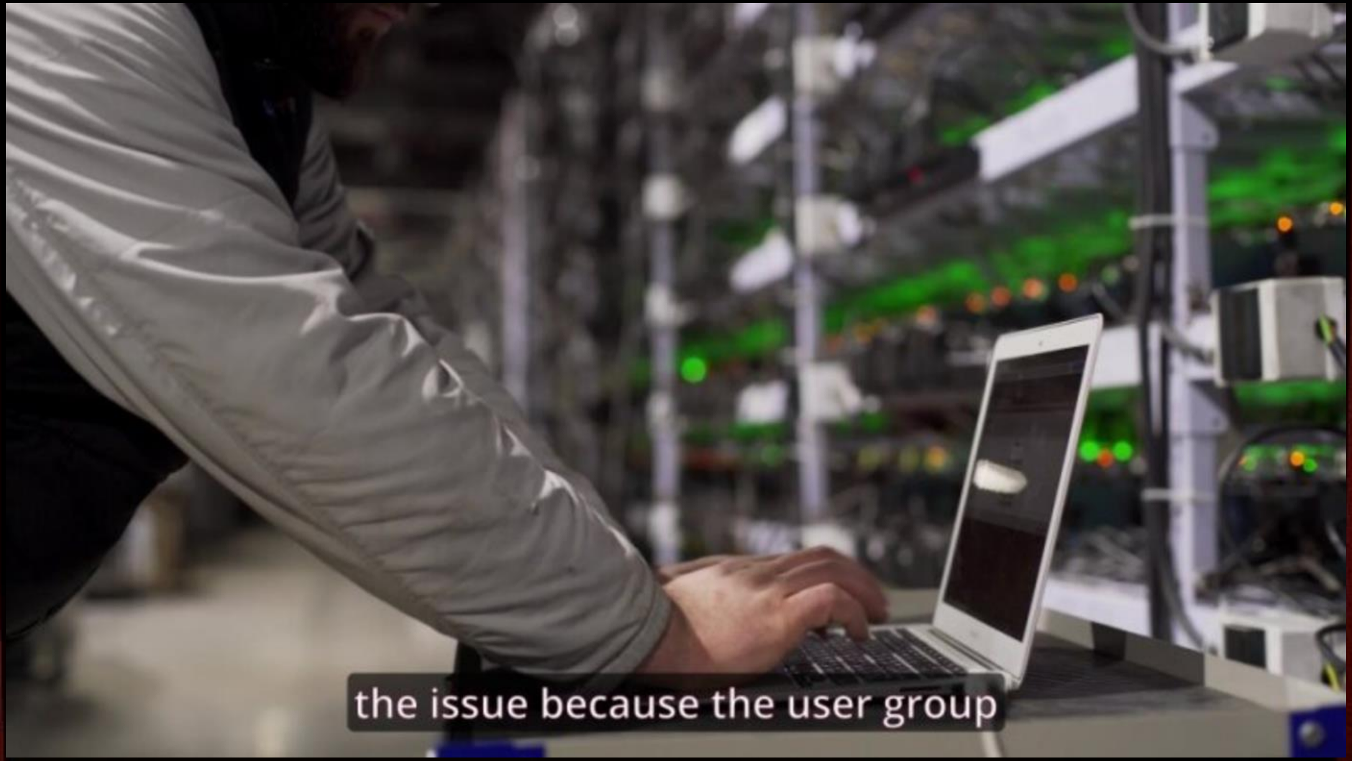
WELCOME TO TECHNICAL TALK WITH RF



October 20, 2025

TECH TALK WITH RELIABILITY FIRST

WELCOME TO
TECHNICAL TALK WITH RF

October 20, 2025

TECH TALK WITH RELIABILITY FIRST

WELCOME TO
TECHNICAL TALK WITH RF

October 20, 2025

TECH TALK WITH RELIABILITY FIRST

WELCOME TO

TECHNICAL TALK WITH RF

October 20, 2025

TECH TALK WITH RELIABILITY FIRST

TECHNICAL TALK WITH RF

Join the conversation at

SLIDO.com

#TechTalkRF

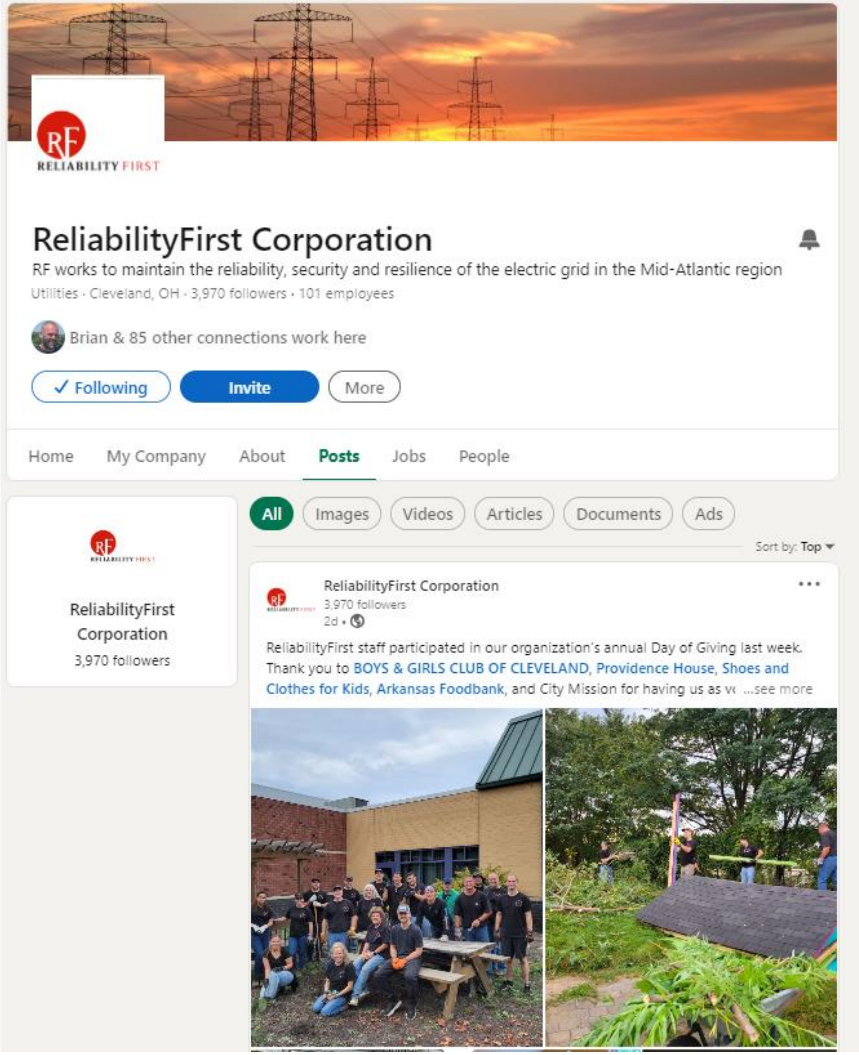
FORWARD TOGETHER RELIABILITYFIRST

TECHNICAL TALK WITH RF

Follow us on

LinkedIn

Linkedin.com/company/reliabilityfirst-corporation



RELIABILITY FIRST

ReliabilityFirst Corporation

RF works to maintain the reliability, security and resilience of the electric grid in the Mid-Atlantic region

Utilities · Cleveland, OH · 3,970 followers · 101 employees

Brian & 85 other connections work here

ReliabilityFirst Corporation
3,970 followers

ReliabilityFirst Corporation
3,970 followers
2d •

ReliabilityFirst staff participated in our organization's annual Day of Giving last week. Thank you to BOYS & GIRLS CLUB OF CLEVELAND, Providence House, Shoes and Clothes for Kids, Arkansas Foodbank, and City Mission for having us as v(...see more

TECH TALK REMINDERS

Please keep your information up-to-date

- CORES and Generation Verification Forms

Following an event, send EOP-004 or OE-417 forms to disturbance@rfirst.org

CIP-008-6 incident reports are sent to the E-ISAC and the DHS CISA

Check our monthly CMEP update and newsletter:

- 2025 ERO Periodic Data Submittal schedule
- Timing of Standard effectiveness

BES Cyber System Categorization (CIP-002-5.1a)

- Assess categorization (low, medium, or high) regularly and notify us of changes

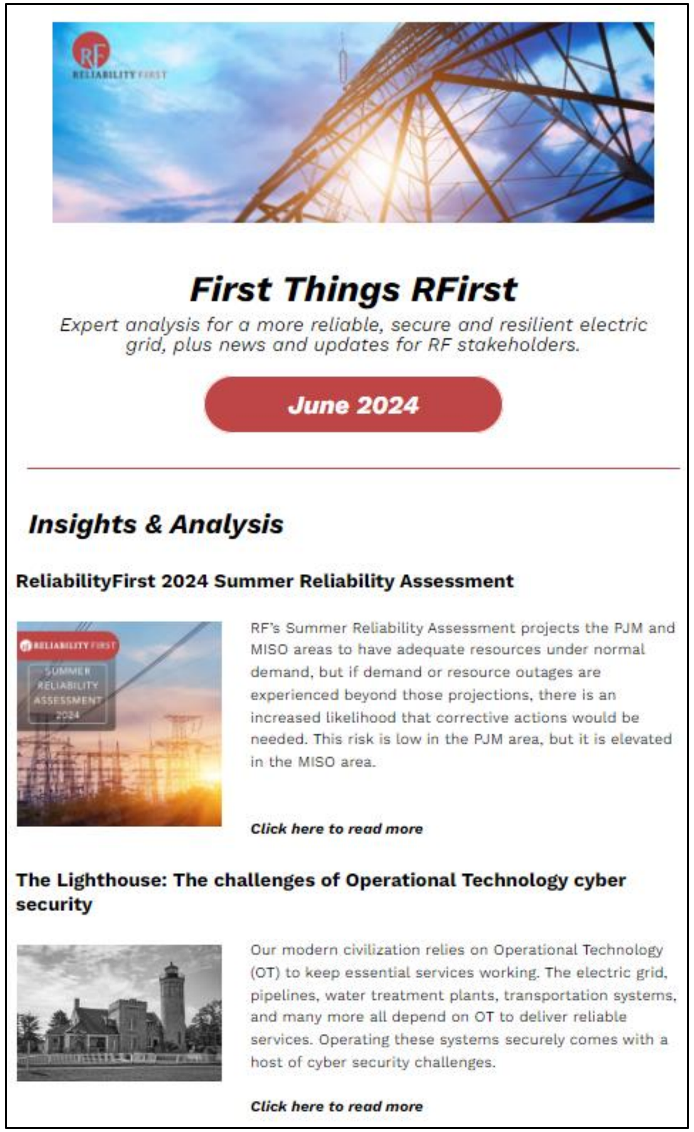
CIP Evidence Request Tool V9 was released and is on NERC's website

TECH TALK REMINDER

Are you getting our newsletter ***First Things RFirst?***

- Sign up today **here**

Also, make sure to check out our **2024 Impact Report** and **video**



First Things RFirst

Expert analysis for a more reliable, secure and resilient electric grid, plus news and updates for RF stakeholders.

June 2024

Insights & Analysis

ReliabilityFirst 2024 Summer Reliability Assessment

RF's Summer Reliability Assessment projects the PJM and MISO areas to have adequate resources under normal demand, but if demand or resource outages are experienced beyond those projections, there is an increased likelihood that corrective actions would be needed. This risk is low in the PJM area, but it is elevated in the MISO area.

Click here to read more

The Lighthouse: The challenges of Operational Technology cyber security

Our modern civilization relies on Operational Technology (OT) to keep essential services working. The electric grid, pipelines, water treatment plants, transportation systems, and many more all depend on OT to deliver reliable services. Operating these systems securely comes with a host of cyber security challenges.

Click here to read more

WELCOME TO TECHNICAL TALK WITH RF

October 20, 2025

FORWARD TOGETHER RELIABILITYFIRST

FORWARD TOGETHER RF RELIABILITYFIRST

TECH TALK ANNOUNCEMENT

RELIABILITYFIRST

Upcoming In-Person Events, February 2026: Internal Controls Workshop & ERO Women's Leadership

RELIABILITY FIRST
INTERNAL CONTROLS WORKSHOP
FEB. 23-25, 2026 | CLEVELAND, OH

ERO WOMEN'S LEADERSHIP CONFERENCE
FEB. 25-26, 2026 | CLEVELAND, OH
Hosted by RELIABILITY FIRST

Join us this coming February at The Aviator in Cleveland, OH for a unique, interactive Internal Controls Workshop. Then be sure to stick around for the 2026 ERO Women's Leadership Conference!

Be sure to register today and be a part of the hotel discount. Register via Eventbrite or link on ReliabilityFirst website.

TECH TALK ANNOUNCEMENT

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

"Currently Compliant"

Episode 7 | Abeyance

NERC released the seventh installment of its compliance podcast, "Currently Compliant." This episode features Lonnie Ratliff, NERC's Director of Compliance Assurance, and special guest Erin Cullum Marcussen, Senior Manager of Compliance at Southwest Power Pool as they discuss with host Ryan Mauldin the topic of **Abeyance**.

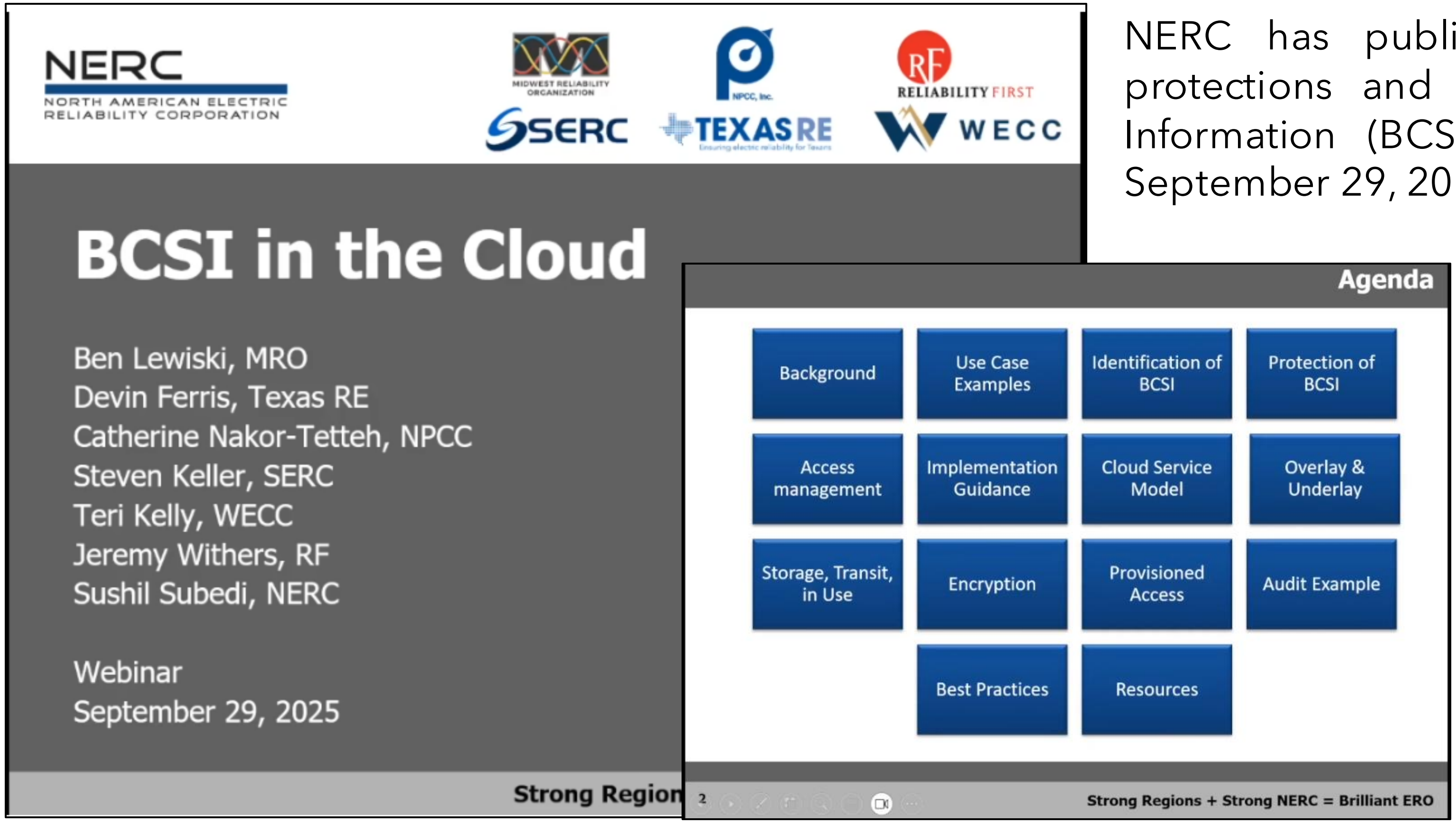
The episode defines the concept of abeyance and clarifies how it will be used within the ERO Enterprise. The discussion addresses common questions, including the crucial role of "good faith" implementation, how abeyance periods are determined, and what entities should do if they are not audited during an abeyance period. The conversation also covers how feedback will be gathered and communicated to industry.

TECH TALK ANNOUNCEMENT

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Webinar Posted: “BCSI in the Cloud”

Streaming Webinar | BCSI in the Cloud


NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION
MIDWEST RELIABILITY ORGANIZATION
NPCC, Inc.
RELIABILITY FIRST
SERC
TEXAS RE
WECC

BCSI in the Cloud

Ben Lewiski, MRO
Devin Ferris, Texas RE
Catherine Nakor-Tetteh, NPCC
Steven Keller, SERC
Teri Kelly, WECC
Jeremy Withers, RF
Sushil Subedi, NERC

Webinar
September 29, 2025

Strong Region

Agenda

Background	Use Case Examples	Identification of BCSI	Protection of BCSI
Access management	Implementation Guidance	Cloud Service Model	Overlay & Underlay
Storage, Transit, in Use	Encryption	Provisioned Access	Audit Example
	Best Practices	Resources	

2 Strong Regions + Strong NERC = Brilliant ERO

NERC has publicly shared the streamed webinar on protections and controls related to BES Cyber System Information (BCSI), which was originally conducted on September 29, 2025.

The webinar includes reviewing examples, considerations, and best practices and is posted on the NERC website.

TECH TALK ANNOUNCEMENT

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

A DIVISION OF NERC
E-ISAC
ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER

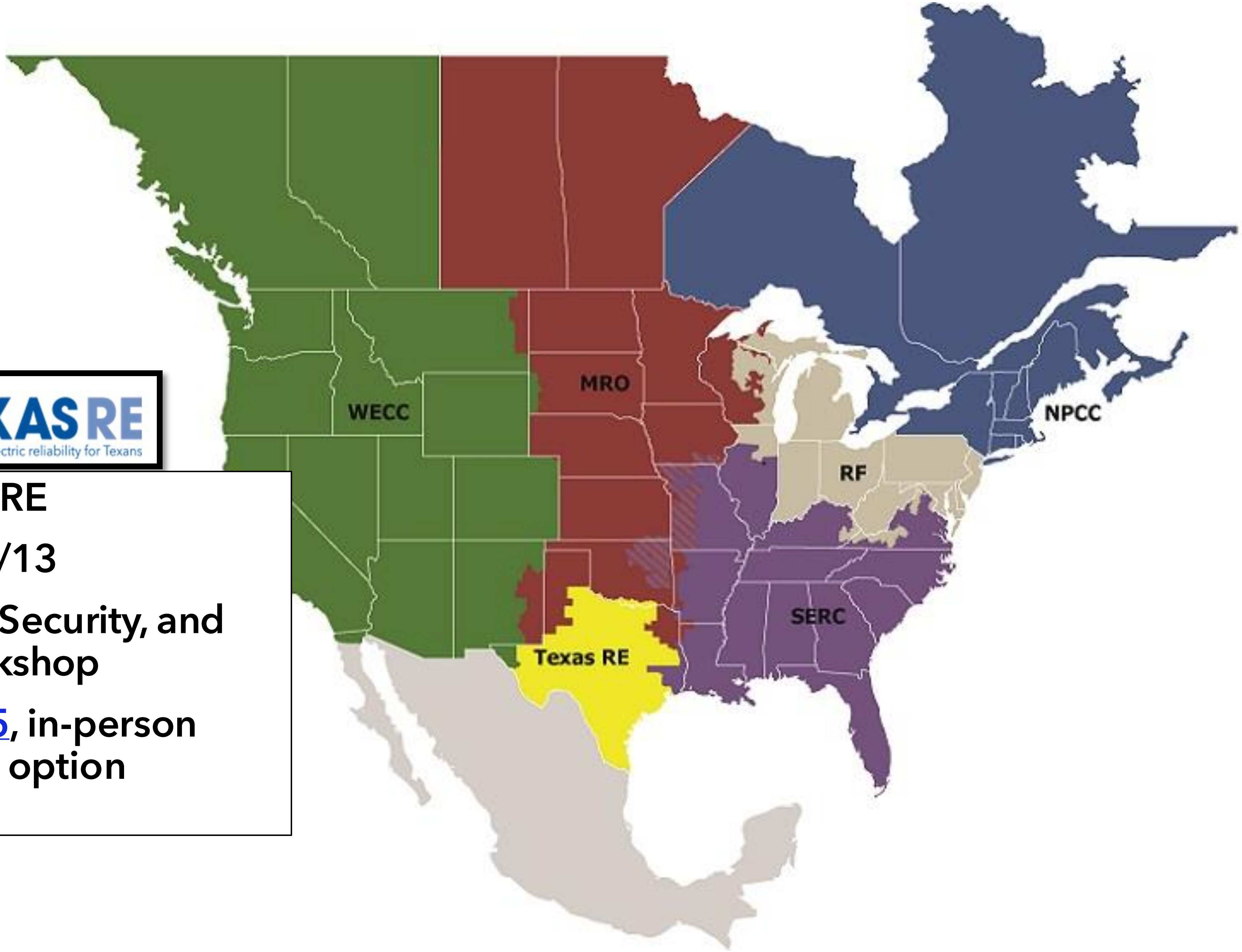
NERC Statement on the Cybersecurity Information Sharing Act of 2015

Full Statement

NERC and the E-ISAC continue to follow developments around the Cybersecurity Information Sharing Act of 2015 (CISA 2015) reauthorization. As a private entity, E-ISAC information sharing activities remain business as usual. We also understand the important protections CISA 2015 afforded to utilities when sharing information with the government.

As Congress considers CISA 2015 reauthorization, information sharing and cooperation within and across critical infrastructure sectors remains vitally important. […]

As the industry continues its efforts to inform Congress of the importance of CISA 2015 in facilitating industry cooperation with the federal government, the industry should also continue sharing information across the sector and with other sectors through the E-ISAC and other trusted information sharing partnerships. More than 400 million North Americans depend on us to assure the reliability and security of the North American grid.



TEXAS RE
Ensuring electric reliability for Texans

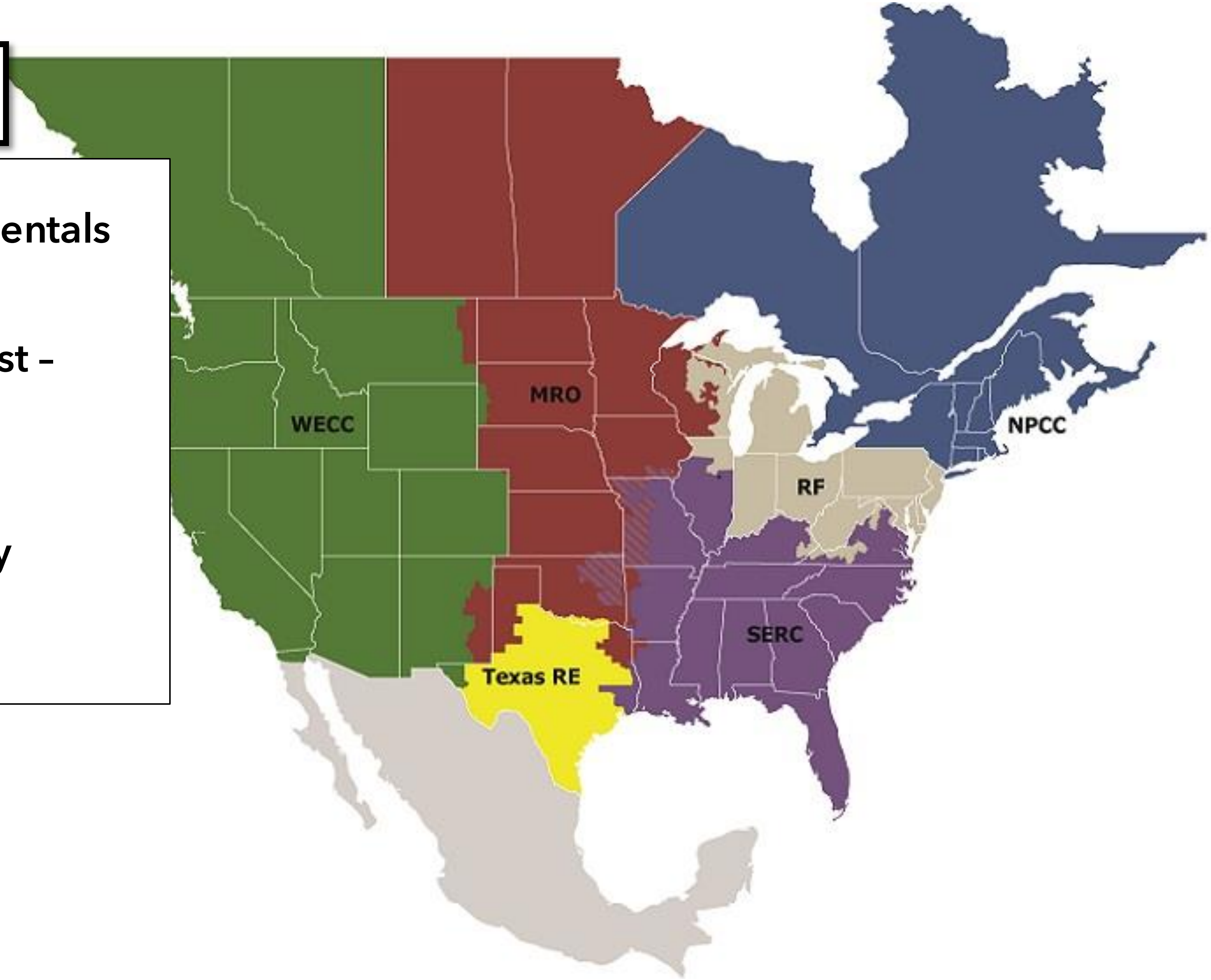
Talk with Texas RE

- TPL-008, 11/13

Fall Standards, Security, and Reliability Workshop

- November 5, in-person with WebEx option

WECC



WECC Grid Fundamentals

- November 4-5

Reliability in the West –
A Discussion Series

- November 5

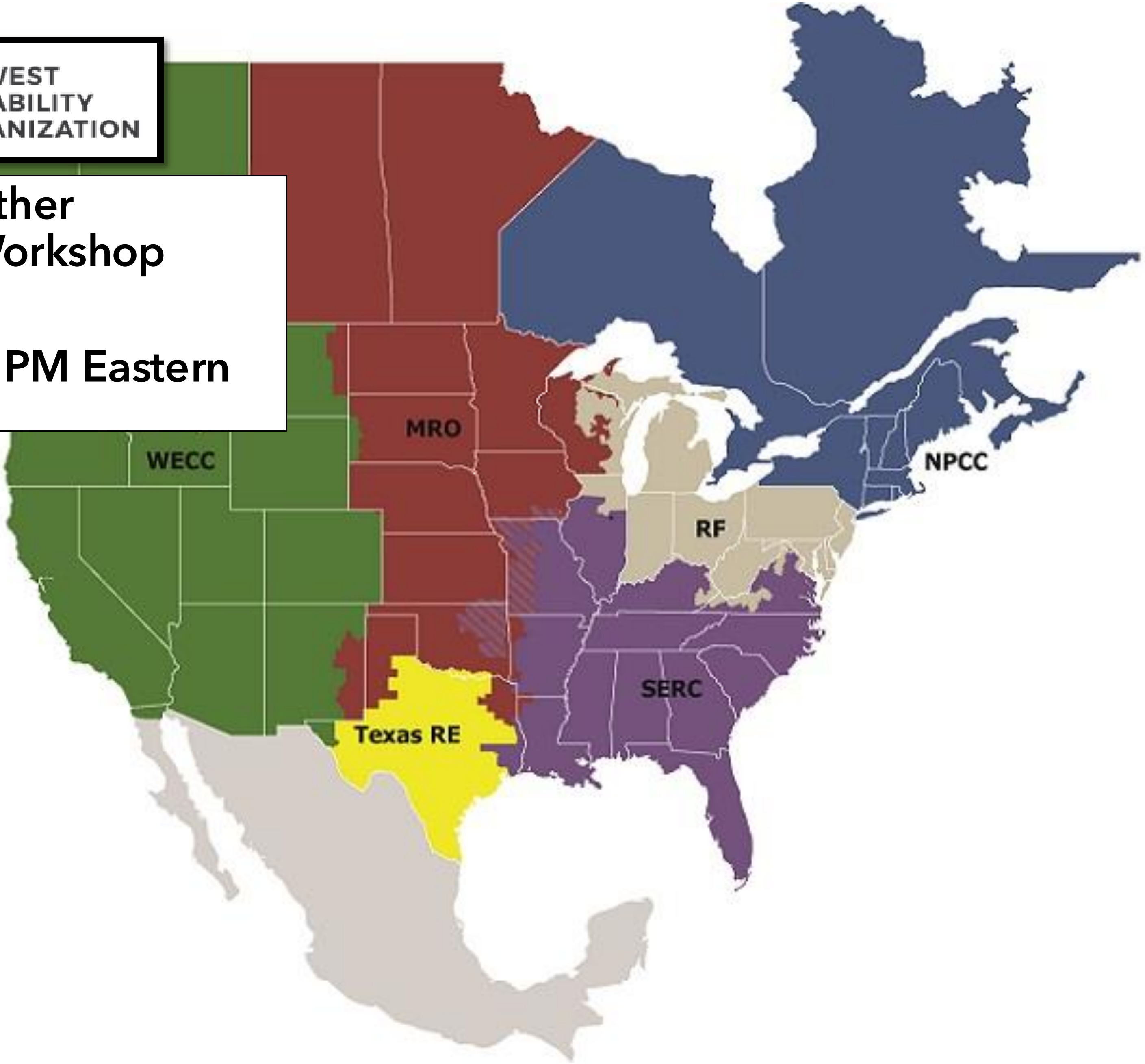
Reliability & Security
Oversight Update

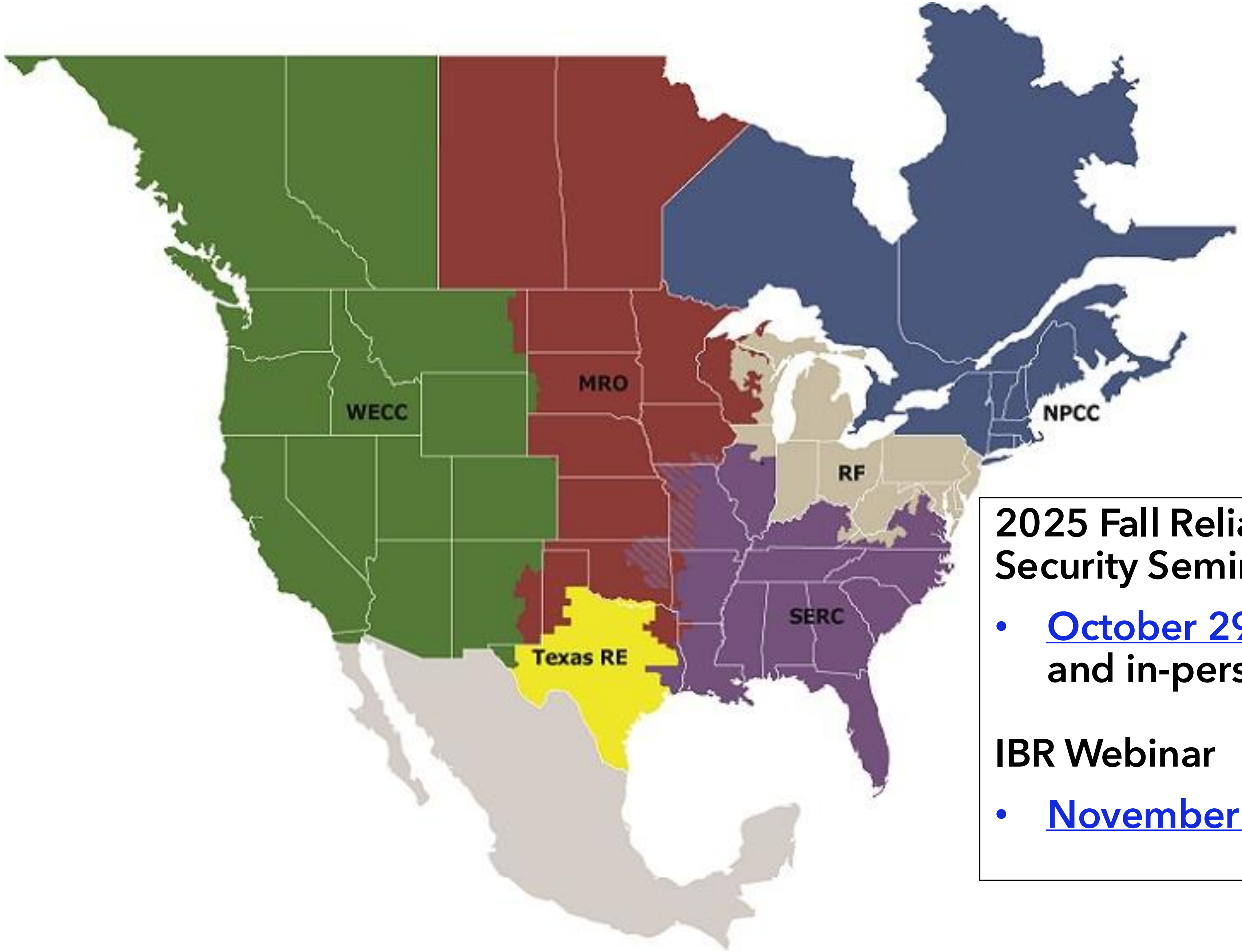
- November 20

MIDWEST RELIABILITY ORGANIZATION

2025 Cold Weather Preparedness Workshop

- October 22,
  9:30 – 12:30 PM Eastern



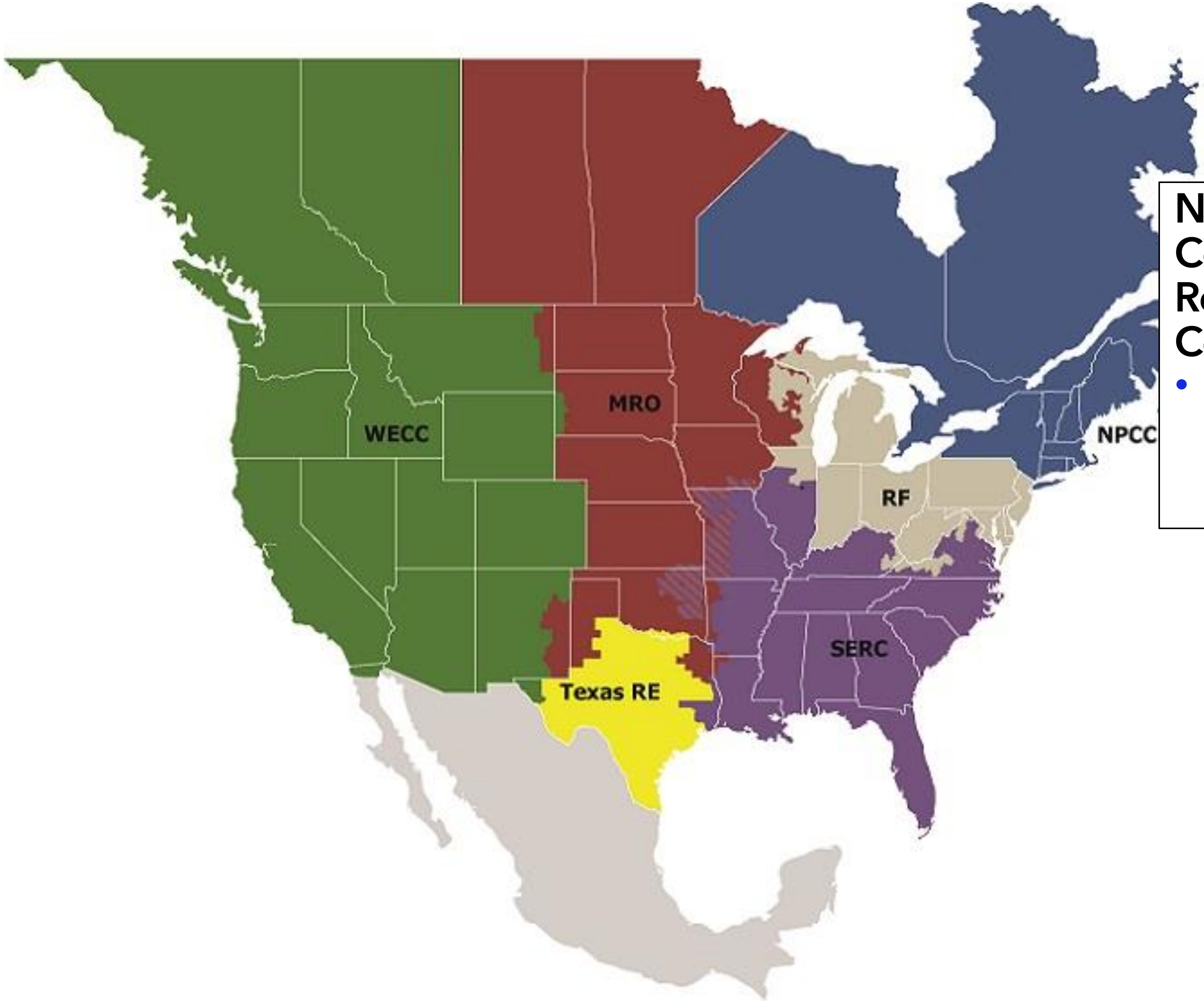


2025 Fall Reliability and Security Seminar

- October 29-30, virtual and in-person options

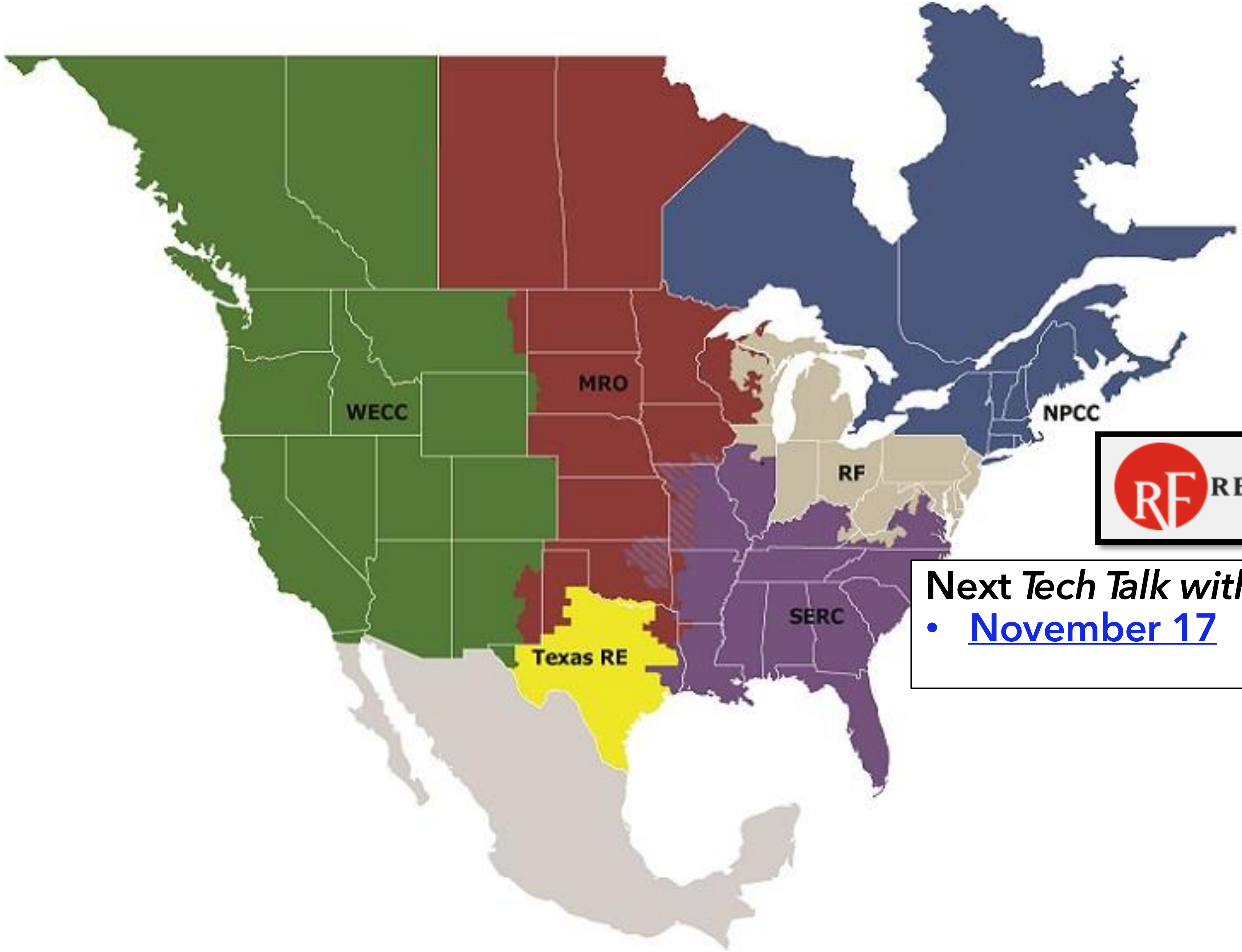
IBR Webinar

- November 5, virtual



NPCC Fall 2025 Compliance and Reliability Conference

- November 5 - 6 in-person and remote options



RELIABILITYFIRST

Next *Tech Talk with RF*

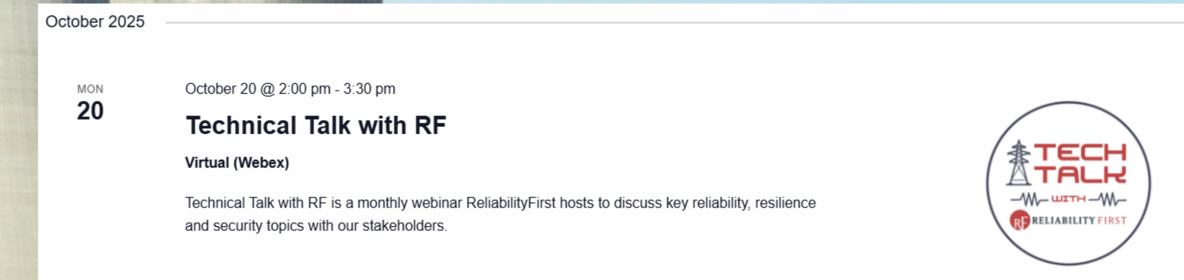
- November 17

FORWARD TOGETHER RF RELIABILITYFIRST

TECH TALK REMINDER

Tech Talk with RF announcements are posted on our calendar on www.rfirst.org under Calendar

CLICK HERE



October 2025

MON
20

October 20 @ 2:00 pm - 3:30 pm

Technical Talk with RF

Virtual (Webex)

Technical Talk with RF is a monthly webinar ReliabilityFirst hosts to discuss key reliability, resilience and security topics with our stakeholders.

FORWARD TOGETHER RF RELIABILITYFIRST

TECHNICAL TALK WITH RF

Join the conversation at

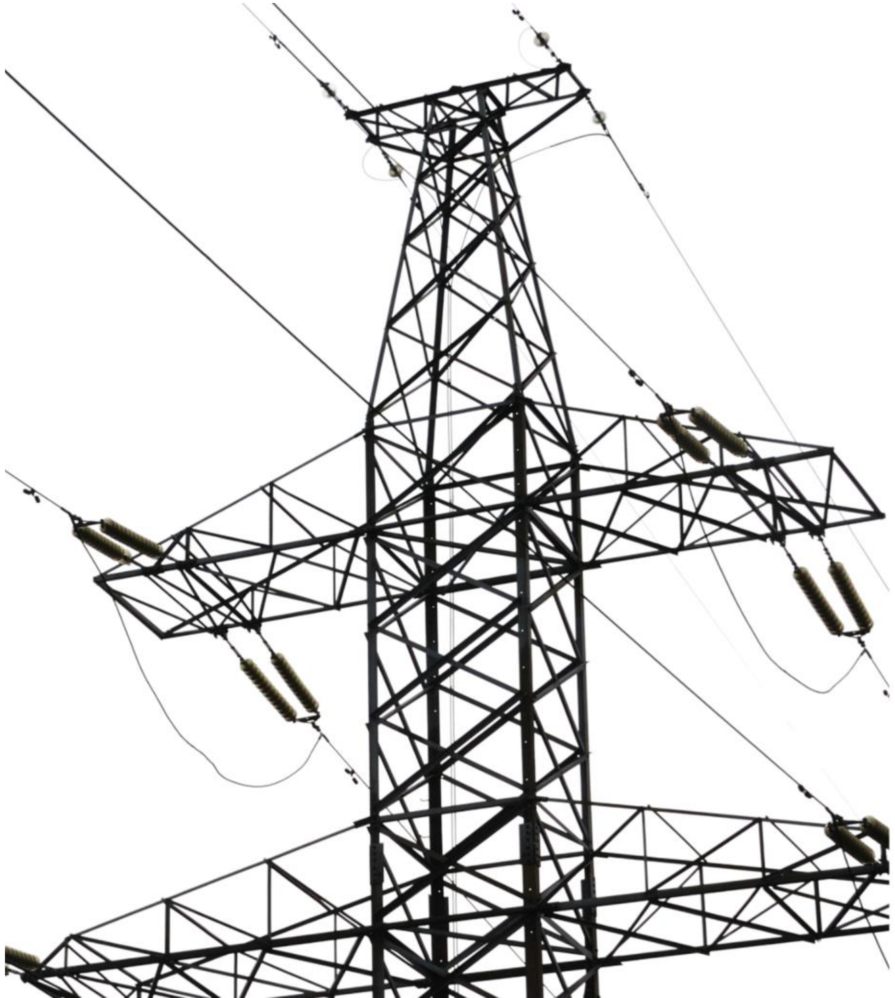
SLIDO.com

#TechTalkRF

Anti-Trust Statement

It is ReliabilityFirst's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct which violates, or which might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition.

It is the responsibility of every ReliabilityFirst participant and employee who may in any way affect ReliabilityFirst's compliance with the antitrust laws to carry out this policy.



AGENDA

FIRST ENERGY CIP-003-9 IMPLEMENTATION

- **DONNA BURSICK,** DIRECTOR, OT SYSTEMS & TX/DX PRODUCTS, FIRSTENERGY
- **JASON MCCORMICK,** DIRECTOR, CYBER SECURITY GOVERNANCE, FIRSTENERGY
- **GRANT MCDONALD,** TECHNICAL ADVISOR, IT TRANSMISSION SYSTEMS, FIRST ENERGY

HOW TO ADDRESS THE RISK OF INSUFFICIENT TRAINED OT CYBER SECURITY PERSONNEL

- **MIKE HOLCOMB,** FELLOW, DIRECTOR – ICS/OT CYBERSECURITY, FLUOR

ICS SECURITY WITHOUT THE GUESSWORK: A RISK-FIRST APPROACH

- **STACY BRESLER,** MANAGING PARTNER, ARCHER ENERGY SOLUTIONS

CIP STANDARDS UPDATE

- **LEW FOLKERTH,** PRINCIPAL RELIABILITY CONSULTANT, RELIABILITYFIRST

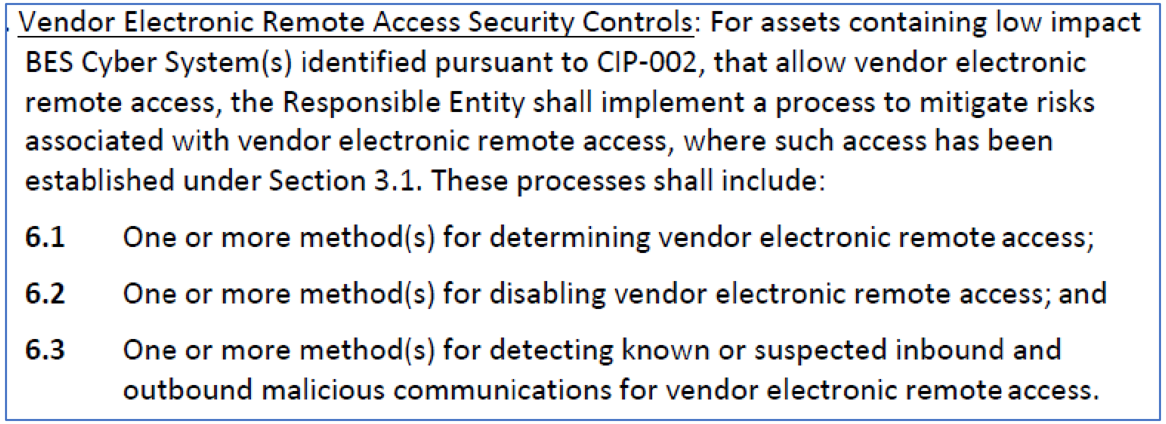
RF October Technical Talk FirstEnergy CIP-003-9 Implementation

10/20/25

CIP-003-9 FirstEnergy Project Details

Background

- Project began in May 2024
- Phase One – Technical Assessment
- Phase Two – Implementation/Documentation/Controls
- Conduct RF Assist Visit – 2025
- Internal Compliance Date – 2/1/26
- Compliance Date – 4/1/26



. 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.

Conclusion

FirstEnergy does not permit the type of vendor remote, or vendor initiated remote access defined in FERC order 829.

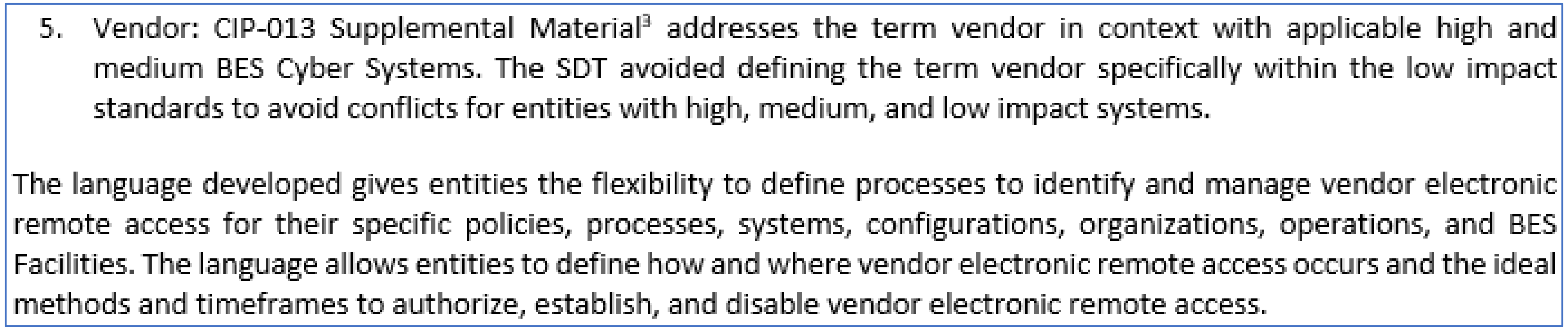
- All access is controlled through FirstEnergy's standard policies and procedures outlined under CIP-004. Each individual user is given a unique user ID and access privileges after proper CIP training and background check.
- Vendor-initiated remote access has two types: user-based access and system-to-system access. Vendor initiated system-to-system access is not permitted by FirstEnergy.

If the CIP environment changes in the future:

- FirstEnergy would use existing infrastructure or add additional intermediate systems as described in CIP-005 compliance program.

Method to Determine Vendor Electronic Remote Access

Excerpt from CIP-003-9 Technical Rationale on “Vendor” definition



5. Vendor: CIP-013 Supplemental Material[3] addresses the term vendor in context with applicable high and medium BES Cyber Systems. The SDT avoided defining the term vendor specifically within the low impact standards to avoid conflicts for entities with high, medium, and low impact systems.

The language developed gives entities the flexibility to define processes to identify and manage vendor electronic remote access for their specific policies, processes, systems, configurations, organizations, operations, and BES Facilities. The language allows entities to define how and where vendor electronic remote access occurs and the ideal methods and timeframes to authorize, establish, and disable vendor electronic remote access.

FirstEnergy Internal CIP Definitions – common across standards

- **Vendor** [FE Internal] - A commercial supplier that enters into an agreement with FirstEnergy to provide a product or service. A Vendor is a Distributor, Integrator, or Original Equipment Maker (or any combination thereof) as defined in this program. A Vendor does not include:

  A commercial supplier that is providing personnel to FirstEnergy solely functioning in the role of contingent labor (i.e., perform functions like those of FirstEnergy full time employees) that follow the relevant CIP-004 processes for background checks and access authorization.

  NERC-registered entities that FirstEnergy may have a business relationship with that provide reliability functions such as, but not limited to, a Balancing Authority, Transmission Operator, or Reliability Coordinator.

  Any organization that provides Open-Source Software as defined in this program.

- **Vendor Remote Access** [FE Internal] - Interactive Remote Access to a BES Cyber System by an external party that is providing a service under a procurement contract (e.g., break-fix support services, point-in-time implementation support, integration service, etc.). This term does not include contractors working for FirstEnergy as consultants or contingent labor. See FE-CIP-CSEC-PRG-130 Supply Chain Risk Management for determining what is a “vendor” for the purposes of this definition.

Vendor Low-Impact Electronic Remote Access Assessment

Dial-Up

No Access

Low Impact BCS only

- Substation relays accessed through a substation concentrator via telco provided 4-wire circuit
- Identified and documented at low-impact walk downs
- Tracked at low-impact change control meetings
- Use continually declined
- Access protected with SCADA disconnect point
- Managed by procedure

Sunset Activities

- Less than 10 sites remain configured for dial-up access
- New PCs do not support modem connectivity

Remaining sites were disabled

Crossbow

Contingent Labor

Low and Medium impact BCS

- Substation devices accessed through a centrally managed application that utilizes high-speed MPLS network
- NERC CIP-005 compliant solution
  - Intermediate system
  - encryption terminates at the Intermediate System
  - Requires MFA to use
- Continues to be expanded today
  - Tx and Dx protective relays
  - IT Devices
  - Meters

Follow the relevant CIP-004 processes for background checks and access authorization that are required of FirstEnergy full time employees

Power System Equipment

Data provided to Vendors

Data diodes

- Provide operating information regarding SVCs to vendors that provide warranty services
- Data diode is not an electronic access point
  - No BCS device access
  - Only outbound operational data dumps

Circuit Breaker Sentinel(CBS)

- Provides breaker operational data to vendor that provides warranty services
- Access is via a dial-up 4g modem
- CBS functionality was evaluated by internally and determined to have no impact on the operation of the breaker

The CBS is not part of a BCS

Generation & Other

Generation, Network

Generation

Plant Controllers

- No vendor remote access permitted to generation assets

Network

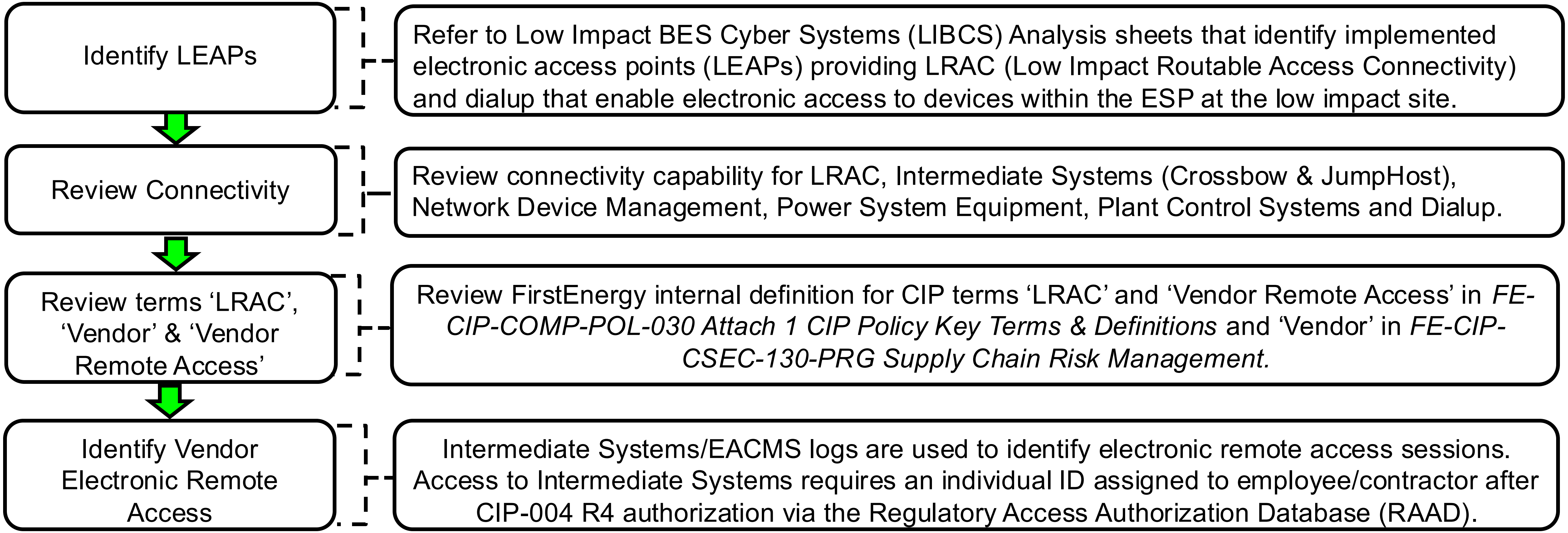
Network Device Management

- Low & Medium Impact Network Devices.

Follow the relevant CIP-004 processes for background checks and access authorization that are required of FirstEnergy full time employees

Process – Procedures – Controls

Method to Determine Vendor Remote Access



Identify LEAPs

Refer to Low Impact BES Cyber Systems (LIBCS) Analysis sheets that identify implemented electronic access points (LEAPs) providing LRAC (Low Impact Routable Access Connectivity) and dialup that enable electronic access to devices within the ESP at the low impact site.

Review Connectivity

Review connectivity capability for LRAC, Intermediate Systems (Crossbow & JumpHost), Network Device Management, Power System Equipment, Plant Control Systems and Dialup.

Review terms ‘LRAC’, ‘Vendor’ & ‘Vendor Remote Access’

Review FirstEnergy internal definition for CIP terms ‘LRAC’ and ‘Vendor Remote Access’ in *FE-CIP-COMP-POL-030 Attach 1 CIP Policy Key Terms & Definitions* and ‘Vendor’ in *FE-CIP-CSEC-130-PRG Supply Chain Risk Management.*

Identify Vendor Electronic Remote Access

Intermediate Systems/EACMS logs are used to identify electronic remote access sessions. Access to Intermediate Systems requires an individual ID assigned to employee/contractor after CIP-004 R4 authorization via the Regulatory Access Authorization Database (RAAD).

Controls

- Change Control - identifies modifications to the CIP environment
- Annual Basis of Compliance – program/procedures/controls/evidence documents demonstrate compliance

Questions?

Humans Wanted: Why Technology Alone Can't Secure Power Plants

Mike Holcomb

Disclaimer

❑ The information provided in this presentation is for educational purposes only.

❑ All knowledge obtained must be used for legitimate, authorized purposes.

❑ The views written and discussed in this course are those of the presenter and not that of their employers or other affiliated organizations.

About Mike

❑ Fellow for Cyber Security at Fluor

❑ ICS/OT Cybersecurity Global Lead

❑ Founder of BSidesICS and BSidesGreenville

❑ CISSP, GRID, GICSP, ISA 62443, GPEN, GCIH, etc.

❑ Master’s degree from SANS Technology Institute

❑ Posts on LinkedIn and YouTube on OT/ICS Cybersecurity

About Mike

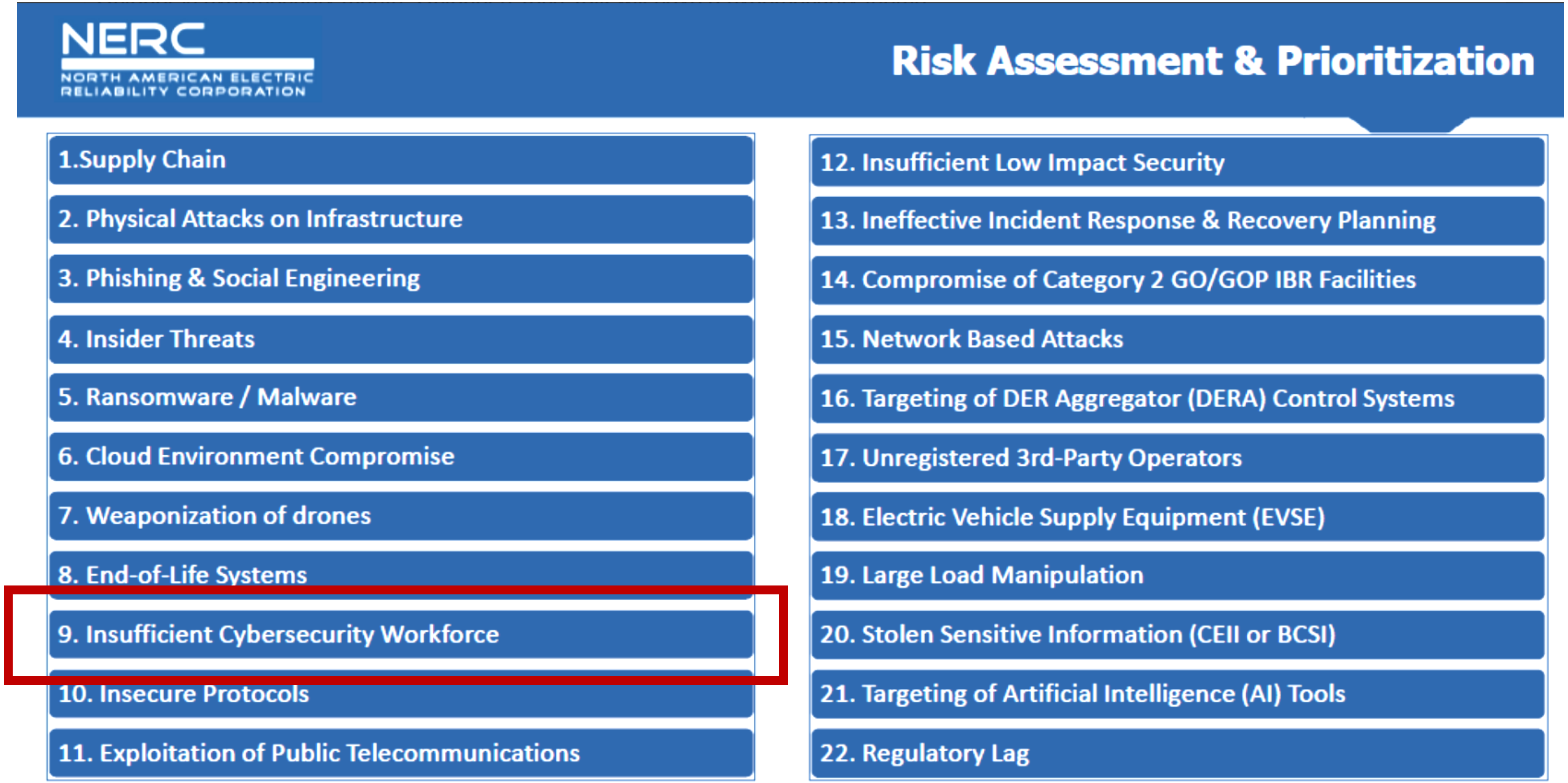
RANGE ROVER

Why We Are Here

❑ The number of attack targeting OT/ICS environments, and connected IT networks, is increasing dramatically

We are not prepared

Emerging Security Risk Survey Results



NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Risk Assessment & Prioritization

1.Supply Chain

2. Physical Attacks on Infrastructure

3. Phishing & Social Engineering

4. Insider Threats

5. Ransomware / Malware

6. Cloud Environment Compromise

7. Weaponization of drones

8. End-of-Life Systems

9. Insufficient Cybersecurity Workforce

10. Insecure Protocols

11. Exploitation of Public Telecommunications

12. Insufficient Low Impact Security

13. Ineffective Incident Response & Recovery Planning

14. Compromise of Category 2 GO/GOP IBR Facilities

15. Network Based Attacks

16. Targeting of DER Aggregator (DERA) Control Systems

17. Unregistered 3rd-Party Operators

18. Electric Vehicle Supply Equipment (EVSE)

19. Large Load Manipulation

20. Stolen Sensitive Information (CEII or BCSI)

21. Targeting of Artificial Intelligence (AI) Tools

22. Regulatory Lag

Is It #9 On YOUR List?

How badly are you struggling to hire OT/ICS cybersecurity team members?

Not Everyone Works in OT/ICS Cybersecurity

❑ <1% of IT cybersecurity professionals are interested in OT/ICS cybersecurity

❑ <1% of engineers and other automation professionals are interested in OT/ICS cybersecurity

Interest Has Increased Over the Last Few Years

But momentum is slowing.

Challenges in Hiring Talent

What challenges in hiring talent are you experiencing?

Challenges in the Hiring Pipeline

❑ Not wanting to be on-site

❑ Equivalent positions in IT pay more

❑ Unrealistic expectations

❑ Lack of belief in the mission

❑ Takes time to develop a well-rounded skillset

❑ Bolt-on security in legacy environments

❑ Cultural differences between IT and OT

❑ Compliance requirements

❑ Stress and burnout

❑ Affordable training

❑ Affordable certifications

The Three Pillars of a Resilient Cyber Workforce

Recruit

You cannot afford to wait for talent to appear. You must GROW it!

Retain

It's less expensive, and more secure, to keep talent than replace it.

Reskill

Your next great cybersecurity team member might already work for you.

Recruit

- □ Host internship programs
- □ Partner with local trade schools and community colleges
- □ Recruit from relevant fields
- □ Evolve your hiring criteria
- □ Promote the mission

Retain

❑ Establish career paths for upward movement

❑ Provide budget for training and certifications

❑ Provide flexible working conditions where possible

❑ Remember that team members want to feel seen, appreciated and that their work makes a difference

Reskill

- ❑ Cross-train between IT and OT/ICS
- ❑ Consider imbedding team members in other roles
- ❑ Provide budget for training and certifications
- ❑ Establish mentorship programs

The Three Pillars of a Resilient Cyber Workforce

Recruit

You cannot afford to wait for talent to appear. You must GROW it!

Retain

It's less expensive, and more secure, to keep talent than replace it.

Reskill

Your next great cybersecurity team member might already work for you.

Free Training for ICS/OT Cyber Security

THANK YOU!

❑ Please don’t hesitate to reach out!

linkedin.com/in/mikeholcomb
mikeholcomb.com
mike@mikeholcomb.com
youtube.com/@utilsec
github.com/utilsec

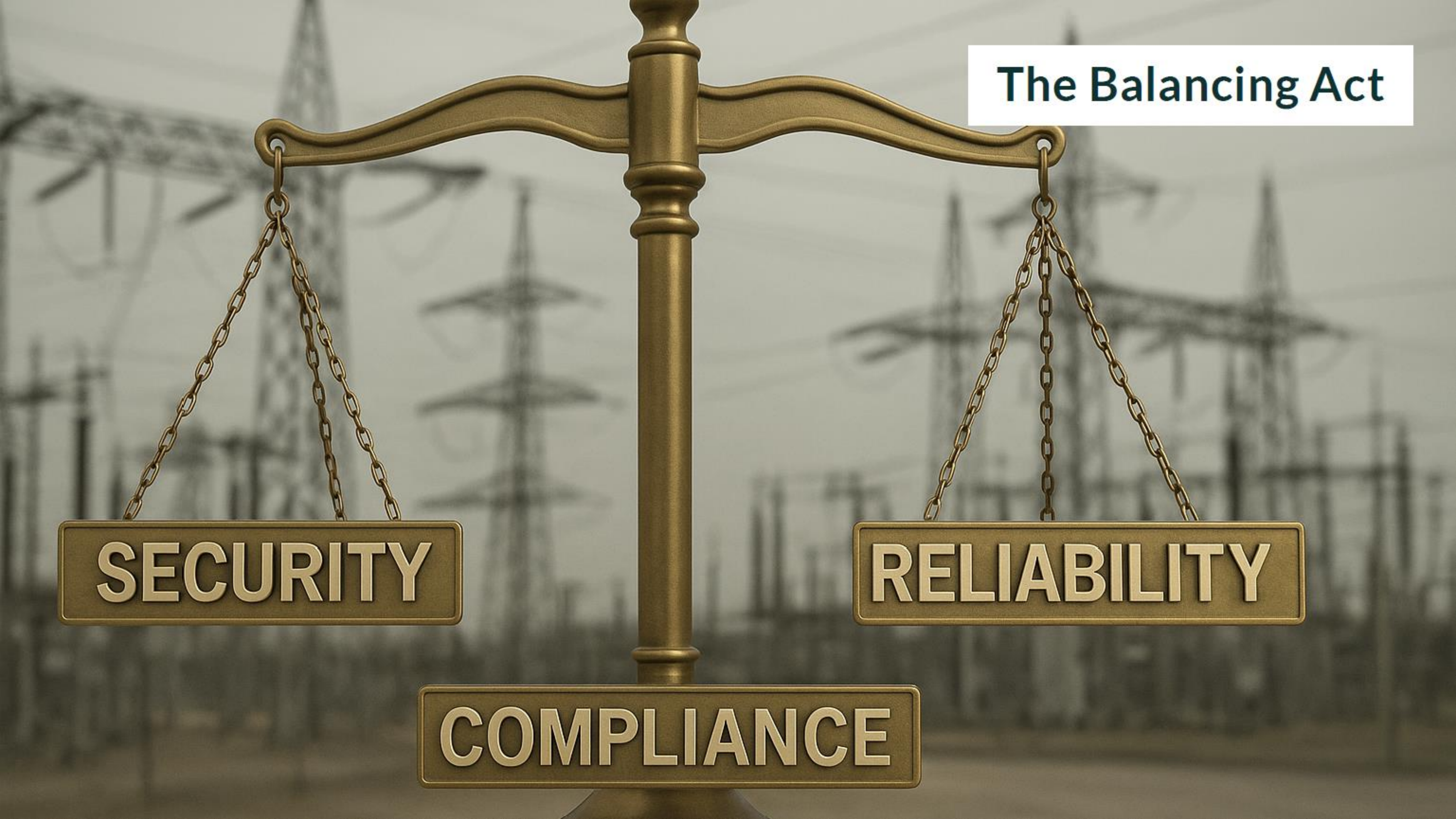
Mike Holcomb
Helping YOU Secure ICS/OT

ICS Security Without the Guesswork:

A Risk-First Approach

Presented by: Stacy Bresler, Managing Partner | Archer Energy Solutions LLC

The Balancing Act



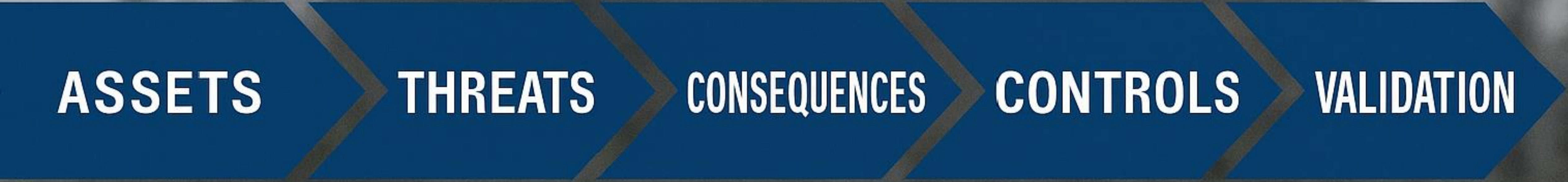
The Checklist Trap

From Reaction to Reflection

Incidents

Regulations

Risk Cycle



ASSETS

THREATS

CONSEQUENCES

CONTROLS

VALIDATION

Risk-First Thinking Explained

Context Revealed

Seeing What Matters: Visibility with Purpose

The Hidden Connections

Living Off the Land: The Quiet Threat

RAW DATA

INSIGHT

ACTION

Turning Data into Decisions

Controls That Count

Culture: The Hardest Control of All

Making Compliance Work for You

Risk Reduced Over Time

CLARITY

From Guesswork to Clarity

Stacy Bresler

ARCHER

ISO 127001 Lead Auditor | NIST CSF 2.0 Lead Implementer | NERC Certified Lead Audit | Recovering NERC CIP Auditor (WECC) | Suffering Musician | Grandfather to the Perfect Granddaughter | Devoted husband and father of three Amazing Grown Men | Disney enthusiast | Hates Spiders

🌐 archerint.com

☎ 503-789-5515

@ s.bresler@archerint.com

CIP STANDARDS UPDATE

Lew Folkerth, PE, LPI, +9

Principal Reliability Consultant

October 20, 2025

RELIABILITY FIRST

FORWARD TOGETHER RELIABILITYFIRST

SEPTEMBER 18, 2025 COMMISSION ACTIONS

LOW IMPACT

VIRTUALIZATION

SUPPLY CHAIN

RM25-8-000 CIP-003-11 NOPR

The CIP-003-11 Notice of Proposed Rulemaking (NOPR) requests comments on three proposed actions:

1. Approve CIP-003-11,
2. Order the strengthening of the low impact requirements in response to cybersecurity threats, and
3. Order a study on evolving threats as they relate to low impact systems.

Comments are due November 22, 2025.

RM24-8-000 VIRTUALIZATION NOPR

The virtualization CIP standards NOPR requests comments on the approval of the virtualization versions of the CIP standards.

Comments on this NOPR are due November 22, 2025.

RM24-8-000 VIRTUALIZATION NOPR

The NOPR expresses concerns and questions regarding the elimination of Technical Feasibility Exceptions (TFEs), to be replaced by "per system capability."

- The NOPR questions the continued need for these exceptions at all, pointing out that they were instituted to prevent early retirement of long-life legacy equipment. It has been 15 years since these exceptions were put in place, and most, if not all, of these legacy systems should have been retired by now.
- The NOPR asks four questions regarding "per system capability" exceptions:
  - How will these exceptions be monitored other than through CMEP processes?
  - How will entities be informed as to legitimate use of these exceptions?
  - What obligations will an entity have to mitigate the security gaps introduced by these exceptions?
  - How will NERC ensure consistency across the ERO in the review of these exceptions?

The NOPR asks for comments and suggestions for alternative approaches.

SUPPLY CHAIN ORDER 912

Order 912 addresses two dockets:

1. RM24-4-000, Supply Chain Risk Management Reliability Standards Revisions
2. RM20-19-000, Equipment and Services Produced or Provided by Certain Entities Identified as Risks to National Security

SUPPLY CHAIN ORDER 912

Order 912 requires NERC to develop revisions to supply chain requirements to:

A. Include timing requirements for supply chain risk assessments including:
   i. A maximum time between a supply chain risk assessment and the installation of related equipment,
   ii. A requirement to periodically reassess the risk associated with existing vendors, and
   iii. Establish a maximum time frame for which a risk assessment will be valid.

B. Establish a process to document, track, and respond to all identified supply chain risks.

C. Include Protected Cyber Assets (PCAs) as applicable assets.

The supply chain revisions must be submitted for approval by May 22, 2027.

ADDITIONAL CIP ACTIVITY

CIP-002

CIP-008

CIP-014

CIP-015

CLOUD

CIP-002 BES CYBER SYSTEM CATEGORIZATION

- CIP-002-7 filed and is part of the virtualization update NOPR
- Project 2021-03 Phase One
  - CIP-002-8 filed and pending FERC action
    - Transmission Owner (TO)/Transmission Operator (TOP) Control Center categorization
- Project 2021-03 Phase Two in development
  - CIP-002/CIP-014 – Update IROL language
  - CIP-002 – Adjust TOP high impact categorization
  - CIP-002 – Explicitly identify Protected Cyber Assets (PCA), Electronic Access Control or Monitoring Systems (EACMS), and Physical Access Control Systems (PACS)

CIP-003/CIP-008 INCIDENT REPORTING AND RESPONSE PLANNING

- Project 2022-05 Modifications to CIP-008 Reporting Threshold
  - Response to FERC Order 848
  - In development – informal comment period open until 10/24
  - Add EACMS and PACS to CIP-008
  - Modify the reporting threshold for CIP-003 R2 Section 4 and for CIP-008

CIP-014 PHYSICAL SECURITY

- Project 2023-06 CIP-014 Risk Assessment Refinement
- In development
- Response to FERC Order in Docket RD23-2-000
- Reduce confusion around assessment and identification of critical substations

CIP-015 INTERNAL NETWORK SECURITY MONITORING

- Project 2025-02 Internal Network Security Monitoring Standard Revision
- In development
- Response to FERC Order 907
- Extend Internal Network Security Monitoring (INSM) to EACMS and PACS outside an Electronic Security Perimeter (ESP)

CLOUD

- Project 2023-09 Risk Management for Third-Party Cloud Services
- In development
- Industry initiated
- Enable, but not require, use of cloud services in various aspects of operations
- Working on a whitepaper to explain the team’s approach, expect to post for comment this year

REFERENCES

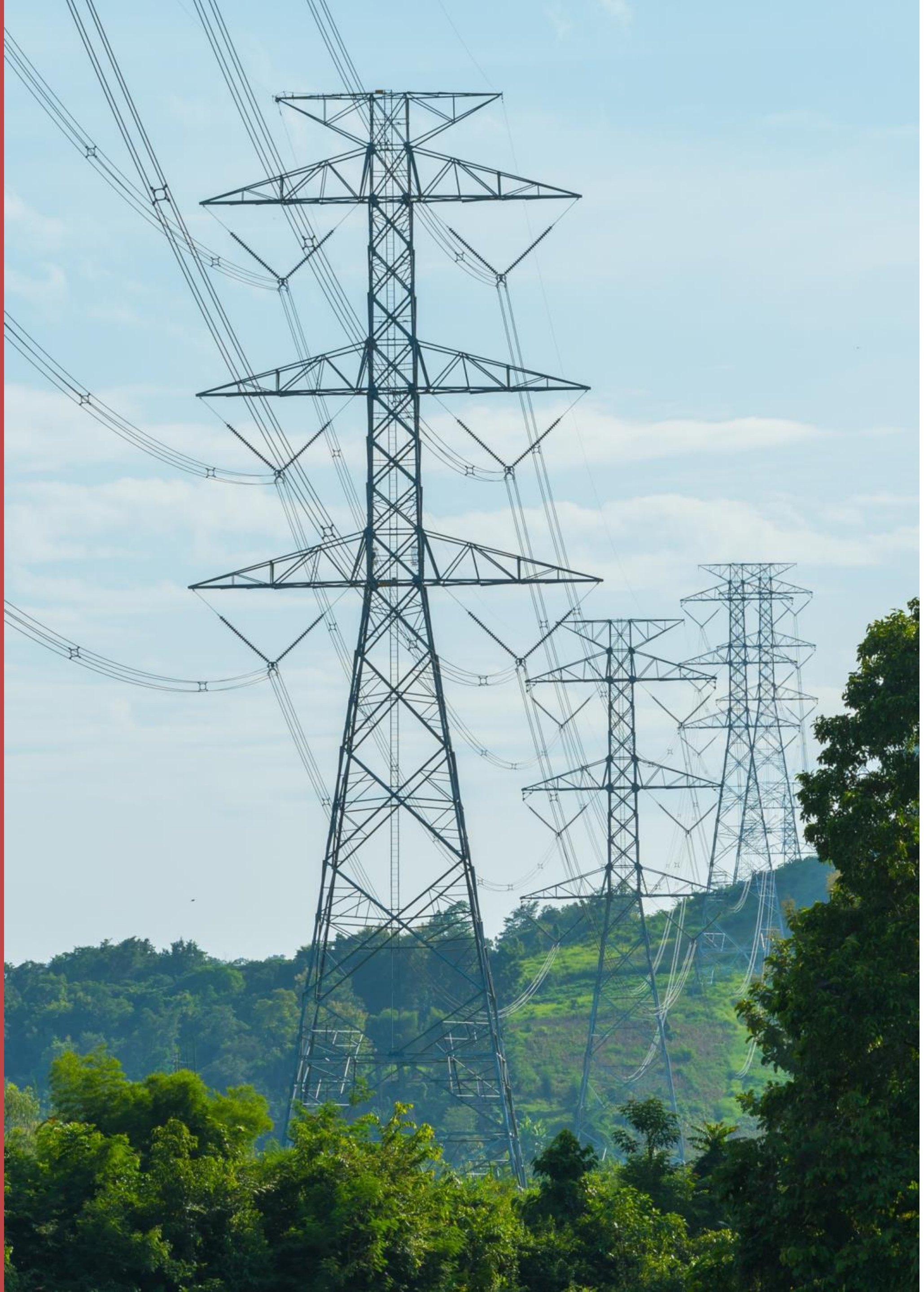
- NERC Standards Development Page - https://www.nerc.com/pa/Stand/Pages/Standards-Under-Development.aspx
- Project observer mailing lists
  - Link and instructions on each project's page (see next slide)
- FERC eLibrary - https://elibrary.ferc.gov/idmws/search/fercgensearch.asp
- FERC eSubscription - https://ferconline.ferc.gov/eSubscription.aspx
- FERC Meeting Notices – ferc.gov main page

REFERENCES

- Weekly NERC bulletins (NERC Info list)
  - Similar to project observers, ask to be added to the "NERC-info" list
- **TO SUBSCRIBE:** If you would like to be added to a NERC Distribution List, you must first register an account in the **ERO Portal**. Once you have registered your ERO Portal account, authenticated your credentials with DUO, and completed your profile, please submit a ticket through the **Help Desk** by selecting the "NERC Email Distribution List" option under the Applications menu. In the Description Box, please specify which lists you would like your email address to be added to. If you are unsure of which Distribution List you would like to be added to, an excellent starting point is the **Committees**. You can note the committee abbreviation, which represents the distribution list you would like to join, in the Description Box. If you have other NERC-related or specific Standards projects you're interested in, you may request those as well. If you're interested in general information, please request to be added to the NERC-info distribution list, which covers most NERC announcements.

LIMITED DISCLOSURE

FORWARD TOGETHER RELIABILITYFIRST

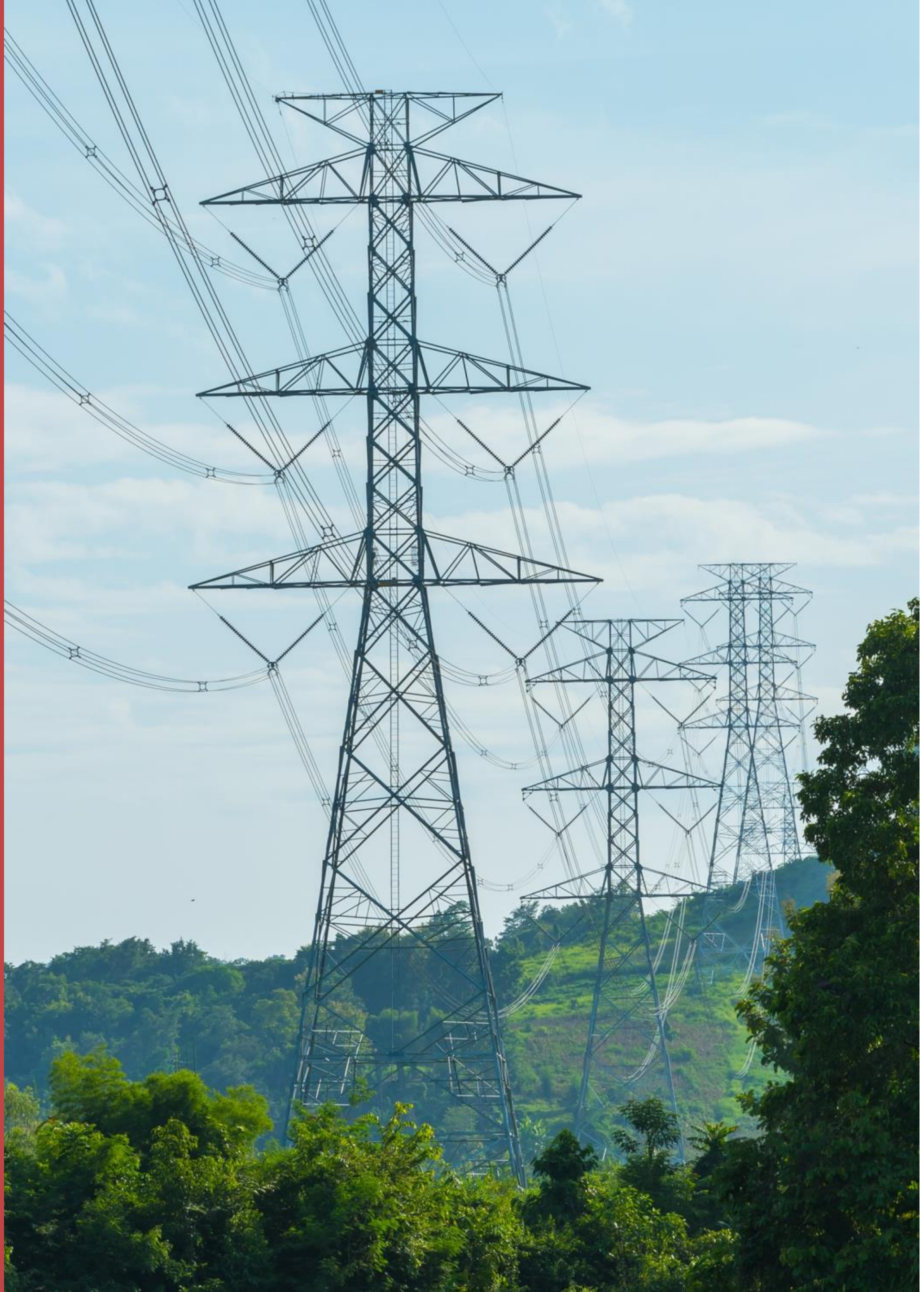


QUESTIONS & ANSWERS

Lew Folkerth

lew.folkerth@rfirst.org

FORWARD TOGETHER RF RELIABILITYFIRST



THANK YOU

Join us for our next Tech Talk – November 17th 2-3:30 pm EST

Webinar Link

Join the conversation at SLIDO.com

#TechTalkRF