WELCOME TO TECHNICAL TALK WITH RF

October 26, 2026

FORWARD TOGETHER RELIABILITYFIRST

TECHNICAL TALK WITH RF

FORWARD TOGETHER RF RELIABILITYFIRST

Join the conversation at

SLIDO.com

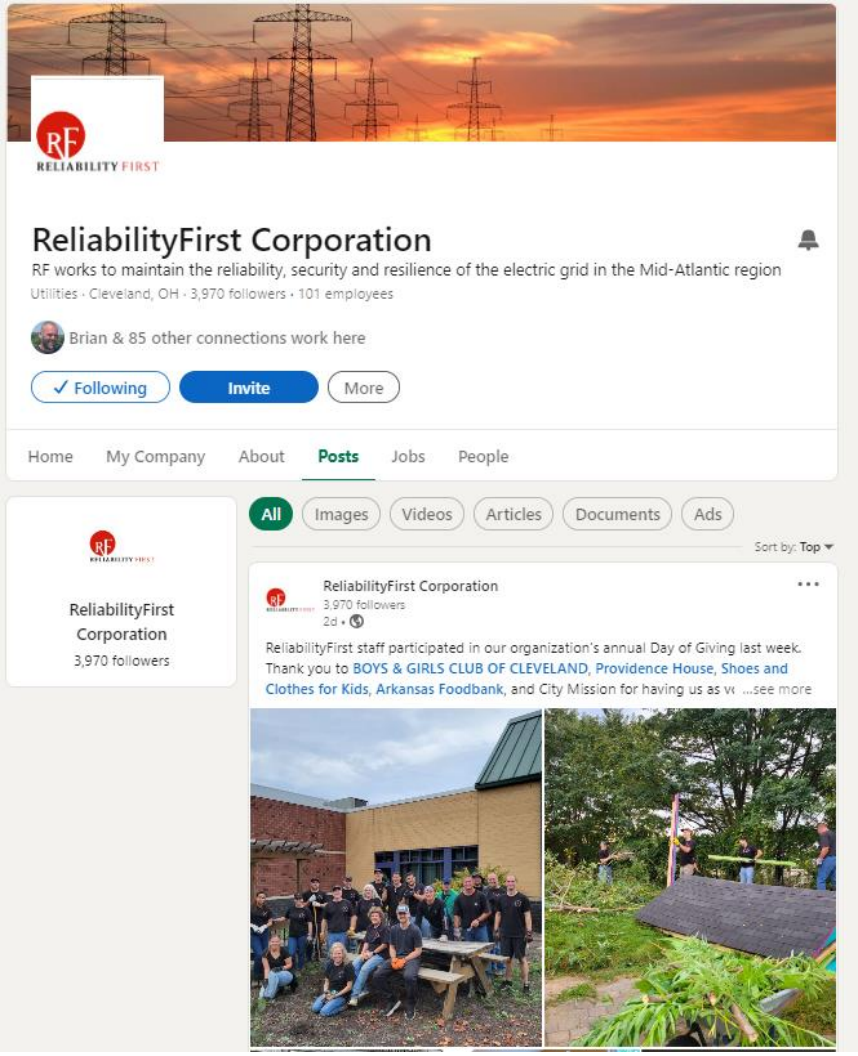
#TechTalkRF

TECHNICAL TALK WITH RF

Follow us on

LinkedIn

Linkedin.com/company/reliabilityfirst-corporation



FORWARD TOGETHER RELIABILITYFIRST

FORWARD TOGETHER RELIABILITYFIRST

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:
- 2026 ERO Periodic Data Submittal schedule
- Timing of Standard effectiveness

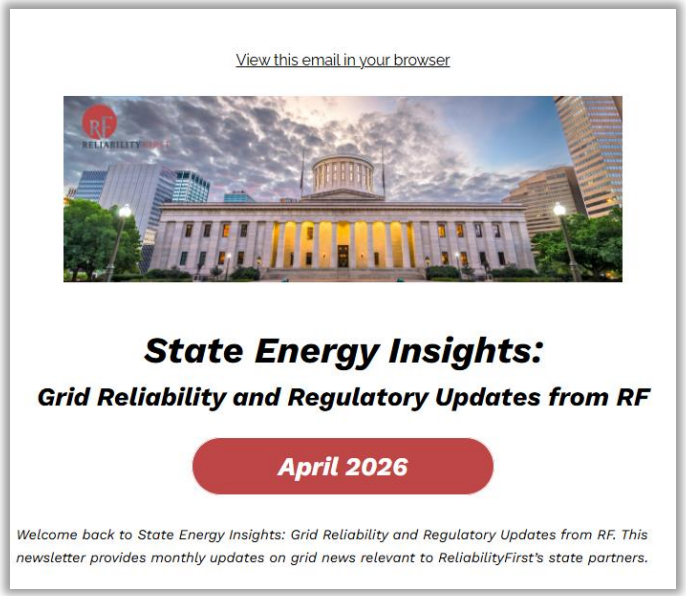
BES Cyber System Categorization (CIP-002-5.1a)
- Assess categorization (low, medium, or high) regularly and notify us of changes

CIP Evidence Request Tool V10.1 was released and is on NERC's website

TECH TALK REMINDER

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

- Sign up today **here**

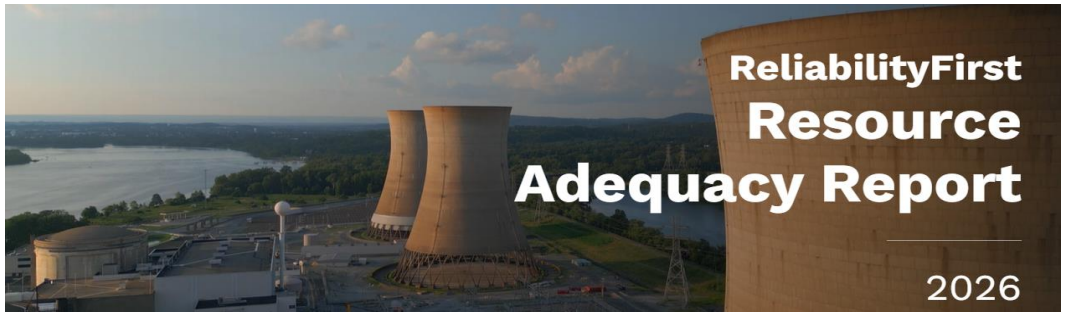


Make sure to check out our

2025 Impact Report and **video**

Visit our website to read RF's

2026 Resource Adequacy Report



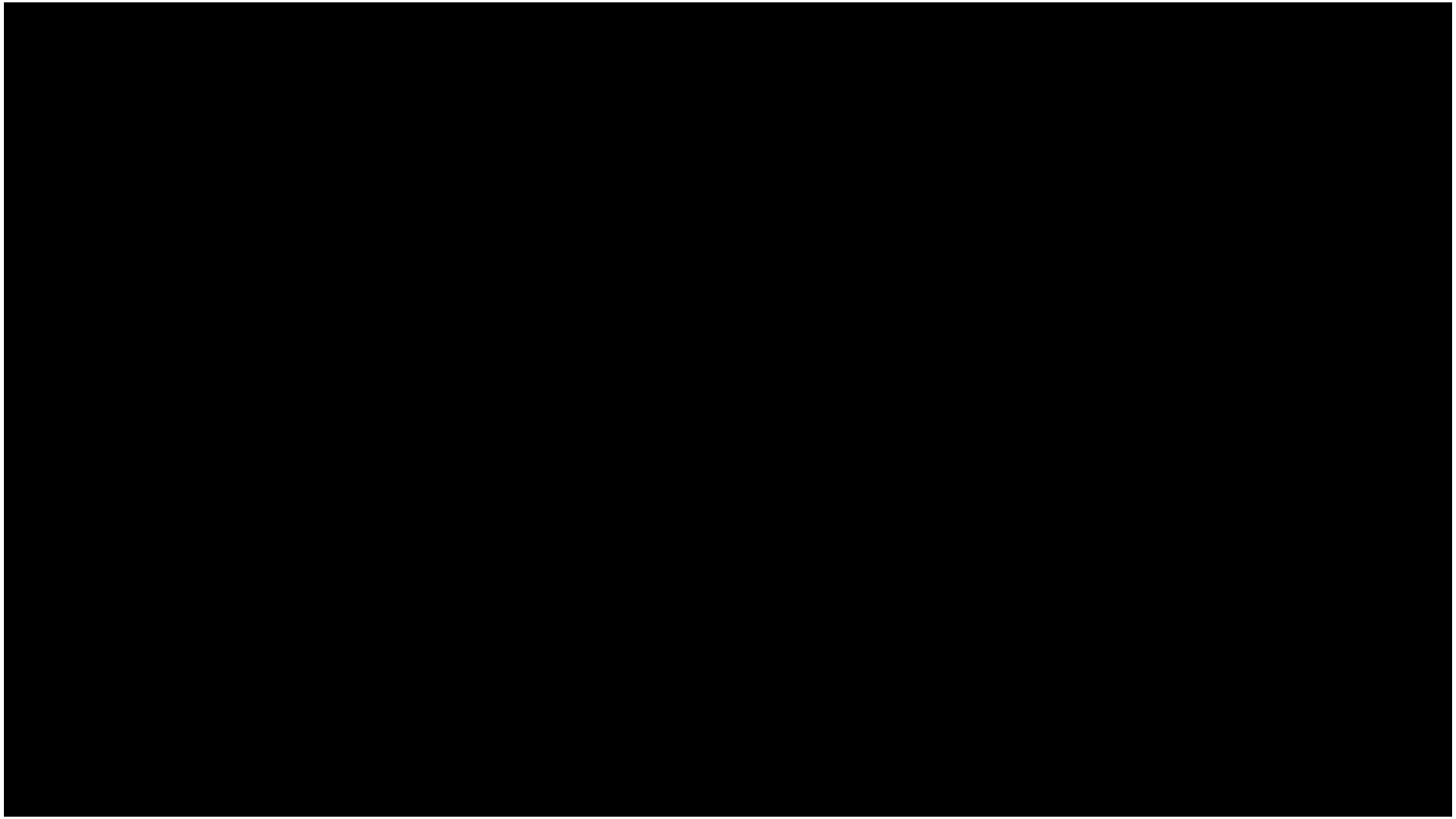
FORWARD TOGETHER RELIABILITYFIRST

FORWARD TOGETHER RELIABILITYFIRST

WELCOME TO TECHNICAL TALK WITH RF

October 26, 2026

THANK YOU FOR ATTENDING OUR 2026 FALL SUMMIT



https://youtu.be/5XjwyOdjnxI

FORWARD TOGETHER RELIABILITYFIRST

JOIN US FOR OUR 2027 FALL SUMMIT IN…

FORWARD TOGETHER RELIABILITYFIRST

TECH TALK ANNOUNCEMENT

NERC

NERC's Computational Loads Standards Pass Final Ballot, Advance to Board Adoption

NERC's foundational Computational Loads Reliability Standards and their associated implementation plans have passed final ballot, marking a significant milestone in an accelerated effort to address emerging reliability risks associated with the rapid growth of large electrical loads, including data centers and artificial intelligence facilities. The proposed standards will now be sent to the NERC Board of Trustees (Board) to request adoption. Once adopted by the Board, NERC will file the Reliability Standards for Project 2026-02 Computational Loads with the Federal Energy Regulatory Commission (FERC) for final regulatory approval in the United States.

Developed through extensive collaboration among NERC and Regional Entity staff, the electric industry, data center and cryptocurrency industry participants, technical experts, and other stakeholders, the proposed standards establish requirements to support the reliable integration of large computational loads into the bulk power system. They build on insights from NERC's Level 3 Essential Action Alert issued in May 2026, incident reviews, and the work of the Large Loads Working Group (LLWG).

For more information about NERC's ongoing work with large loads and opportunities for stakeholder engagement, visit the Large Loads Action Plan page and see the Q3 2026 Update.

FORWARD TOGETHER RELIABILITYFIRST

TECH TALK ANNOUNCEMENT

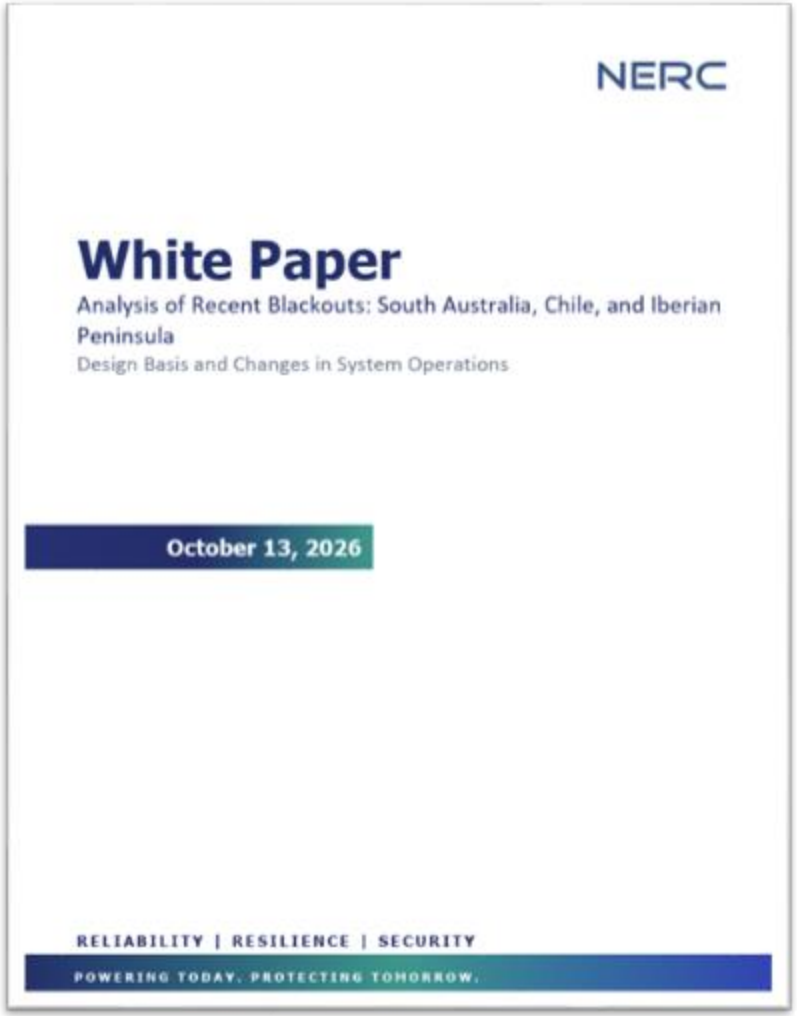
NERC

NERC Examines International Blackouts to Strengthen North American Grid Reliability

Full Announcement | White Paper

As electric grids worldwide undergo significant transformation, a new NERC white paper examines three major international blackouts and identifies critical lessons for strengthening the reliability and resilience of North America's bulk power system. The paper looks at events in South Australia (September 2016), Chile (February 2025), and Spain and Portugal (April 2025), highlighting common reliability challenges and recommending improvements to system design, planning, and operations.

The white paper underscores the importance of designing power systems that can adapt to changing operating conditions while maintaining the essential reliability services historically provided by synchronous generators. This includes strengthening system-wide planning and coordination, advancing modeling and real-time monitoring capabilities, and evaluating technologies that can provide fast-acting frequency and voltage support as the resource mix evolves.


NERC

White Paper

Analysis of Recent Blackouts: South Australia, Chile, and Iberian Peninsula

Design Basis and Changes in System Operations

October 13, 2026

RELIABILITY | RESILIENCE | SECURITY

POWERING TODAY. PROTECTING TOMORROW.

FORWARD TOGETHER RELIABILITYFIRST

TECH TALK ANNOUNCEMENT

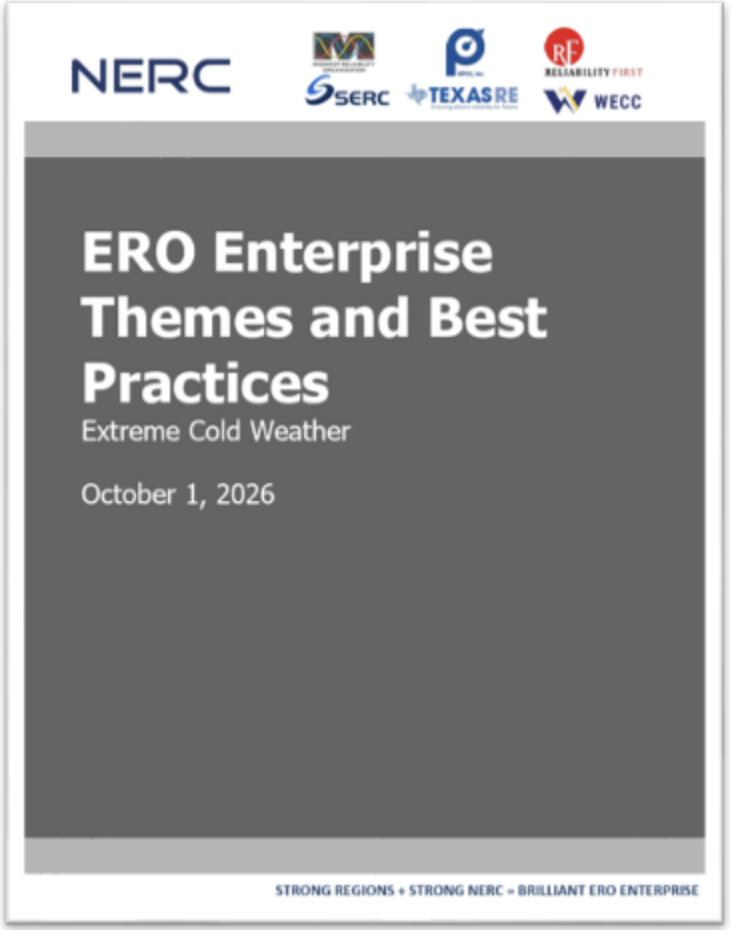
NERC

ERO Enterprise Themes and Best Practices Posted: Extreme Cold Weather

Full Report

The ERO Enterprise is actively engaged in identifying and addressing challenges associated with extreme cold weather preparedness. To support these efforts, the ERO Enterprise has published the Extreme Cold Weather Themes and Best Practices report, which compiles insights gathered through outreach, educational activities, discussions at Regional Entity and NERC technical committee meetings, and monitoring, enforcement, and mitigation activities.

The report highlights common themes and challenges that can affect a registered entity's ability to prepare for and respond to extreme cold weather events. In addition, it outlines best practices designed to address these identified challenges and support registered entities in strengthening the mitigation measures they are implementing to reduce the risks associated with extreme cold weather.



FORWARD TOGETHER RELIABILITYFIRST

TECH TALK ANNOUNCEMENT

GridExIX

GridEX IX Registration Is Live

Full Announcement | Registration Link

NERC's Electricity Information Sharing and Analysis Center (E-ISAC) is pleased to announce that GridEx IX Planner registration is open!

Conducted biennially by the E-ISAC, GridEx provides industry and government the opportunity to practice how they would respond to and recover from coordinated cyber and physical security threats to the grid. GridEx participation is open to E-ISAC members as well as relevant cross-sector, government, and vendor partners connected to the electric industry. Registrants will be vetted prior to confirmation, which may include a request for additional information.

GridEx IX will take place November 16-17, 2027. Visit our website to learn more.

Please contact Gridex@eisac.com with any questions.

FORWARD TOGETHER RELIABILITYFIRST

TECH TALK ANNOUNCEMENT

NERC

"Currently Compliant"

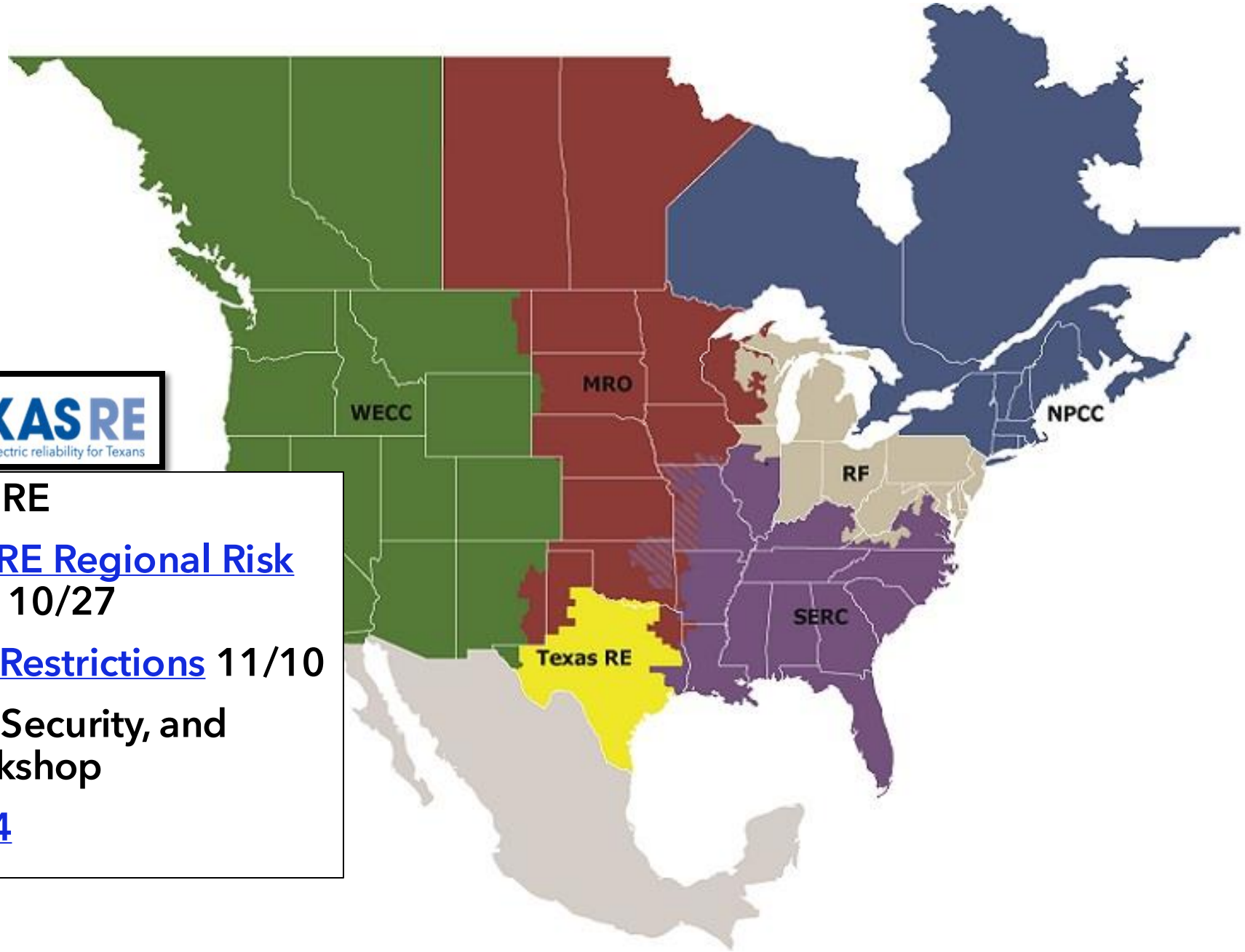
Full Announcement | Podcast

NERC released the eleventh and twelfth installments of its compliance podcast, "Currently Compliant."

Episode 11 reviews the phased implementation plans and requirements for PRC-028, PRC-029, and PRC-030—three standards that emphasize ride-through capabilities to ensure inverter-based resources (IBR) stay connected and support the grid during disturbances. Hosted by NERC Senior Compliance Assurance Engineer Ryan Mauldin and featuring insights from subject matter experts Curtis Crews, principal engineer at Western Electricity Coordinating Council; James McGrane, senior counsel at NERC; and Beth Rettig, senior technical auditor at ReliabilityFirst, this episode outlines the timelines and expectations for these critical standards.

Episode 12 follows up on FERC Order 919 approving the CIP Virtualization Standards from Project 2016-02. This episode takes a closer look at the early adoption details and how entities can access additional resources. It is hosted by NERC Compliance Assurance Manager Holly Peterson-Rowe and features insights from subject matter experts Gabriela Barragan, CIP cyber and physical security analyst at TexasRE; Udhay Ganesan, principal risk assessment and mitigation engineer at Midwest Reliability Organization; Chris Lewis, technical auditor at ReliabilityFirst; and James McGrane, senior counsel at NERC.

FORWARD TOGETHER RELIABILITYFIRST



TEXAS RE
Ensuring electric reliability for Texans

Talk with Texas RE

- 2026 Texas RE Regional Risk Assessment 10/27
- Gas Supply Restrictions 11/10

Fall Standards, Security, and Reliability Workshop

- November 4

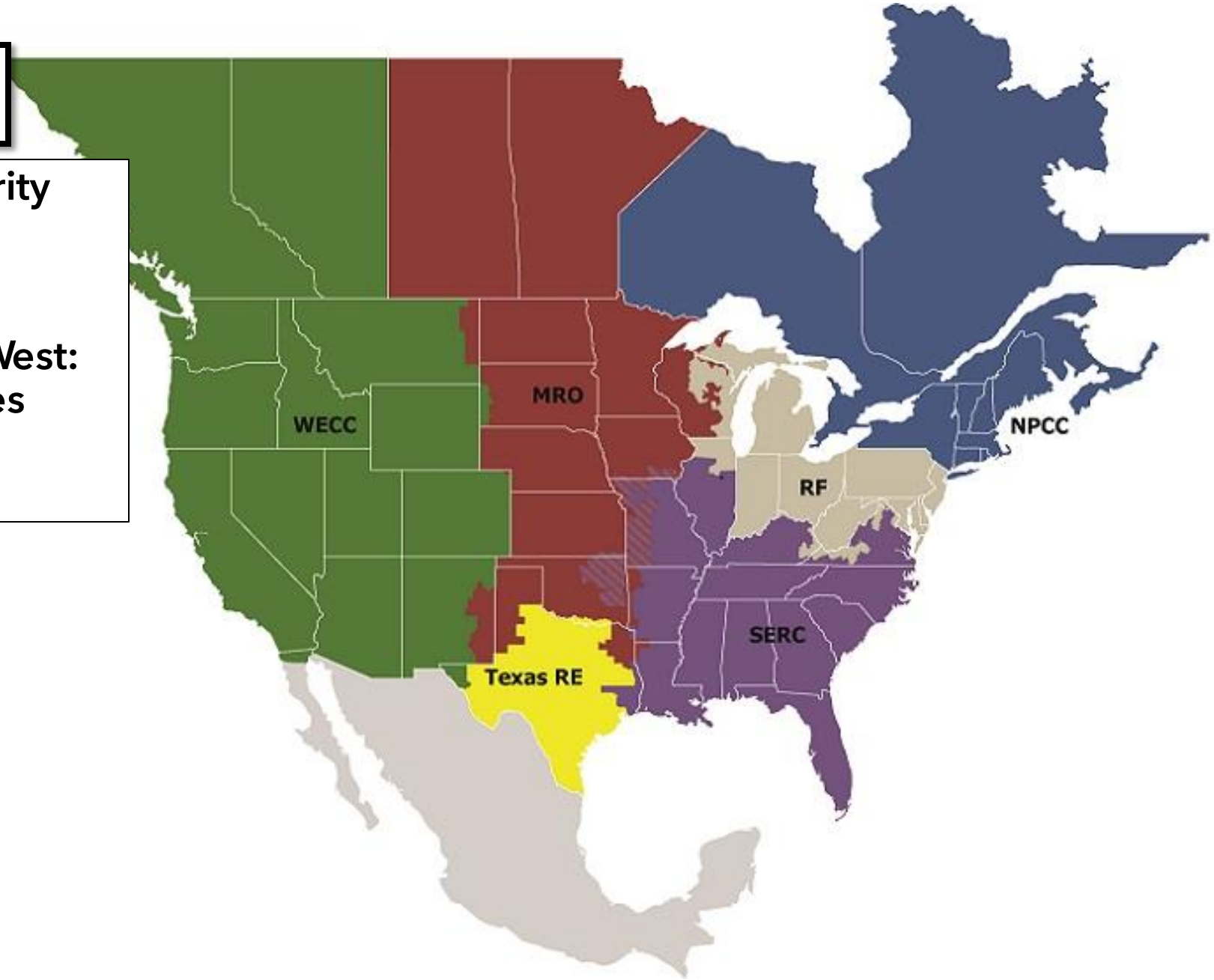
WECC

Reliability & Security Oversight Update

- November 19

Reliability in the West: A Discussion Series

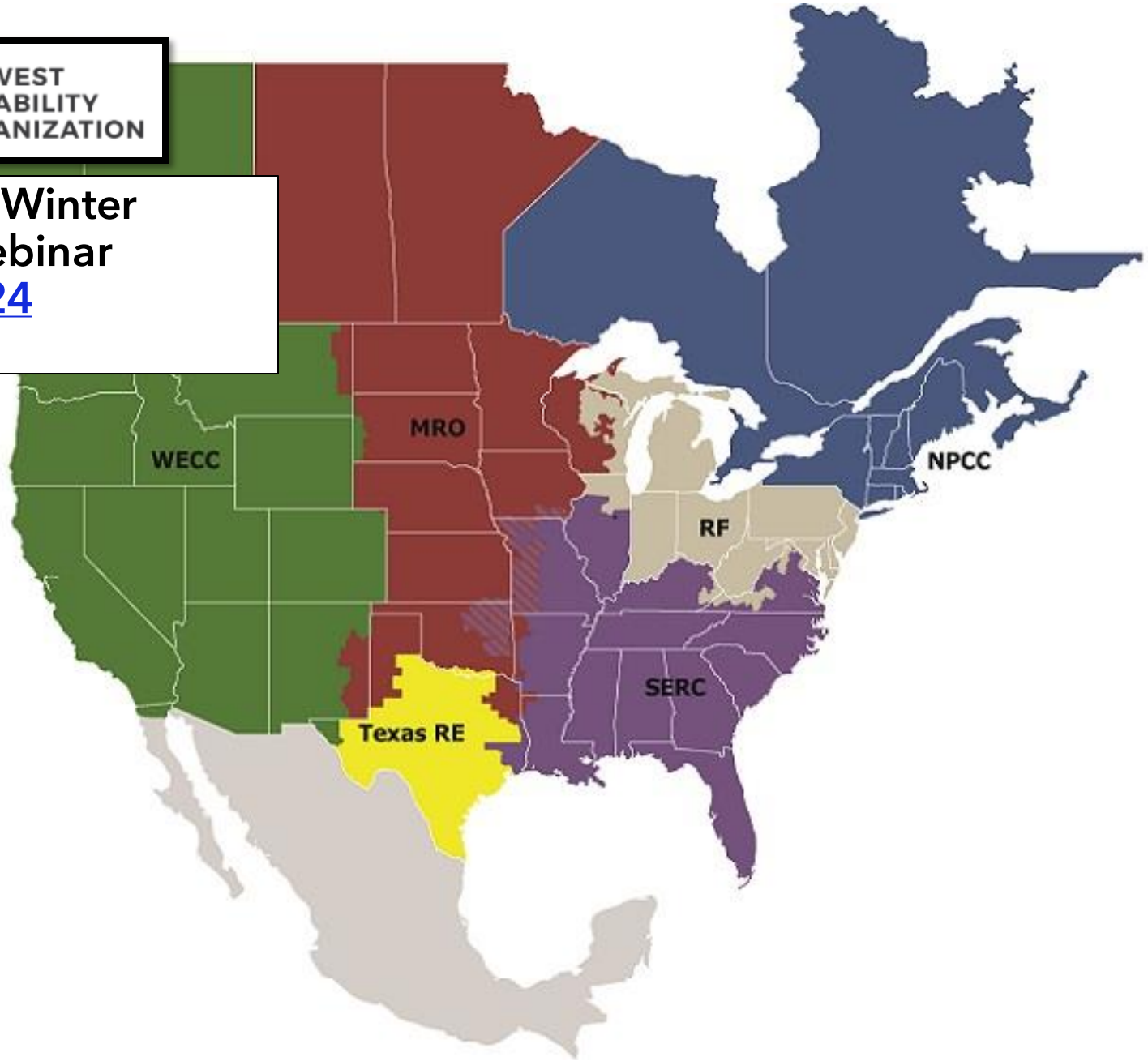
- November 4

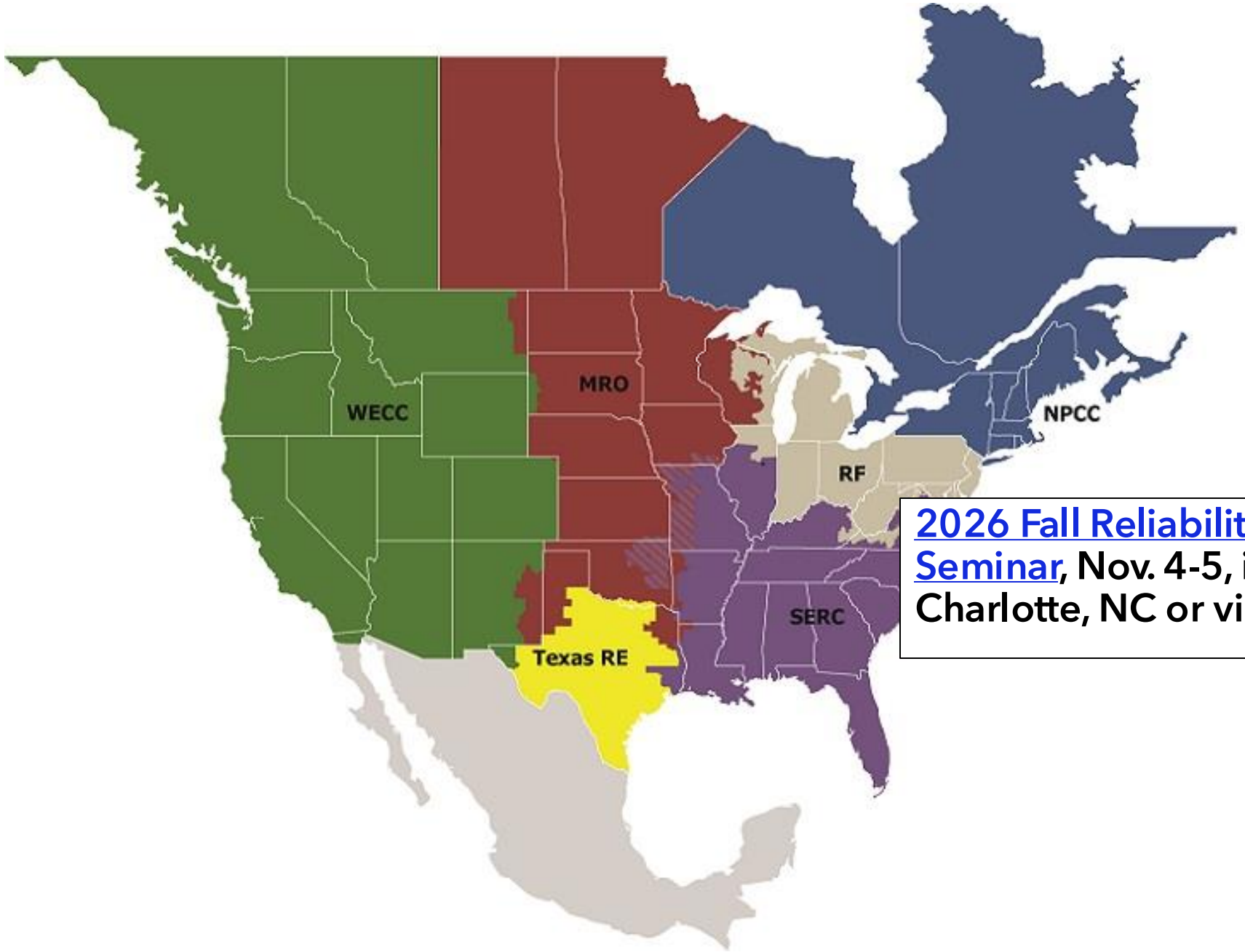


MIDWEST RELIABILITY ORGANIZATION

2026 Regional Winter Assessment Webinar

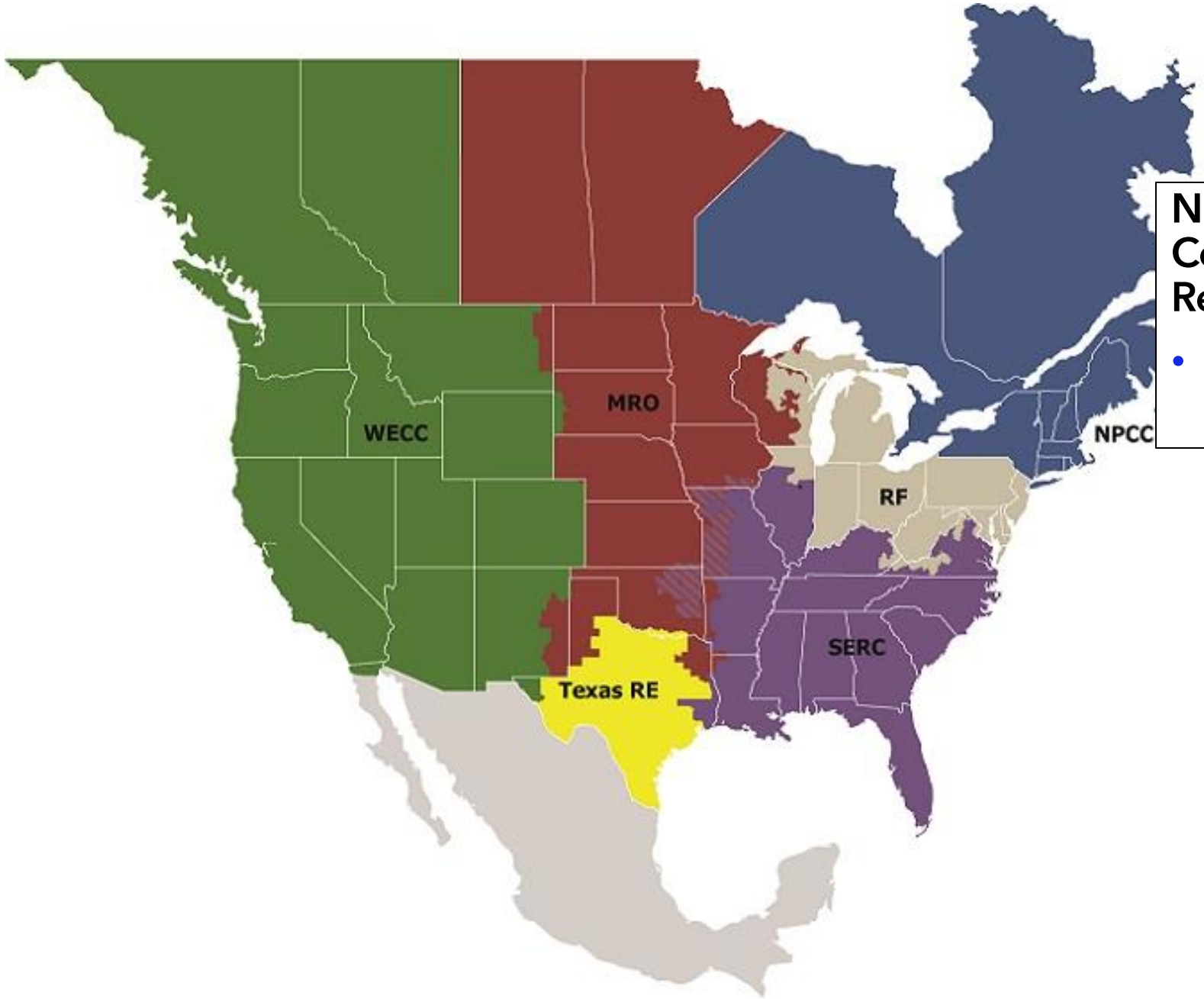
- November 24





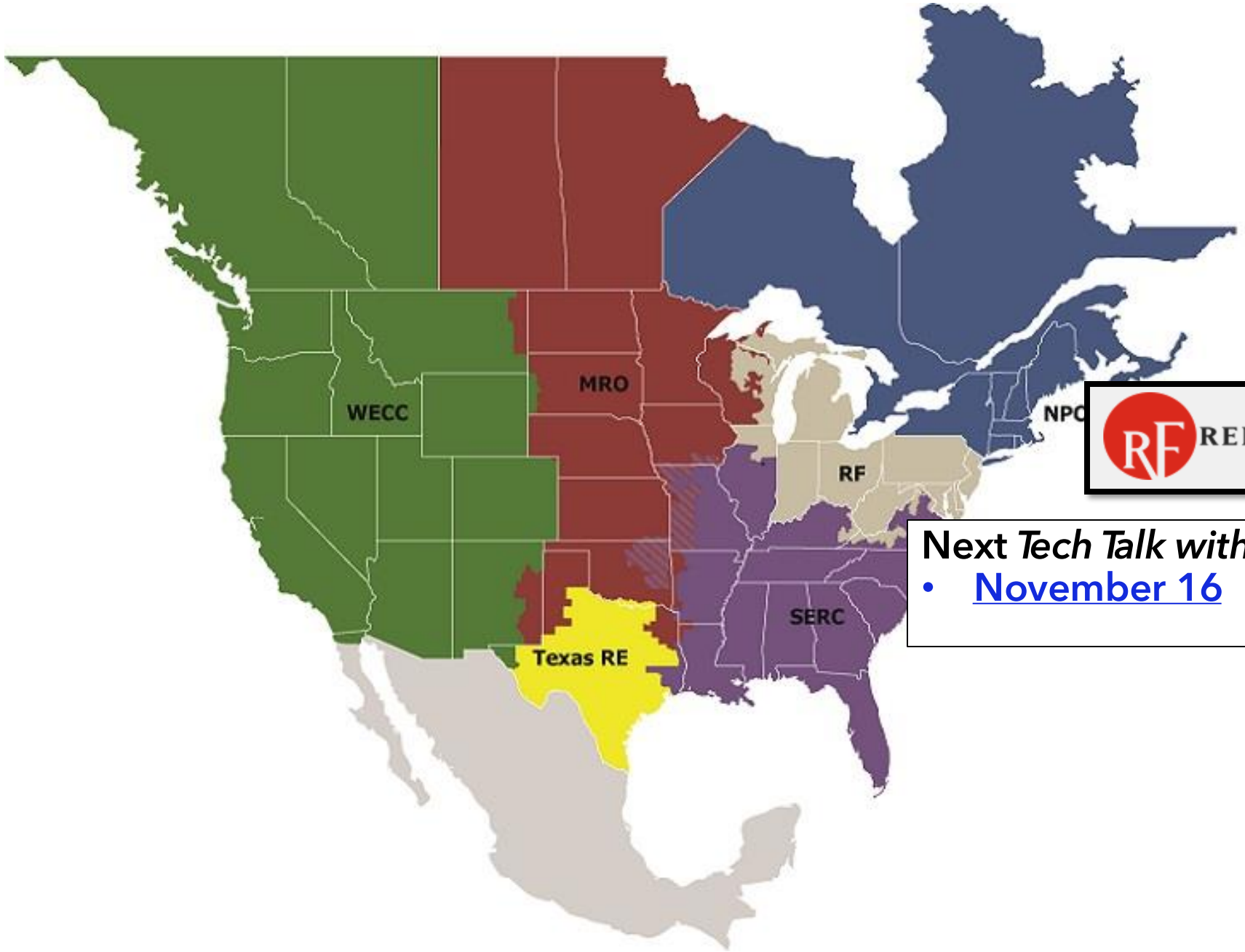
SERC Reliability Corporation

[2026 Fall Reliability & Security Seminar](), Nov. 4-5, in-person in Charlotte, NC or virtually



NPCC 2026 Fall Compliance and Reliability Conference

- November 4-5, register early!



RELIABILITYFIRST

Next *Tech Talk with RF*

- November 16

TECH TALK REMINDER

FORWARD TOGETHER RELIABILITYFIRST

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

CLICK HERE

MON
26

October 26, 2026 @ 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.

TECH TALK WITH RELIABILITY FIRST

TECHNICAL TALK WITH RF

FORWARD TOGETHER RF RELIABILITYFIRST

Join the conversation at

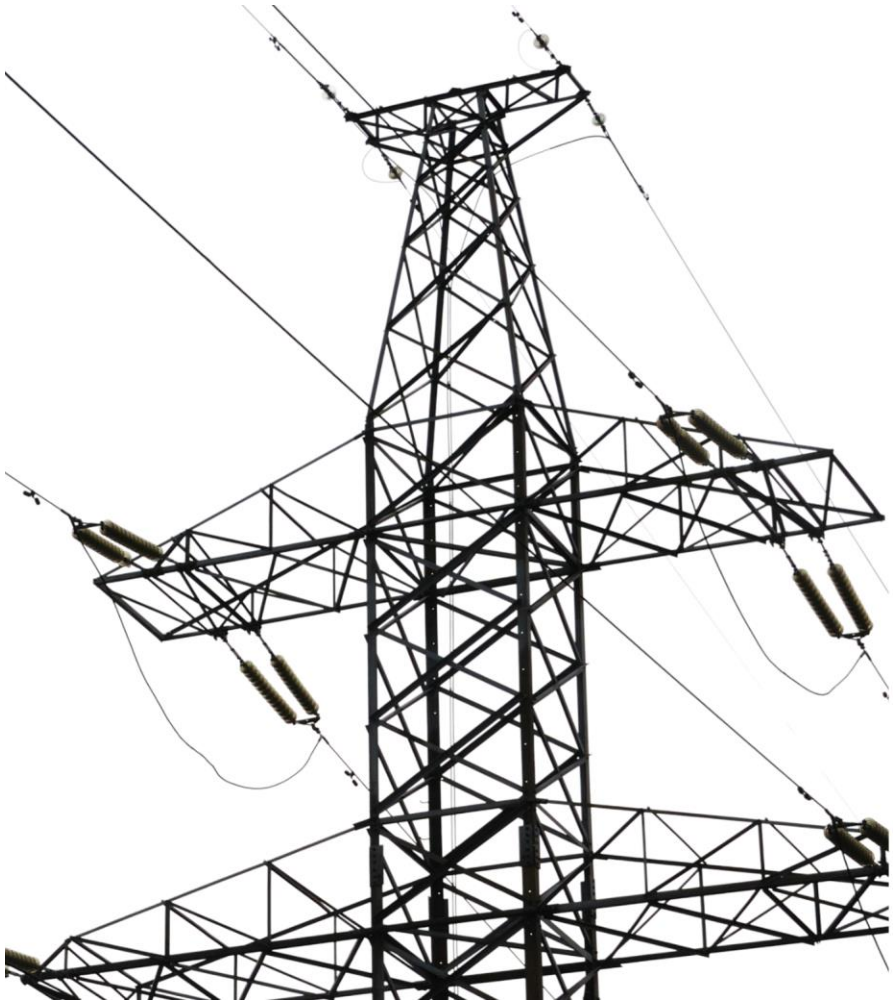
SLIDO.com

#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.



FORWARD TOGETHER RELIABILITYFIRST

FORWARD TOGETHER RELIABILITYFIRST

AGENDA

SUPPLY CHAIN BULK POWER SYSTEM IMPACTS FROM EXECUTIVE ORDER 14421

PATRICK MILLER, PRESIDENT AND CEO, AMPYX CYBER

HOW CYBER DECOYS CAN STRENGTHEN DETECTION AND RESPONSE

RON ROSS, SENIOR RELIABILITY CONSULTANT, ENTITY ENGAGEMENT, RELIABILITYFIRST

DAVID SOPATA, PRINCIPAL RELIABILITY CONSULTANT, ENTITY ENGAGEMENT, RELIABILITYFIRST

SUPPLY CHAIN BULK POWER SYSTEM IMPACTS FROM EXECUTIVE ORDER 14421

WHAT IT REACHES, WHAT IT REQUIRES, AND WHAT IT DOESN'T CHANGE

Patrick C. Miller

- More than 35 years in electric power across North America, South America, and Europe
- CIPC, GCIP, CISA, CRISC, CISSP-ISSAP, SSCP, NSA-IAM, CVI, TCP, SCP
- Former utility staff (electric, water, and telecommunications sectors)
- One of the original architects of NERC CIP standards
- First NERC CIP auditor in the US
- Former Manager, CIP Audits and Investigations, WECC
- Current NERC SCWG, SITES, and SPIDERWG contributor
- Speaker/contributor to multiple FERC Technical Committees, NOPRs and Orders
- Contributing author for DHS CISA Cross-Sector Cyber Performance Goals (CPGs)
- Contributing author for NARUC/DOE Cybersecurity Baselines for Electric Distribution
- Expert Witness: US-China Economic and Security Review Commission (US Congress, 2025)
- Advisor, Senate 119th Congress, 2nd Session: Bill - Quantum Grid Utility Assurance and Resilient Defense Act of 2026
- Former Principal Investigator, US Department of Energy, National Electric Sector Cybersecurity Organization
- Cybersecurity Advisory Team for State Solar, NARUC/NASEO
- INL and NTIA Software Bill of Materials (SBOM) Energy POC Stakeholders
- DOE SETO and NREL/NLR Industry Advisory Board for the Securing Solar for the Grid (S2G)
- EnergySec Founder, Former CEO, Director/Chair, Instructor, and President Emeritus
- US Coordinator, Professor, Centro de Ciberseguridad Industrial (CCI; Madrid/LATAM)
- Instructor, Cyber Information Security Leader (CISL; Copenhagen)
- Former SANS ICS456 Instructor: Essentials for NERC Critical Infrastructure Protection
- Control System Cyber Security Association International (CS2AI) Global Senior Fellow
- Program Committee for multiple prominent security conferences (RSAC, LevelZero, ISC CPH, CCI Congress, CyberTek)
- Global advisor to multiple industrial hardware/software vendors, boards of directors, & government agencies

Upon making the determinations described in subsection (a) ..., the Secretary ... may impose conditions on the continued use, operation, maintenance, servicing, or updating of foreign manufactured or operated bulk-power system electric equipment acquired or installed before the date of this order, including requirements to identify, isolate, monitor, secure, disconnect, replace, or remove such equipment.

EO 14421, Sec. 2(b), 91 FR 55995

BEFORE WE START

- Not a NERC Reliability Standard
- No change to your BES footprint or your CIP obligations
- Not, by itself, a ban
- It does reach equipment you own today, including some outside your CIP asset list

THE ORDER

- Executive Order 14421, Declaring a National Emergency to Secure the United States Bulk-Power System
- Signed August 26, 2026, published at 91 FR 55995 on August 31
- Authority is the International Emergency Economic Powers Act (IEEPA) and the National Emergencies Act (NEA), not the Federal Power Act
- Defines the bulk-power system for its own purposes, including transmission rated 69 kV and above, local distribution excluded (Sec. 5(a))
- A prohibition needs two findings, a Covered Foreign Entity nexus plus undue or unacceptable risk (Sec. 2(a))
- Covered Foreign Entity is defined by reference to the ITAR country list at 22 C.F.R. 126.1, plus countries the Secretary designates (Sec. 5(e))

SAME WORDS DIFFERENT LINE

Line	Source	How it's drawn	What it decides
Transmission vs. local distribution	FPA Sec. 201(b)(1), 16 U.S.C. 824(b)(1); FERC Order No. 888 seven-factor test (1996)	By function, not voltage	Federal vs. state jurisdiction over rates and service
Bulk-power system	FPA Sec. 215(a)(1), 16 U.S.C. 824o(a)(1)	By function, no voltage; local distribution excluded	Outer limit of ERO authority (Sec. 215(i))
Bulk Electric System	NERC Glossary; FERC Orders No. 743 (2010) and 773 (2012)	100 kV bright line, plus inclusions and exclusions	Where Reliability Standards, CIP included, apply
EO 14421 bulk-power system	EO 14421 Sec. 5(a), 91 FR 55995	Adapted from FPA 215 (“electric” for “transmission”), plus 69 kV+ transmission; local distribution excluded	What the prohibition and Sec. 2(b) conditions can reach

WHERE THE LINES FALL

- 100 kV is NERC's BES threshold, not a statutory or jurisdictional boundary
- In December 2015 FERC found most of nearly 2,500 circuit miles of one utility's 115 kV system to be local distribution, serving about 19 percent of its peak load
- The BES can reach below 100 kV through its inclusions, and exclude radials and local networks above it
- Under the order, a 69 kV line operated as transmission is in scope, and a line found to be local distribution is presumably out
- Not yet answered, who makes the local distribution call for the order, DOE on its own or by reference to FERC's record

WHERE WE ARE

Date	Event
May 1, 2020	EO 13920, the first version; suspended Jan 2021 and not renewed; its one prohibition order revoked Apr 2021; no rules
Aug 26, 2026	EO 14421 signed
Sep 9, 2026	DOE request for information (RFI), 91 FR 57322
Sep 16, 2026	DOE informational webinar
Oct 6, 2026	DOE FAQ updated
Oct 9, 2026	RFI comments closed
Dec 24, 2026	Implementing rules due, "as needed" (Sec. 3(b))
Feb 22, 2027	Federal Acquisition Regulation (FAR) recommendations due (Sec. 4)
Aug 26, 2027	Emergency ends unless a continuation notice is published

WHAT IS IN SCOPE

- Classic bulk-power iron, transformers, breakers, capacitor banks, generation
- Grid-connected inverters and battery energy storage
- Control gear, RTUs, PLCs, IEDs
- The software, firmware and services attached to all of it
- Remote-access capability tied to a Covered Foreign Entity
- DOE's 2024 BESS report estimates 90 to 100 percent of BESS contain at least one PRC-sourced component

THREE GATES

Gate 1: Is it foreign-produced BPS equipment?	Gate 2: Is there a covered transaction?	Gate 3: Are both findings made?
On the Sec. 5(b) list and not made, produced or assembled in the US (Sec. 5(c)). Includes 69 kV+ transmission; local distribution excluded at any voltage (Sec. 5(a)).	Initiated after August 26, 2026, and "initiated" isn't defined. Installed equipment is reached through Sec. 2(b) conditions and Sec. 3(a), after the same findings.	A Covered Foreign Entity nexus plus undue or unacceptable risk (Sec. 2(a)). Required for installed equipment too.

Note: The order says the definition "includes" 69 kV lines; it never says below 69 kV is excluded. Most people read 69 kV as a floor, but DOE has not confirmed.

NOTHING GRANDFATHERED

- Section 2(a), the prohibition, looks forward. It can bar transactions initiated after August 26, 2026
- Sec. 2(b) looks back. Once the same findings are made, it reaches equipment acquired or installed before August 26, 2026
- Conditions can run from identify and monitor to disconnect and remove
- Before directing isolation or removal, the Secretary must consider reliability, safety, availability of secure replacements and continuity of service, and may phase compliance
  - Power transformer lead time, about 128 weeks; generator step-up, about 144 (Wood Mackenzie, Q2 2025)
- The prohibitions apply notwithstanding contracts, licenses or permits that predate the order (Sec. 2(d))

SIDE BY SIDE

	EO 14421	CIP-013-2	CIP-003-9 Att. 1, Sec. 6
Threshold	Sec. 5(b) equipment in the order's BPS, incl. 69 kV+ transmission	High and medium impact BCS, plus EACMS and PACS	Assets containing low impact BCS
Covers	Equipment, components, software, firmware, services, remote access	Procurement and installation planning	Vendor electronic remote access
Requires	Prohibition or conditions	A documented plan and risk assessment	Determine, disable, detect
Trigger	Transaction initiated after Aug. 26, plus a Covered Foreign Entity nexus and a risk finding	Procurement	Presence of vendor remote access

NOT COVERED BY CIP-013

- None of CIP-013-2 R1.2's six processes asks who owns or controls the manufacturer, or where it was built
- R1.2.5 comes closest, and it only verifies that vendor software and patches are authentic and unaltered
- Primary equipment (transformers, breakers, capacitor banks) isn't a Cyber Asset, so most of the order's equipment list has no CIP-013 counterpart
- CIP-013-4 Draft 1 (Project 2025-06) drew 30.64 percent weighted approval against a two-thirds threshold, with roughly 90 percent quorum
- DOE says CIP compliance is not an exemption from the order (DOE FAQ Q13, Q20)

WHAT WE ALREADY BUILT

- CIP-003-9, effective April 1, 2026, added vendor electronic remote access controls at low impact
- Whatever list you keep for Section 6 is organized by who has access
- The order would want it sorted by who owns the manufacturer
- In my experience, most entities have the first list but not the second

WHAT THIS ORDER DOESN'T GIVE

- No dedicated cost recovery mechanism for what DOE requires
- No protection if complying with DOE puts you in conflict with CIP; DOE says compliance with one doesn't excuse the other (DOE FAQ Q20)
- Not complying with the order itself, a civil penalty of the greater of $377,700 or twice the transaction value, criminal penalties for willful violations

Your CIP obligations stay fully enforceable through RF and NERC under FPA Section 215, whatever DOE does under this order.

Section 215A is not Section 215. FPA Section 215 (16 U.S.C. 824o) gives us the ERO, Reliability Standards and CIP.

FPA Section 215A (16 U.S.C. 824o-1), added by the FAST Act in 2015, gives DOE emergency order authority after a Presidential grid security emergency declaration.

EO 14421 uses neither; it runs on IEEPA

WHAT DOE ASKED VIA RFI

RFI, 91 FR 57322, 36 questions in eight areas

- A-5, what counts as manufactured in the United States (final assembly, substantial transformation, contract manufacturing, white-labeling)
- B-2, how far into sub-tier suppliers provenance can reasonably be traced
- B-5, what software, firmware and hardware bill-of-materials capability actually exists
- D-1, what data fields asset owners maintain today
- G-6 and G-7, burden on small entities, rates, cooperatives and public power
- Section E, licensing and mitigation, has one question; every other section has three to seven

DOE's 4 STAGES (W/ CAVEAT)

Stage 1	Stage 2	Stage 3	Stage 4
Inventory, manufacturer, model, production facility, firmware, connectivity, support status, lead time	Analyze, origin, ownership, remote access, reliability, safety, replacement availability	Mitigate, isolation and monitoring through disconnection, replacement and vendor change	Verify, reporting, testing, inspection, attestation, recordkeeping

Caveat: This is how DOE organized its RFI questions. It is not an adopted methodology. It may preview the eventual approach, since it tracks the order's own Sec. 2(b) language, but DOE has not directly stated this.

DOE SIGNALS SO FAR

- No determination from the nameplate; brand name and headquarters location alone don't establish design, origin, ownership or control (DOE FAQ Q12; webinar)
- Preserve the facts on deals in motion, timing, milestones, equipment status, dependencies, replacement options, possible mitigation (webinar)
- The order authorizes mitigation agreements (Sec. 2(c)), licensing (Sec. 3(b)) and phased compliance (Sec. 2(b)), none adopted yet; the RFI decides no individual transaction
- Prequalification of equipment and vendors is authorized, with the Secretary's authority preserved regardless; no deadline set (Sec. 2(e); DOE FAQ Q14)

DOE FAQ (UPDATED OCT. 6)

- Behind-the-meter and data center equipment (generators, BESS, UPS) isn't automatically excluded by location (Q5)
- "Initiated" is still undefined; candidates include contract signature, manufacture, shipment, delivery, title transfer and installation (Q8)
- Installed equipment isn't prohibited or subject to removal until the determinations and consultations are complete (Q9)
- No domestic-content threshold, substantial-transformation test or US final-assembly rule yet (Q11)
- CIP compliance isn't an exemption, but NERC evidence such as asset determinations, reliability studies and supply-chain controls may support DOE's analysis (Q20)

Guidance only; it creates no legal requirements, and DOE may update it

WHO EXECUTES IT?

- RFI question H-3 asks whether industry standards, third-party labs and certification bodies could carry implementation and limit the government's initial role
- The ERO model is our sector's working example of delegated federal authority, but it lives in FPA Section 215
- IEEPA has no ERO provision and no certification mechanism
- FCC Covered List precedent, government keeps the list and the determination, private certification bodies and labs execute beneath it
- FCC added foreign-produced power inverters to the Covered List on July 28, 2026, narrowed August 20; applies to new models only

WHAT TO WATCH

- December 24, whether DOE publishes rules, an order, or nothing "as needed"
- A Covered Foreign Entity list or residual Secretary determinations
- How "initiated" gets defined for transactions after August 26
- Updates to DOE's FAQ, where interim guidance may show up before any rule
- The 130+ filed RFI responses, especially on D-1, A-5 and H-3
- CIP-013-4 Draft 2 and whether it moves toward the ownership question
- ITAR 126.1 changes, which move on foreign-policy shifts
- February 22, 2027 FAR recommendations, and August 26, 2027 continuation

THINGS YOU CAN DO NOW

- Extend the equipment inventory beyond the CIP asset list to every Sec. 5(b) item in 69 kV+ substations, control rooms and generating stations
- Record country of manufacture, country of design and controlling parent as three separate fields
- Re-sort your CIP-003-9 Section 6 vendor remote access list by manufacturer ownership
- Record contract, shipment, delivery, title and installation dates for every pending procurement, with evidence
- Pull change-in-law, force majeure and assignment clauses from open supply agreements; same for insurance policies
- Walk a forced relay or RTU replacement through CIP change management to look for process improvement opportunities

CONTACT

Patrick C. Miller – President & CEO, AMPYX CYBER

- Email pmiller@ampyxcyber.com
- LinkedIn https://www.linkedin.com/in/millerpatrickc/
- All other socials @patrickcmiller
- Signal/WA @patrickcmiller.01

Ampyx Cyber Blog

- https://ampyxcyber.com/blog

FORWARD TOGETHER RELIABILITYFIRST

CYBER DECOYS TO STRENGTHEN DETECTION AND RESPONSE

David Sopata, Principal Reliability Consultant

Ron Ross, Principal Reliability Consultant

Entity Engagement

October 26, 2026

FORWARD TOGETHER RELIABILITYFIRST

CYBER DECOYS

- WHAT ARE THEY?
- HOW ARE THEY USED?
- FRAMEWORKS AND ARCHITECTURE
- HOW DO THEY FIT INTO A CIP-015 PROGRAM?
- CAVEATS IN IMPLEMENTING IN A CIP-015 PROGRAM

HOW HAVE DECOYS BEEN USED IN THE PAST?

During World War II, Allied forces used inflatable dummy tanks and fake paratroopers as tactical deception tools to trick the Axis powers about troop locations and invasion timing.

By Unknown author or not provided - U.S. National Archives and Records Administration, Public Domain, https://commons.wikimedia.org/w/index.php?curid=17161127

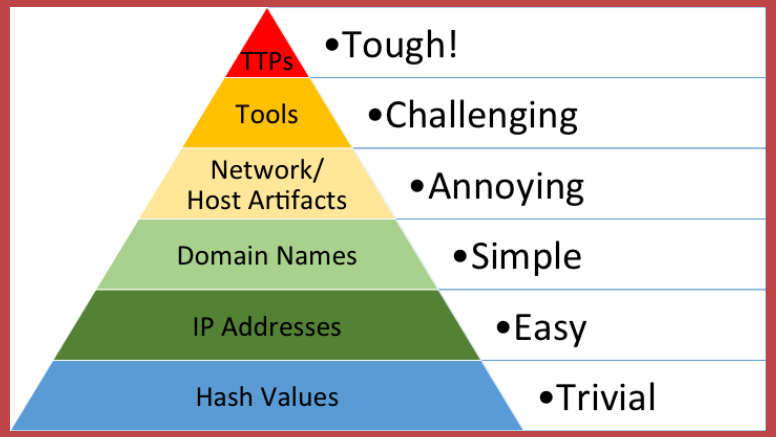
By Murray (Lieut), No 1 Army Film & Photographic Unit - http://media.iwm.org.uk/iwm/mediaLib//46/media-46653/large.jpg This photograph E 8361 comes from the collections of the Imperial War Museums., Public Domain, https://commons.wikimedia.org/w/index.php?curid=25310748

By user: Pajx - Own work, Public Domain, https://commons.wikimedia.org/w/index.php?curid=1003565

Tactics like these helped the Allies trick the Germans into thinking the D-Day invasion would happen at Pas de Calais instead of Normandy.

FORWARD TOGETHER RF RELIABILITYFIRST

Pyramid of Pain (for the Intruder/Attacker/Advisory)



- Source: https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html
- Learn more: https://www.sans.org/tools/the-pyramid-of-pain

WHAT ARE CYBER DECOYS?

According to a new resource from CISA, "*Using Cyber Decoys to Strengthen Detection and Response,*" cyber decoys are fake digital assets like servers, databases, file shares and credentials designed to:

- trick attackers into spending resources, exposing tools used;
- detect intrusions early;
- gather threat intelligence that could be shared with others;
- make the attacker second guess the environment they are in or the information they acquired;
- make your organization a less desirable target;
- provide an accurate detection rate with a high signal-to-noise ratio.

Cyber decoys are typically deployed in zero-trust environments. Zero trust assumes no user, device, application, or network segment is trusted and instead requires continuous verification of access and activity.

https://www.cisa.gov/resources-tools/resources/using-cyber-decoys-strengthen-detection-and-response

AI-generated concept art using Microsoft Copilot.

CYBER DECOY BASICS

Decoys (or Lures):

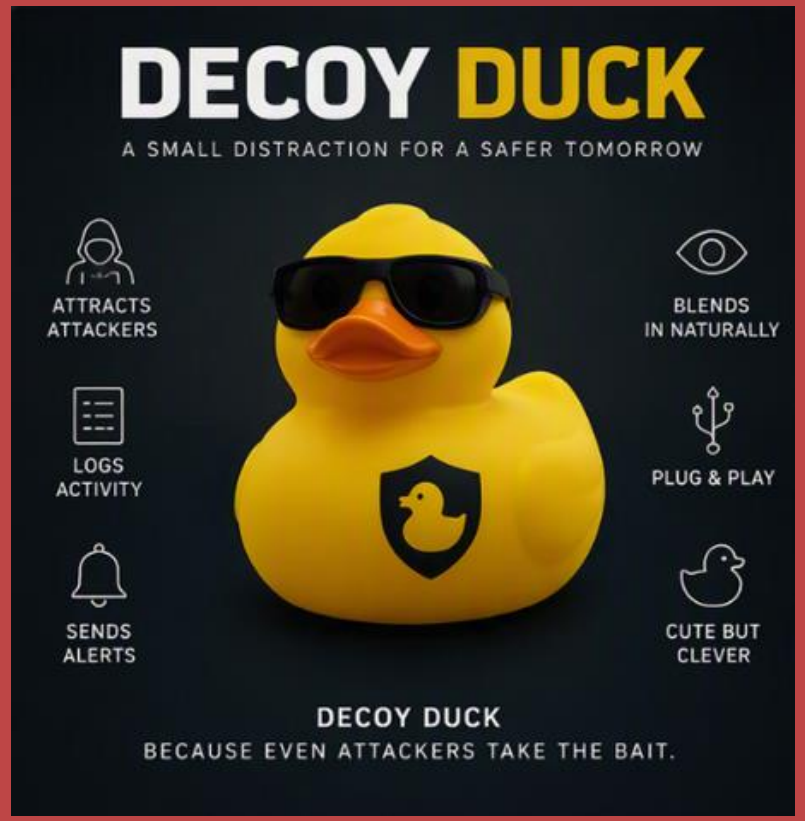
- Assets that appear to be legitimate systems, accounts, or data, but are designed to distract adversaries, detect their presence, or facilitate collection of cyber threat information.
- May be simulated operational technology (OT) or Internet of Things (IoT) devices, such as a fake smart printer or industrial controller, designed to catch lateral movement.

Tripwires:

- Decoys specifically configured such that any interaction (e.g., access, authentication attempt, command execution) generates an alert.
- Any decoy can function as a tripwire if integrated with appropriate monitoring and alerting.
- An example could be fake documents with tempting names, for example *Executive_Salaries.xlsx*, planted on computers to detect unauthorized reading or copying.

CISA - https://www.cisa.gov/sites/default/files/2026-09/using-cyber-decoys-to-strengthen-detection-and-response_508c.pdf

CYBER DECOY BASICS (CONT.)



AI-generated concept art using Microsoft Copilot.

Breadcrumbs:

- Intentionally placed decoy artifacts that adversaries are encouraged to follow, leading to other decoy assets or controlled environments.
- Can be links planted on real devices (such as fake cached passwords) that actively push hackers toward a decoy system.

Honeytokens:

- Data elements or logical objects with no legitimate business use (e.g., fake records, credentials, or files) planted to detect unauthorized access or exfiltration.
- Interaction of any kind strongly suggests malicious or otherwise unauthorized activity.
- These can include single fake data points, such as false user accounts, API keys, or database records, that trigger an alert when used.

CISA - https://www.cisa.gov/sites/default/files/2026-09/using-cyber-decoys-to-strengthen-detection-and-response_508c.pdf

CYBER DECOY BASICS (CONT.)

AI-generated concept art using Microsoft Copilot.

Honeypots:

- Decoy systems or services, often with limited but realistic functionality and intentional vulnerabilities, designed to attract and observe adversaries and divert them from real assets.
- Examples include standalone fake systems or servers, such as a fake database or web server, used to attract and isolate attackers.

Honeynets

- A network of two or more interconnected decoy systems designed to lure, trap, and study malicious actors.
- Simulates a real network, complete with fake servers, routers, firewalls, and vulnerable services.

CISA - https://www.cisa.gov/sites/default/files/2026-09/using-cyber-decoys-to-strengthen-detection-and-response_508c.pdf

HOW CYBER DECOYS WORK

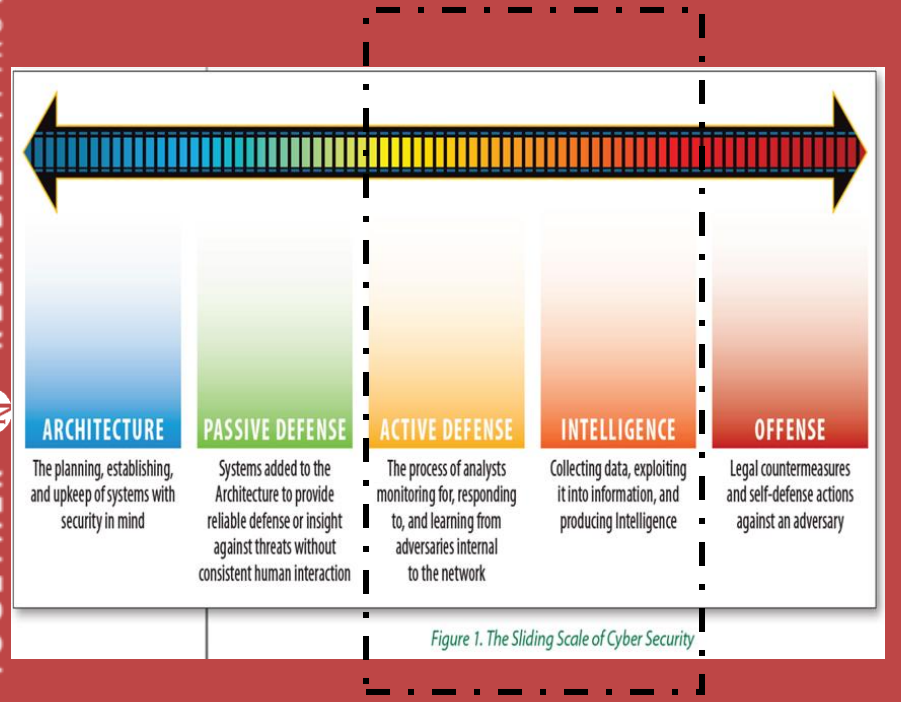


Figure 1. The Sliding Scale of Cyber Security

Source: https://www.sans.org/reading-room/whitepapers/ActiveDefense/sliding-scale-cyber-security-36240

- High-Fidelity Alerts: Any interaction with a decoy generates an immediate, alert because legitimate users have no reason to access them.
- Active Defense: Decoys mislead threat actors into wasting time and revealing their TTPs (tactics, techniques, and procedures).
- Reduce time in your environment: Decoys catch lateral movement and privilege escalation before production assets are compromised.

FORWARD TOGETHER RELIABILITYFIRST

CYBER DECOYS IMPLEMENTATION PROCESS

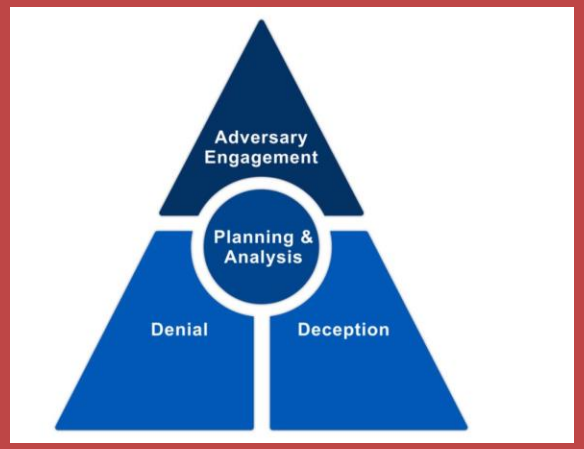
ENGAGING WITH THE ADVERSARY

Prepare	**Step 1:** Assess knowledge of your adversaries and your organization
	Step 2: Determine your operational objective
	Step 3: Determine how you want your adversary to react
	Step 4: Determine what you want your adversary to perceive
	Step 5: Determine channels to engage with your adversary
	Step 6: Determine the success and gating criteria
Operate	**Step 7:** Execute your operation
Understand	**Step 8:** Turn raw data into actionable intelligence
	Step 9: Feedback intelligence
	Step 10: Analyze successes & failures to inform future actions

Source: CISA - https://www.cisa.gov/sites/default/files/2026-09/using-cyber-decoys-to-strengthen-detection-and-response_508c.pdf

FORWARD TOGETHER RELIABILITYFIRST

MITRE ENGAGE™ FRAMEWORK



Source: https://engage.mitre.org/starter-kit/

Prepare	Expose		Affect			Elicit		Understand
Plan	**Collect**	**Detect**	**Prevent**	**Direct**	**Disrupt**	**Reassure**	**Motivate**	**Analyze**
Cyber Threat Intelligence	API Monitoring	Introduced Vulnerabilities	Baseline	Attack Vector Migration	Isolation	Application Diversity	Application Diversity	After-Action Review
Engagement Environment	Network Monitoring	Lures	Hardware Manipulation	Email Manipulation	Lures	Artifact Diversity	Artifact Diversity	Cyber Threat Intelligence
Gating Criteria	Software Manipulation	Malware Detonation	Isolation	Introduced Vulnerabilities	Network Manipulation	Burn-In	Information Manipulation	Threat Model
Operational Objective	System Activity Monitoring	Network Analysis	Network Manipulation	Lures	Software Manipulation	Email Manipulation	Introduced Vulnerabilities	
Persona Creation			Security Controls	Malware Detonation		Information Manipulation	Malware Detonation	
Storyboarding				Network Manipulation		Network Diversity	Network Diversity	
Threat Model				Peripheral Management		Peripheral Management	Personas	
				Security Controls		Pocket Litter		
				Software Manipulation				

FORWARD TOGETHER RF RELIABILITYFIRST

MITRE ATT&CK® ENGAGE FRAMEWORK

FORWARD TOGETHER RELIABILITYFIRST

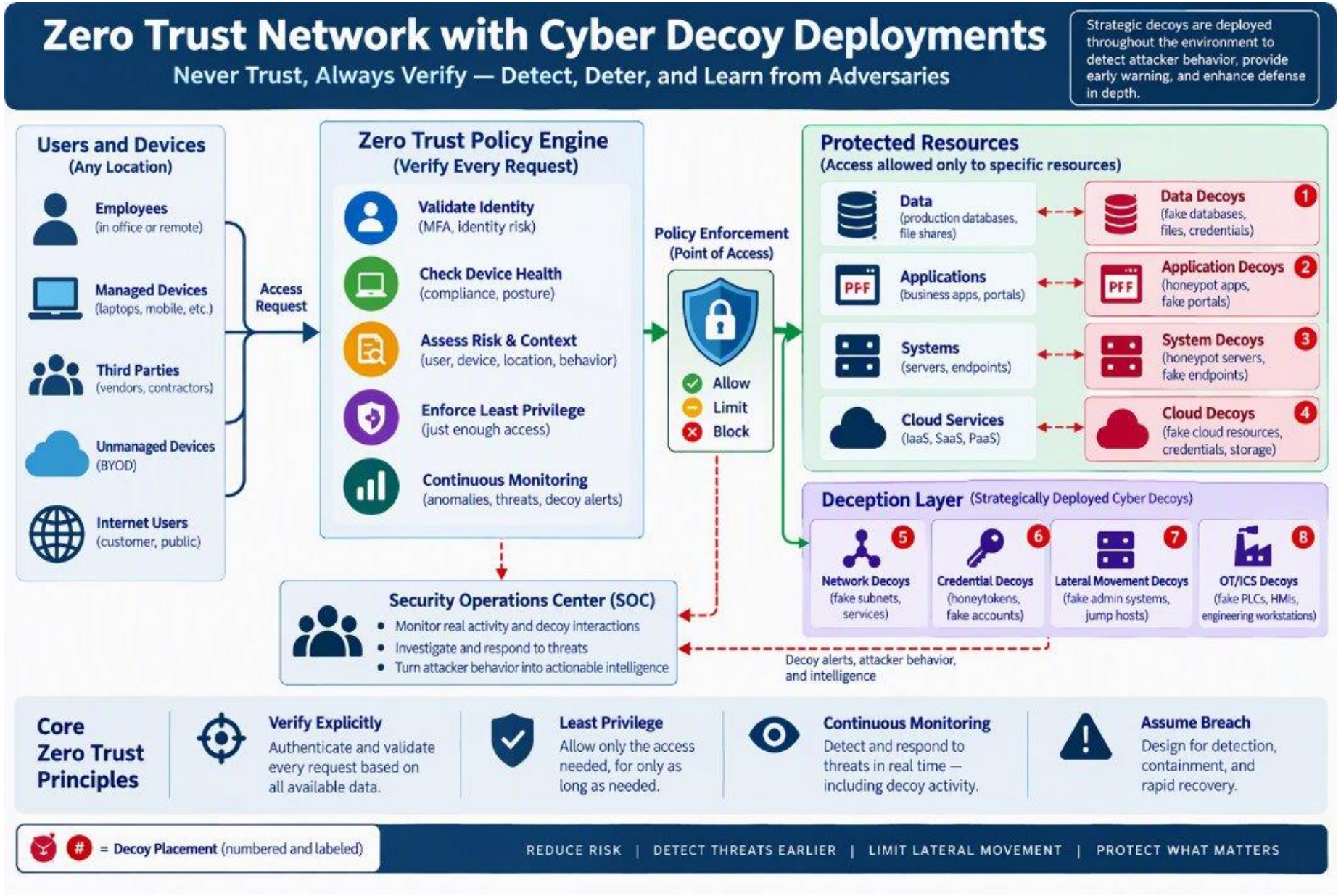
ATT&CK®

ATT&CK® Technique	Adversary Vulnerability	Engagement Activity
When adversaries perform specific actions …	… their actions reveal vulnerabilities …	… that the defender can take advantage of for defensive purposes.

ATT&CK® Technique	Adversary Vulnerability	Engagement Activity
Remote System Discovery (ATT&CK ID: T1018)	When adversaries interact with the environment or personas, they are vulnerable to collect, observe, or manipulate system artifacts that may cause them to reveal behaviors, use additional or more advanced capabilities against the target, and/or impact their dwell time	Decoy Artifacts and Systems

Source: https://attack.mitre.org/

IMPLEMENTATION OF CYBER DECOYS



FORWARD TOGETHER RELIABILITYFIRST

AI-generated concept art using Microsoft Copilot.

CYBER DECOYS AS PART OF A CIP-015 PROGRAM

(CYBER SECURITY – INTERNAL NETWORK SECURITY MONITORING)

- Support CIP-015 R1.1
  - Provide additional network telemetry and high-confidence indicators of adversarial activity.
- Support CIP-015 R1.2
  - Detect anomalous activity through interactions with assets that have no legitimate operational purpose.
- Support CIP-015 R1.3
  - Provide enriched information that allows analysts to quickly evaluate events and determine appropriate response actions.

A strong CIP-015 position would be to include:

- Passive network monitoring (e.g. TAPs or SPANs) as the primary INSM capability
- Protocol analysis and behavioral analytics as the primary detection mechanism
- Cyber decoys as **supplemental** high-fidelity detection capability that enhances detection and evaluation

FORWARD TOGETHER RELIABILITYFIRST

POTENTIAL USES FOR CYBER DECOYS IN A CIP ENVIRONMENT*

Decoy Engineering Workstation	Appears as: Engineering workstation, Relay configuration system, SCADA support workstation Detects: Reconnaissance, Credential theft, Unauthorized remote access
Decoy Historian	Appears to contain: Operational data, Event logs, Transmission information Detects: Data harvesting, Discovery activity
Decoy Jump Host	Appears as: Vendor access server, EACMS resource, Administrative workstation Detects: Lateral movement, Privilege escalation efforts
Credential Decoys	Examples: Fake admin accounts, Fake service accounts, Honeytoken passwords Detects: Credential enumeration, Password dumping, Kerberos attacks
Decoy PLCs and HMIs	Particularly useful for: Generation or Transmission Substation environments Detects: OT protocol reconnaissance, Modbus polling, DNP3 discovery, Unauthorized control attempts

* There are caveats with these type of decoys

AI-generated concept art using Microsoft Copilot.

CAVEATS FOR IMPLEMENTING

Cyber decoys have great potential for high-fidelity alerting, with a high signal-to-noise ratio.

HOWEVER there are caveats:

- Current standards may not allow for these devices within the ESP, for example:
  - Patching
  - Configuration baselines
  - Ports and services
  - Credentials and default credentials
- CIP-008 (Incident Reporting and Response Planning) reporting considerations

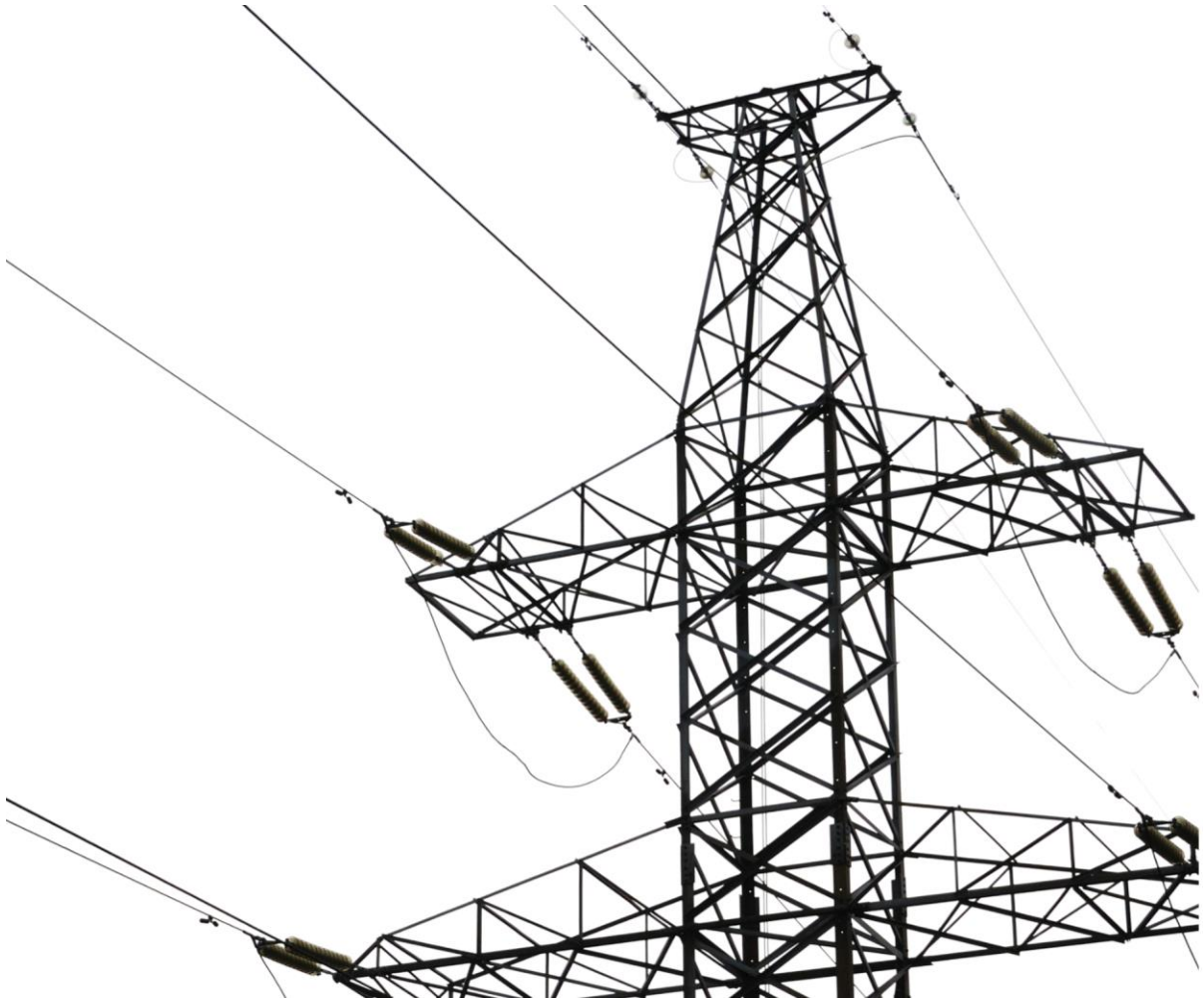
Consider the following for implementation:

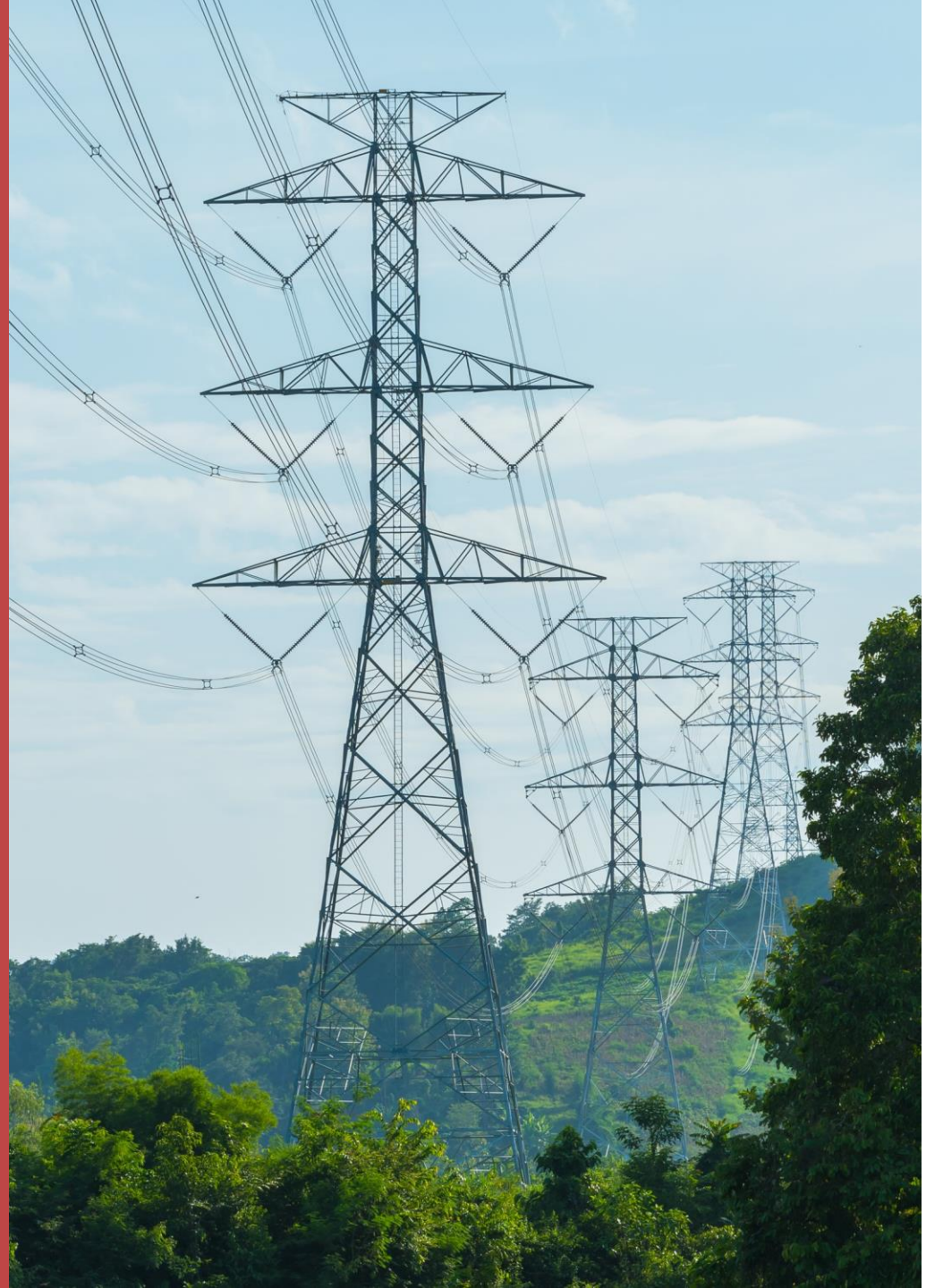
- Maintain appropriate documentation of cyber decoys
- Understand the operating environment
- Consider adversary goals, tools, techniques and procedures
- Segment decoys from production systems

FORWARD TOGETHER RELIABILITYFIRST

Join at SLIDO.com

#TechTalkRF



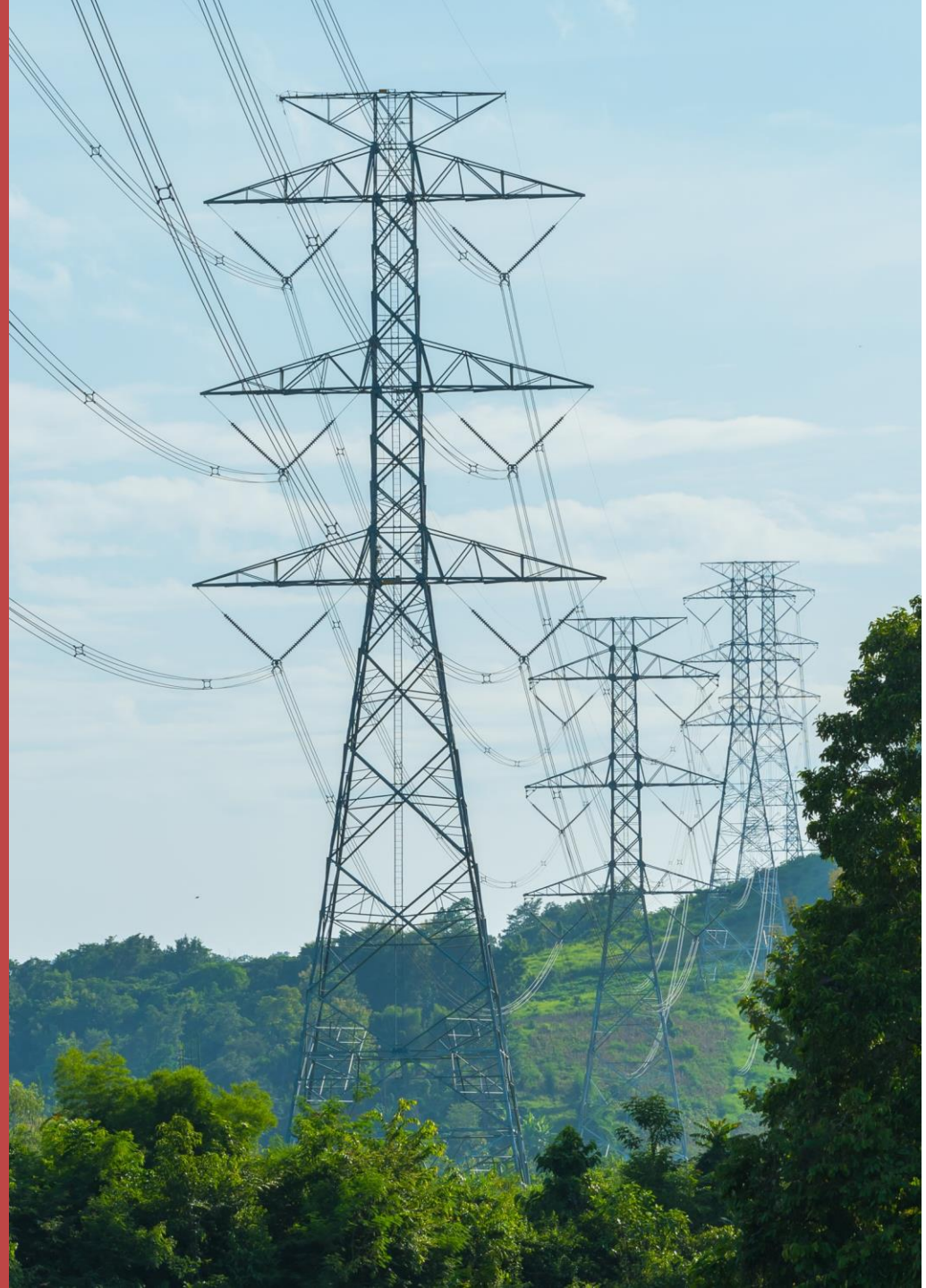


FORWARD TOGETHER RELIABILITYFIRST

QUESTIONS & ANSWERS

Ron.Ross@rfirst.org

David.Sopata@rfirst.org



FORWARD TOGETHER RELIABILITYFIRST

THANK YOU

Join us for our next Tech Talk – November 16th 2-3:30 pm ET

Webinar Link