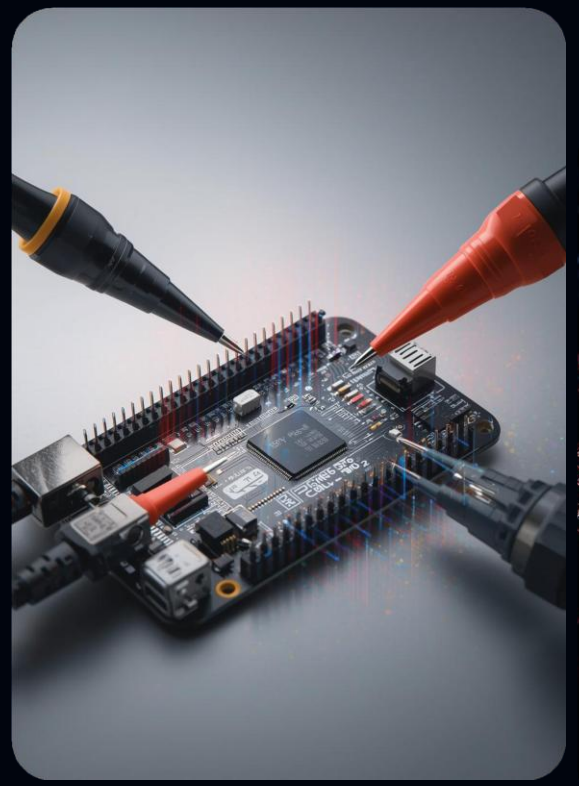
THE HIDDEN ATTACK SURFACE

These interfaces are often left enabled for maintance but can expose systems access.

- UART
- I2C
- JTAG
- Debug Headers
- SPI
- Console Ports

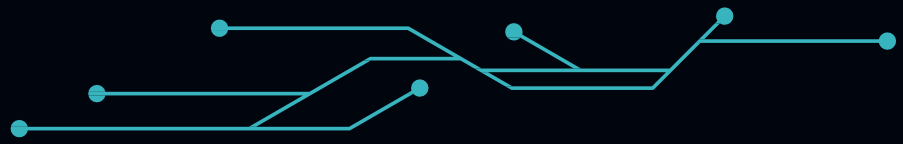


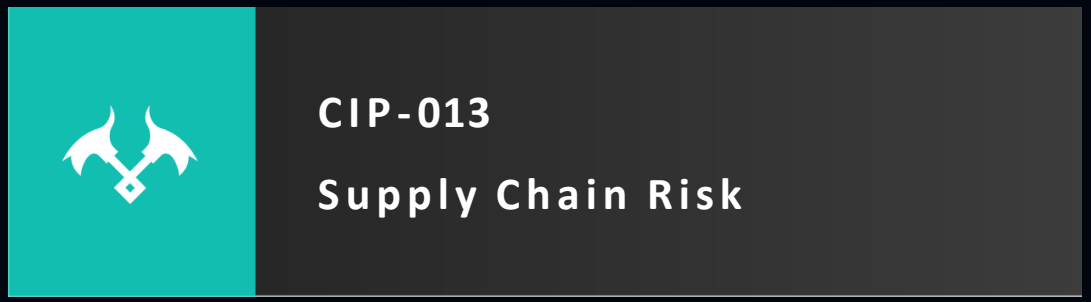




AXE.AI

WHERE THIS INTERSECTS WITH NERC CIP





AXE.AI

AI-Augmented Embedded Security Assessment

We have developed internal research tooling that leverages AI to augement security analysts during embedded security testing

This approach expidites:

- AI-assisted analysis of embedded serial consoles
- Automated identification of bootloaders, prompts, and system behaviors
- Interactive guidance for analysts
- Acceleration of firmware and embedded system analysis
- Bridges hardware Security Research and AI

AXE.AI

DEMO

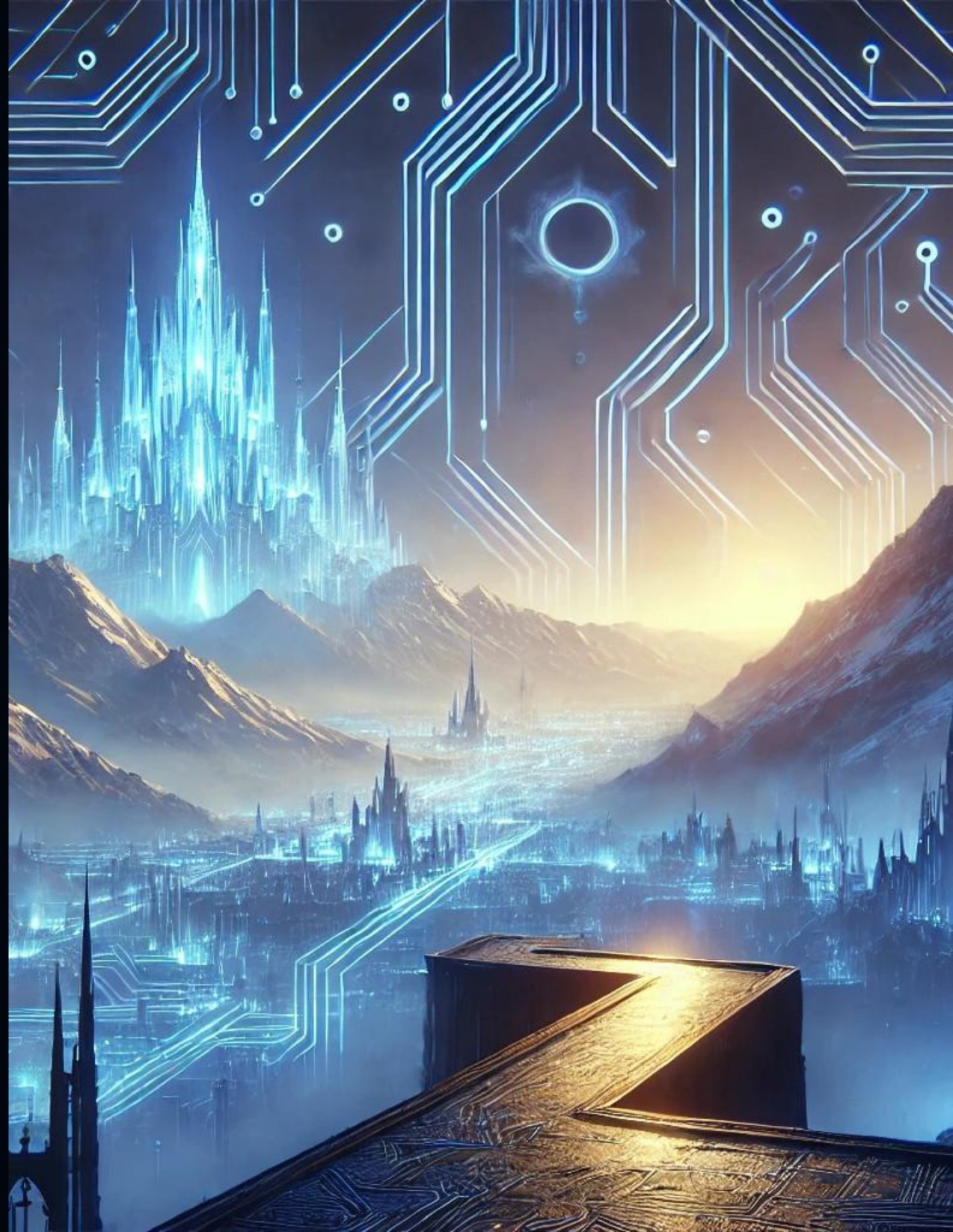
THANK YOU

EMAIL:
matt.prater@strongcrypto.com

jake.bradau@strongcrypto.com

LinkedIn:

AXE.AI



Wrap-Up

Thank you for coming!

You will receive a short survey via e-mail. Please complete it to help Texas RE develop future outreach.