FORWARD TOGETHER RELIABILITYFIRST

WELCOME TO TECHNICAL TALK WITH RF

January 12, 2026

TECH TALK WITH RELIABILITY FIRST

Public

RELIABILITYFIRST FORWARD TOGETHER

WELCOME TO TECHNICAL TALK WITH RF

January 12, 2026

TECH TALK WITH RELIABILITY FIRST

TECHNICAL TALK WITH RF

Join the conversation at

SLIDO.com

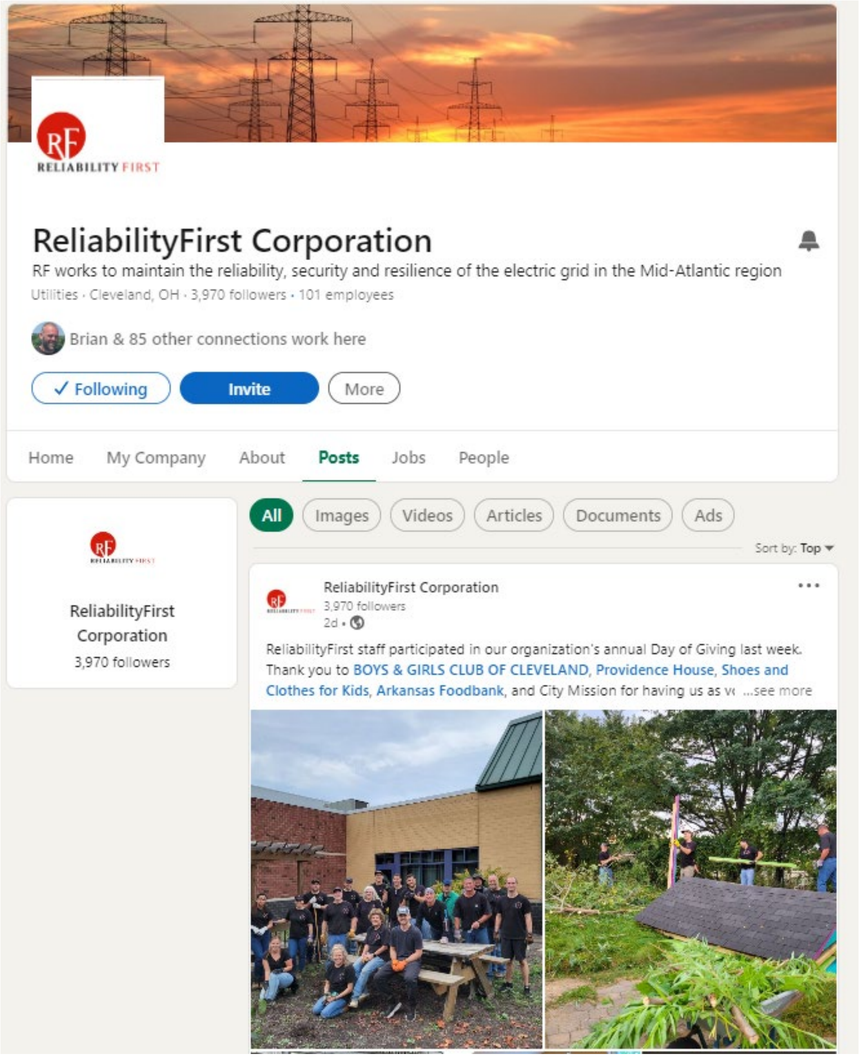
#TechTalkRF

TECHNICAL TALK WITH RF

Follow us on

Linked in

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 vo ...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:

- 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

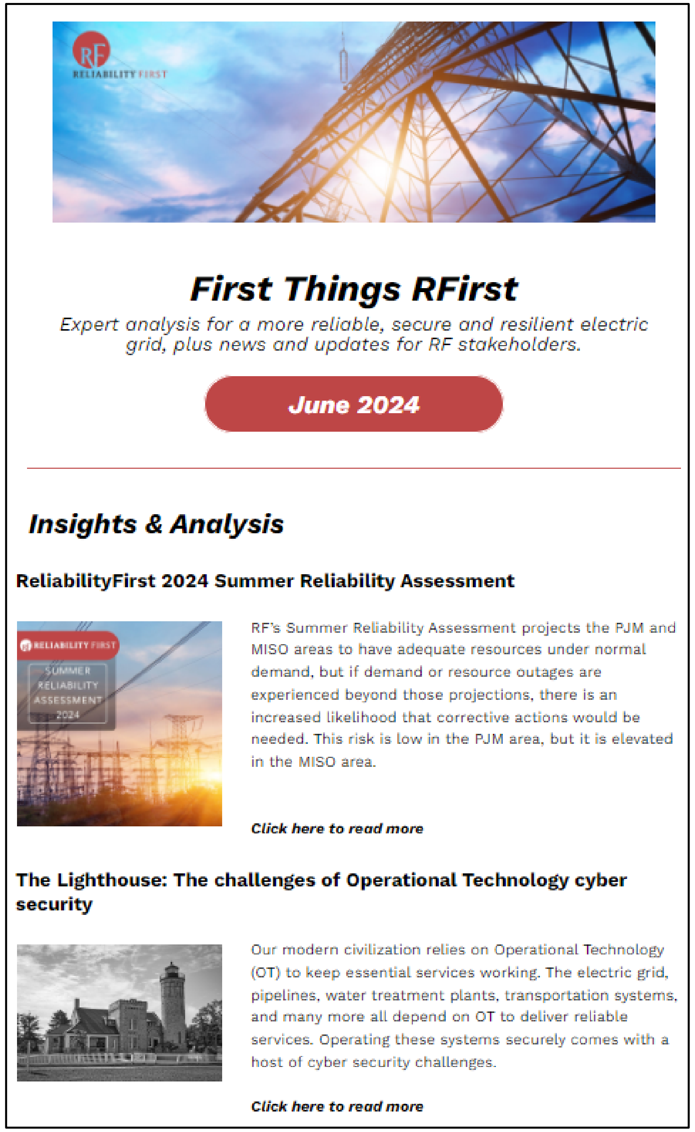
CIP Evidence Request Tool V9 was released and is on NERC's website

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

January 12, 2026

TECH TALK WITH RELIABILITY FIRST

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.

Join us in Cleveland, Ohio February 26th for the

2026 ERO Women's Leadership Conference

Thursday, 2/26/2026
8am - 5pm EST

Reception & Networking Activity
2/25/2026, 5:30 pm

THE AVIATOR

20920 Brookpark Road
Cleveland, OH 44135

Opening Remarks from Joanna Burkey, Founder & Principal of Flat Rock Advisory

Resource Diversity & Resource Mix

How the Unique Attributes of Women can be Leveraged to Optimize Success

Sarah Eppink
Principal & Founder, Aisling Group LLC

Lesley Evancho
Chief Human Resources Officer, EQT

Beth Dowdell
Senior Director of Corporate Services, ReliabilityFirst

Julia Kious Zabell
Executive Director, Case Western Reserve University

Security & Resilience

How Women in the Energy Sector are Ascending the Corporate Ladder and Navigating Challenges

Chris Guiney
Partner, CarterBaldwin, Energy & Infrastructure

Lisa Barton
President & CEO, Alliant Energy

Christine Martin
President, PPL Electric Utilities

Diane Holder
Vice President Engineering & Strategic Engagement, ReliabilityFirst

Human Performance

Fireside Chat Discussing Mental and Physical Well-being

Dr. Tod Podl, MD
Family Medicine, UH Select

Niki Schaefer
Vice President & General Counsel, ReliabilityFirst

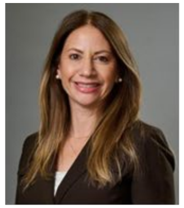
Power Transfer & Relying on Neighbors

Networking and Mentorships

Sara Patrick
President & CEO, MRO

Holly Hawkins
Vice President & General Counsel, SERC

Mèlika Carroll
Head of Global Government Affairs, Cohere



Bluma Sussman
Vice President of Stakeholder Engagement, E-ISAC

Resource Modeling

We will have an onsite photographer during breaks to take professional headshots for attendees!

TECH TALK ANNOUNCEMENT

NERC

NERC Releases New FAQ to Support Category 2 GO/GOP Registration

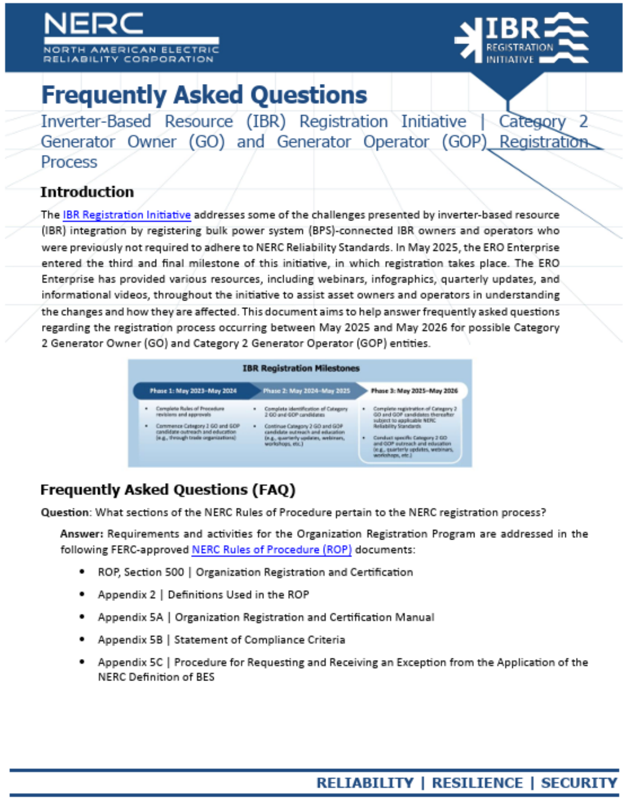
Full Announcement | FAQs | IBR Registration Initiative Overview

NERC has published a new Frequently Asked Questions (FAQ) document to support Generator Owners and Generator Operators registering as Category 2 entities under the Inverter-Based Resource (IBR) Registration Initiative. The FAQ provides additional clarity on the registration process, including eligibility and jurisdiction considerations, documentation expectations, timelines, and common questions.

This FAQ is one of several resources developed as part of NERC's broader effort to support new registrants and promote a clear, consistent understanding of registration requirements. These resources are available on our IBR Registration Initiative page, which serves as a central hub for project updates and guidance.

Through the IBR Registration Initiative, NERC is advancing its mission to ensure the reliability and security of the bulk power system as we navigate the rapidly evolving landscape of energy generation and integration.

IBR REGISTRATION INITIATIVE



NERC NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

IBR REGISTRATION INITIATIVE

Frequently Asked Questions

Inverter-Based Resource (IBR) Registration Initiative | Category 2 Generator Owner (GO) and Generator Operator (GOP) Registration Process

Introduction

The IBR Registration Initiative addresses some of the challenges presented by inverter-based resource (IBR) integration by registering bulk power system (BPS)-connected IBR owners and operators who were previously not required to adhere to NERC Reliability Standards. In May 2025, the ERO Enterprise entered the third and final milestone of this initiative, in which registration takes place. The ERO Enterprise has provided various resources, including webinars, infographics, quarterly updates, and informational videos, throughout the initiative to assist asset owners and operators in understanding the changes and how they are affected. This document aims to help answer frequently asked questions regarding the registration process occurring between May 2025 and May 2026 for possible Category 2 Generator Owner (GO) and Category 2 Generator Operator (GOP) entities.

IBR Registration Milestones

Phase 1: May 2023–May 2024
- Complete Rules of Procedure revisions and approvals
- Commence Category 2 GO and GOP candidate outreach and education (e.g., through trade organizations)

Phase 2: May 2024–May 2025
- Complete identification of Category 2 GO and GOP candidates
- Continue Category 2 GO and GOP candidate outreach and education (e.g., quarterly updates, webinars, workshops, etc.)

Phase 3: May 2025–May 2026
- Complete registration of Category 2 GO and GOP candidates thereafter subject to applicable NERC Reliability Standards
- Conduct specific Category 2 GO and GOP outreach and education (e.g., quarterly updates, webinars, workshops, etc.)

Frequently Asked Questions (FAQ)

Question: What sections of the NERC Rules of Procedure pertain to the NERC registration process?

Answer: Requirements and activities for the Organization Registration Program are addressed in the following FERC-approved NERC Rules of Procedure (ROP) documents:

- ROP, Section 500 | Organization Registration and Certification
- Appendix 2 | Definitions Used in the ROP
- Appendix 5A | Organization Registration and Certification Manual
- Appendix 5B | Statement of Compliance Criteria
- Appendix 5C | Procedure for Requesting and Receiving an Exception from the Application of the NERC Definition of BES

RELIABILITY | RESILIENCE | SECURITY

Public

TECH TALK ANNOUNCEMENT

NERC

Technical Workshop Project 2024-02
Planning Energy Assurance
February 17, 2026

[In person](#) | [Webinar](#)

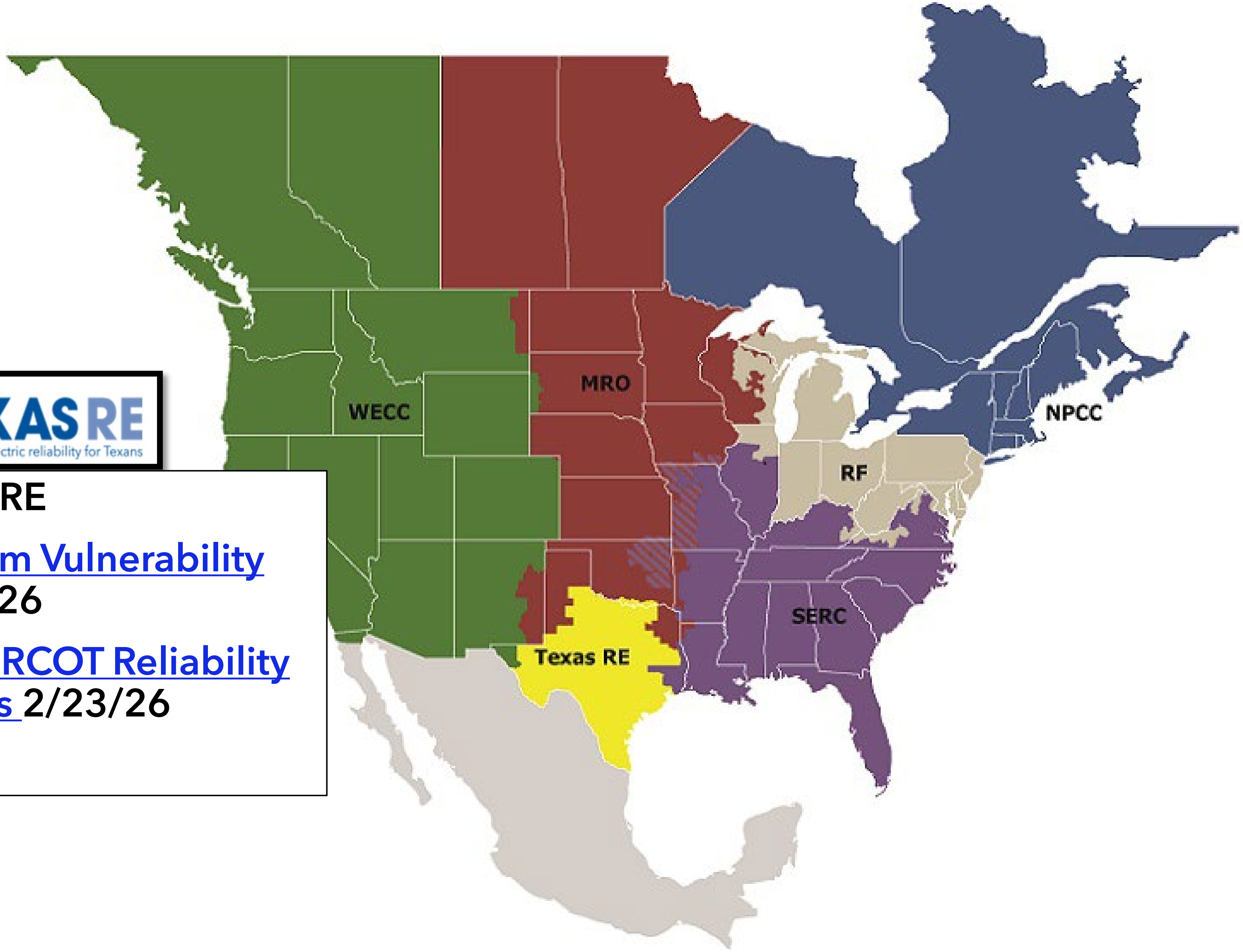
The focus of the Workshop will be to address major themes from the initial formal comment period that concluded on December 10, 2025. There will be three panels that will delve into energy assurance in the state and regulatory space, energy studies thresholds, and mitigation actions for energy shortfalls in the long-term planning horizon.

In person location:
Sourthern Company
241 Ralph McGill Blvd NE
Atlanta, GA 30308

TEXAS RE
Ensuring electric reliability for Texans

Talk with Texas RE

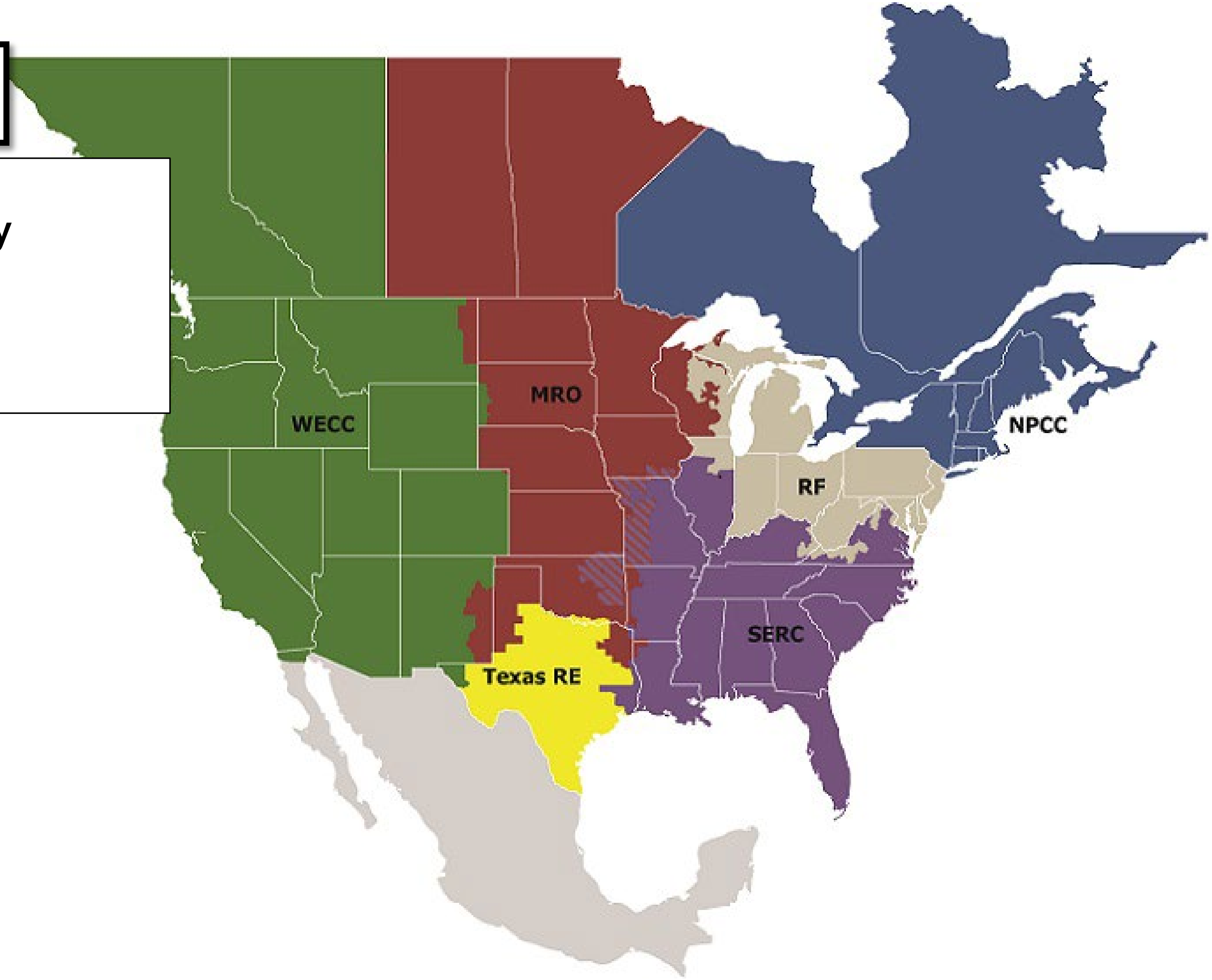
- Power System Vulnerability Index 1/21/26
- NERC and ERCOT Reliability Assessments 2/23/26



WECC

Reliability & Security Oversight Update

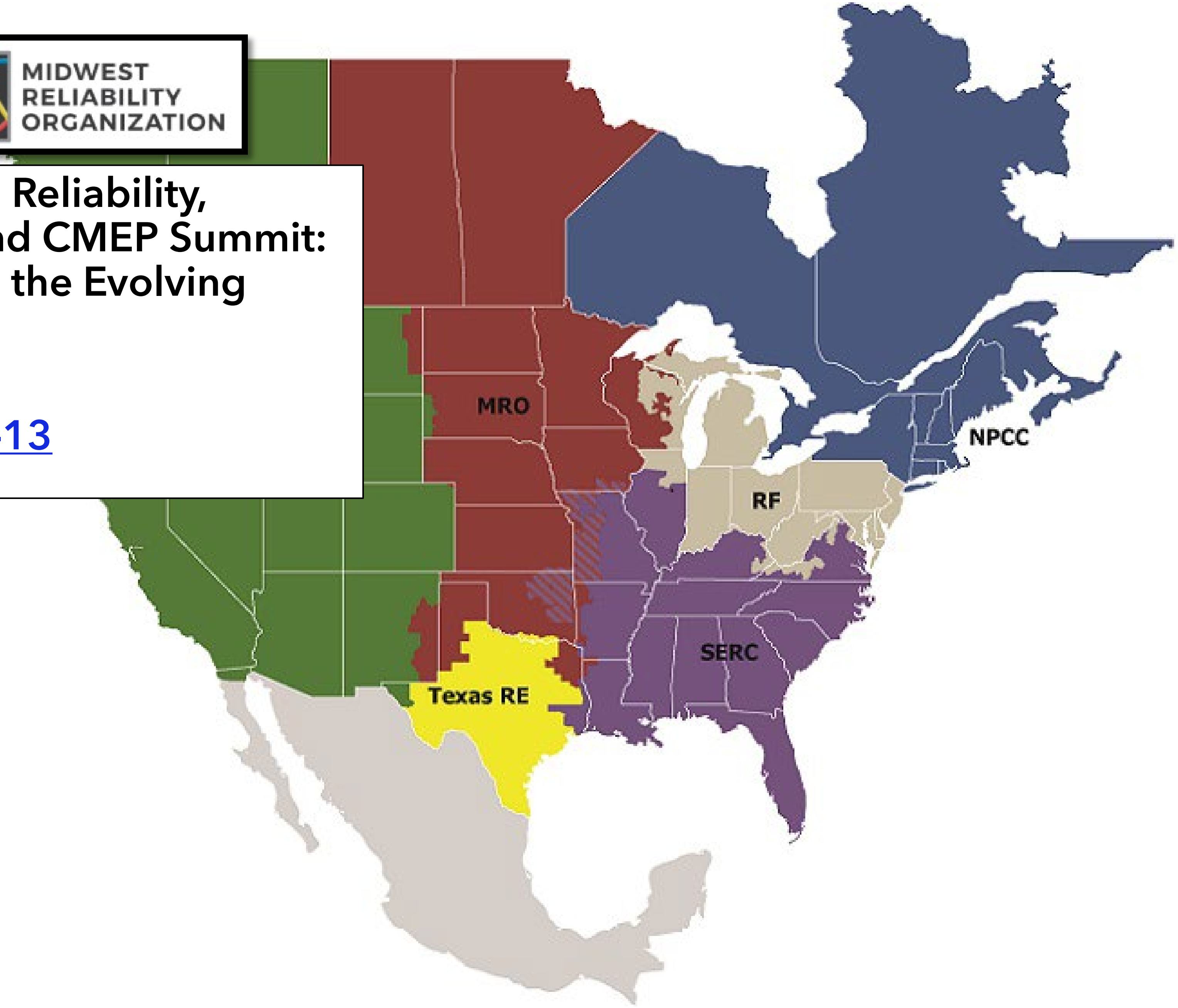
- January 15

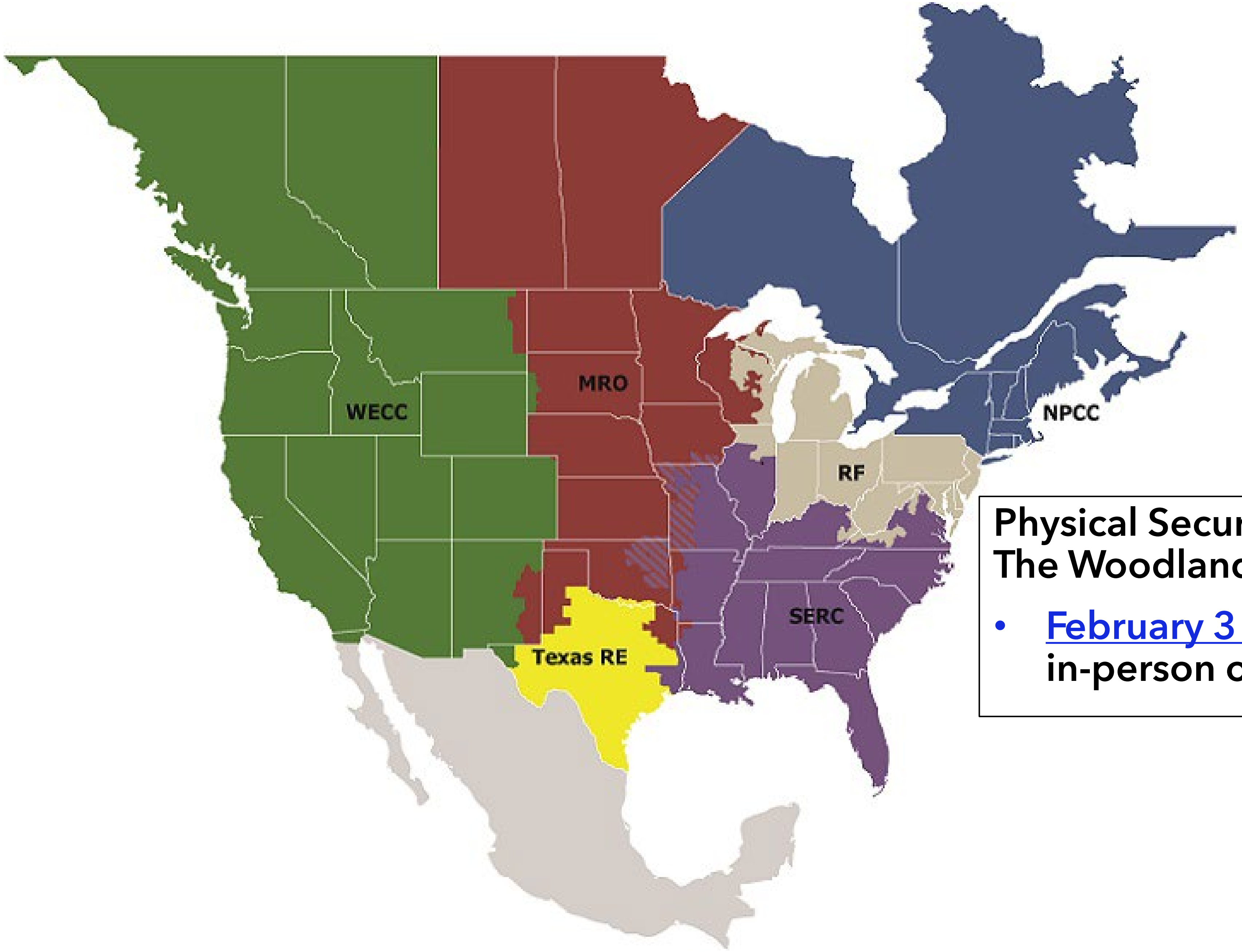


MIDWEST
RELIABILITY
ORGANIZATION

2026 MRO Reliability, Security, and CMEP Summit: Navigating the Evolving Power Grid

- May 12-13

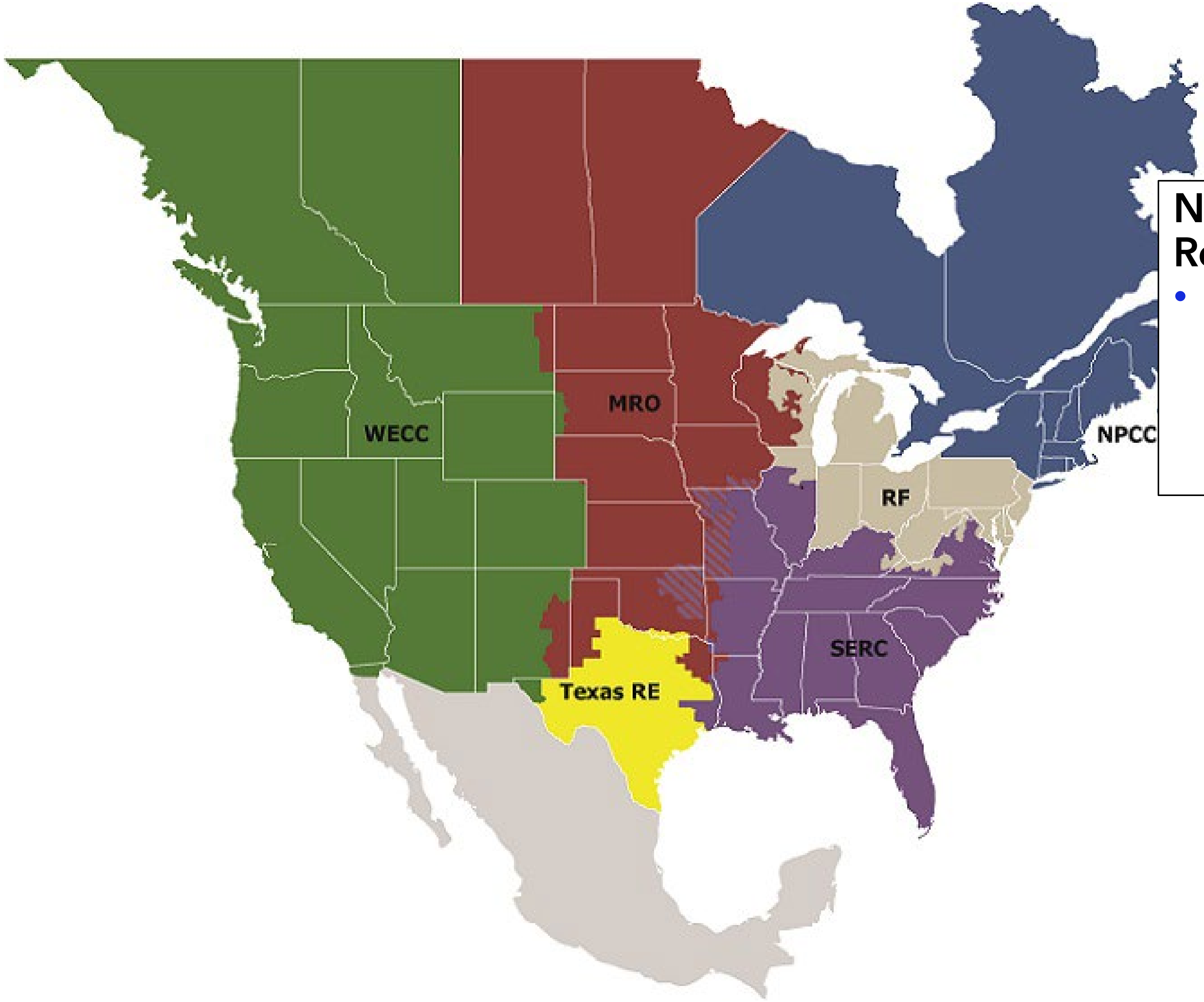




SERC Reliability Corporation

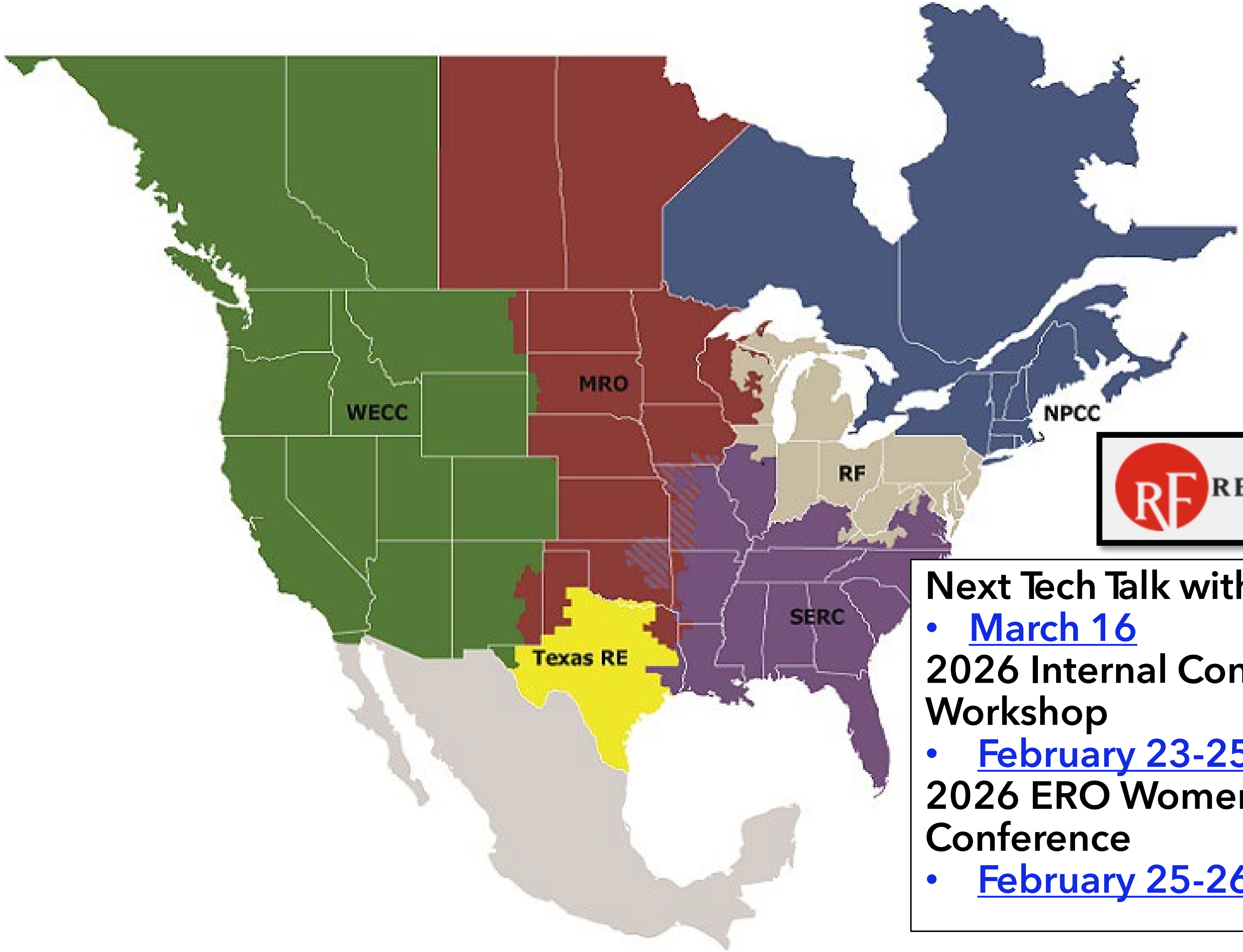
Physical Security Workshop, The Woodlands, TX

- February 3 - 5, in-person only



NPCC Winter Reliability Assessment

- Assessment Projects Sufficient Supply to Meet Winter Demand



RELIABILITYFIRST

Next Tech Talk with RF

- March 16

2026 Internal Controls Workshop

- February 23-25

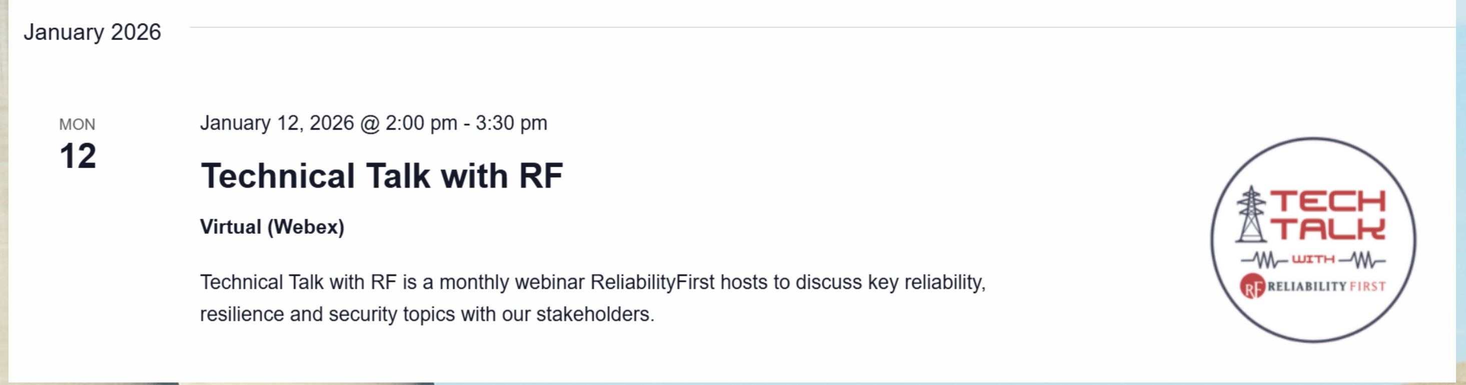
2026 ERO Women's Leadership Conference

- February 25-26

TECH TALK REMINDER

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

CLICK HERE



January 2026

MON
12

January 12, 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.

TECHNICAL TALK WITH RF

Join the conversation at

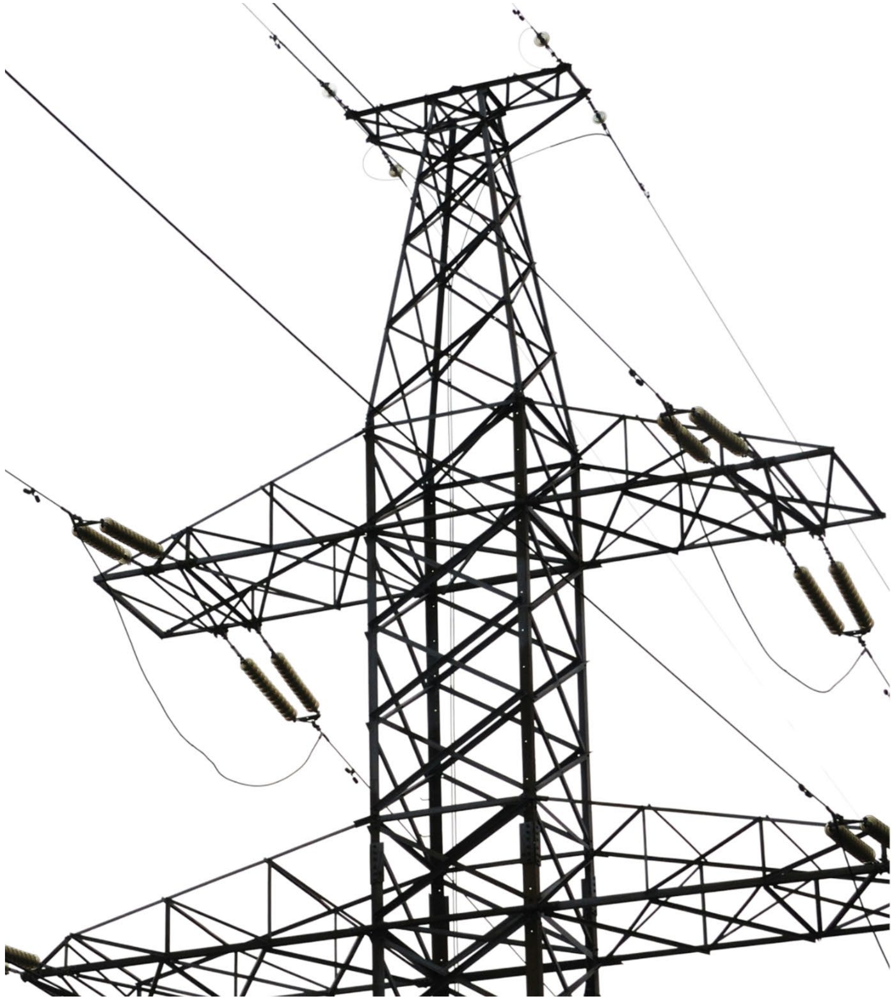
SLIDO.com

#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

CIP CLOUD STANDARDS UPDATE

- **LEW FOLKERTH,** PRINCIPAL RELIABILITY CONSULTANT – EXTERNAL AFFAIRS, RELIABILITYFIRST

2025 ENFORCEMENT YEAR IN REVIEW

- **MARIAN TONEY,** COUNSEL, ENFORCEMENT, RELIABILITYFIRST

STRATEGIES FOR BUILDING AN INTERNAL NETWORK SECURITY MONITORING PROGRAM

- **RON ROSS,** PRINCIPAL RELIABILITY CONSULTANT, ENTITY ENGAGEMENT, RELIABILITYFIRST

PROJECT 2023-09 RISK MANAGEMENT FOR THIRD-PARTY CLOUD SERVICES

DRAFTING TEAM UPDATE

Lew Folkerth, PE, LPI, +9 – Principal Reliability Consultant

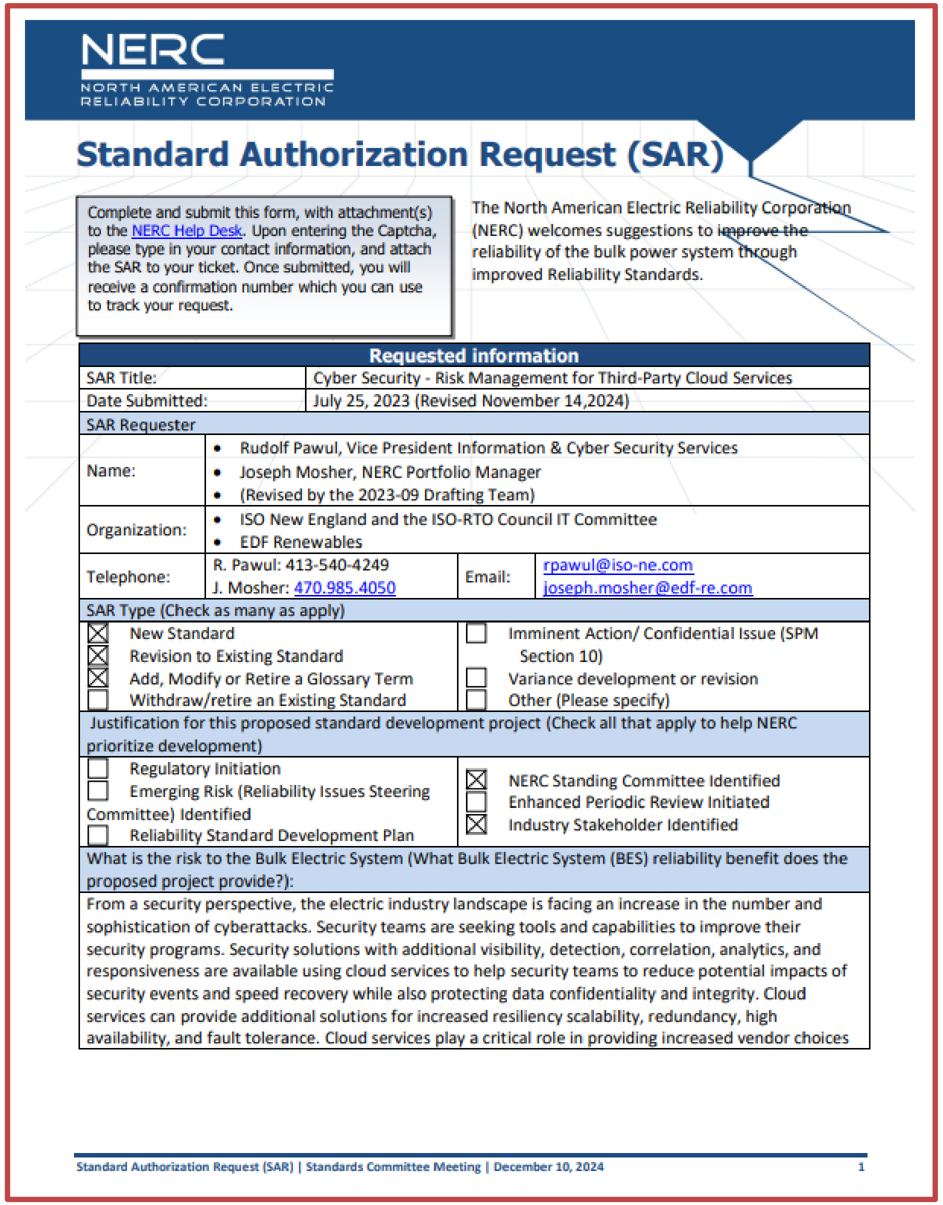
Technical Talk with RF

January 12, 2026

RELIABILITY FIRST

2023-09 SAR KEY POINTS

- Cloud-based solutions are becoming essential to the purpose of keeping the electric grid secure
- Open project scope
  - Any/all CIP defined systems
  - Any/all CIP standards
- Minimize impacts on existing standards
- Must consider risks beyond the scope of the existing standards
- May take holistic or incremental approach
- Risk-based, outcome-driven
- Consider third-party certifications
- Allow but not require cloud use



NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standard Authorization Request (SAR)

Complete and submit this form, with attachment(s) to the NERC Help Desk. Upon entering the Captcha, please type in your contact information, and attach the SAR to your ticket. Once submitted, you will receive a confirmation number which you can use to track your request.

The North American Electric Reliability Corporation (NERC) welcomes suggestions to improve the reliability of the bulk power system through improved Reliability Standards.

Requested information			
SAR Title:	Cyber Security - Risk Management for Third-Party Cloud Services		
Date Submitted:	July 25, 2023 (Revised November 14,2024)		
SAR Requester			
Name:	• Rudolf Pawul, Vice President Information & Cyber Security Services • Joseph Mosher, NERC Portfolio Manager • (Revised by the 2023-09 Drafting Team)		
Organization:	• ISO New England and the ISO-RTO Council IT Committee • EDF Renewables		
Telephone:	R. Pawul: 413-540-4249 J. Mosher: 470.985.4050	Email:	rpawul@iso-ne.com joseph.mosher@edf-re.com

SAR Type (Check as many as apply)

☒ New Standard
☒ Revision to Existing Standard
☒ Add, Modify or Retire a Glossary Term
☐ Withdraw/retire an Existing Standard

☐ Imminent Action/ Confidential Issue (SPM Section 10)
☐ Variance development or revision
☐ Other (Please specify)

Justification for this proposed standard development project (Check all that apply to help NERC prioritize development)

☐ Regulatory Initiation
☐ Emerging Risk (Reliability Issues Steering Committee) Identified
☐ Reliability Standard Development Plan

☒ NERC Standing Committee Identified
☐ Enhanced Periodic Review Initiated
☒ Industry Stakeholder Identified

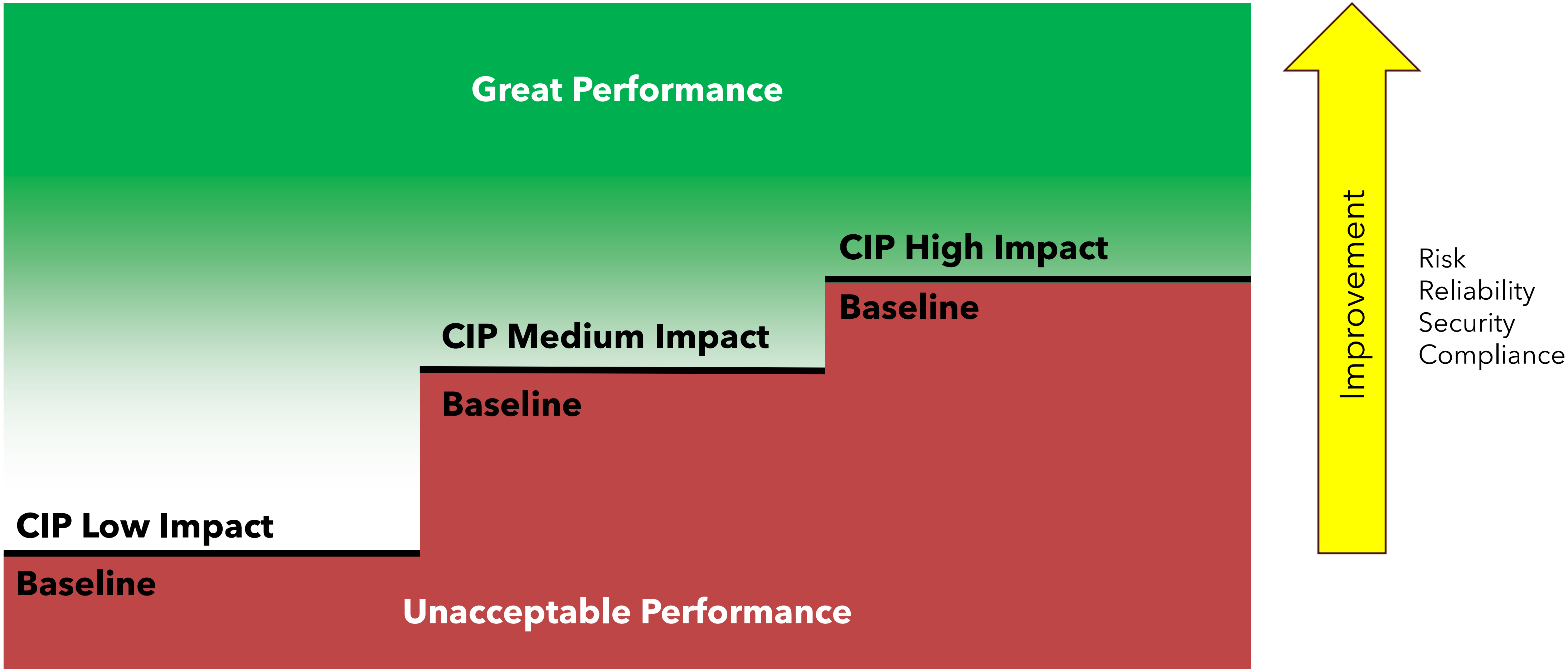
What is the risk to the Bulk Electric System (What Bulk Electric System (BES) reliability benefit does the proposed project provide?):

From a security perspective, the electric industry landscape is facing an increase in the number and sophistication of cyberattacks. Security teams are seeking tools and capabilities to improve their security programs. Security solutions with additional visibility, detection, correlation, analytics, and responsiveness are available using cloud services to help security teams to reduce potential impacts of security events and speed recovery while also protecting data confidentiality and integrity. Cloud services can provide additional solutions for increased resiliency scalability, redundancy, high availability, and fault tolerance. Cloud services play a critical role in providing increased vendor choices

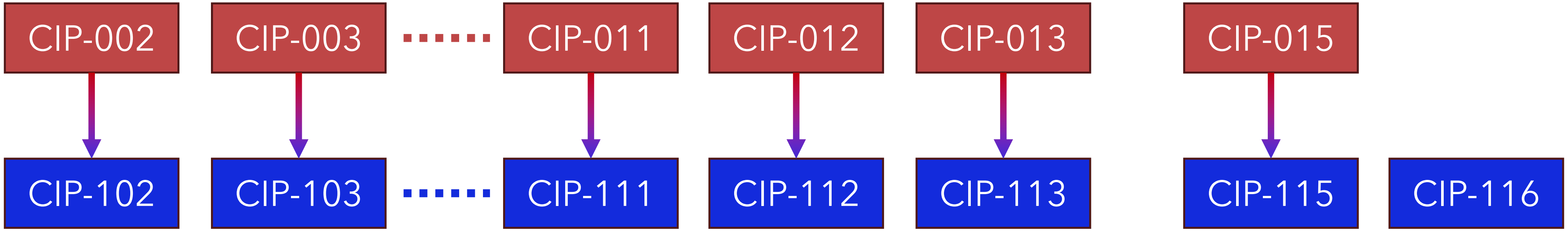
Standard Authorization Request (SAR) | Standards Committee Meeting | December 10, 2024 1

CIP AND OTHER FRAMEWORKS

NIST CSF, NIST 800-53/82, IEC 62443, etc.



2023-09 TENTATIVE APPROACH



- Existing CIP standards will remain in place as untouched as possible
- The new 100-series standards will stand on their own – no reliance on the existing standards
- The 100-series standards will be objective-based
- The 100-series standards will permit cloud usage with appropriate controls
- The 100-series standards will be flexible to permit adoption of emerging technologies as needed
- The 100-series standards will use a System Security Plan (SSP) approach
- Adoption of the 100-series standards will be on an opt-in, system-by-system basis

SYSTEM SECURITY PLAN (SSP)

- The CIP requirements will be objectives, or “what to accomplish”
- The SSP will detail how the objectives are achieved
- Compliance evidence will demonstrate the execution of the SSP

WHITE PAPER

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

CIP & Cloud Services

A New Way Forward

Project 2023-09 Drafting Team

December 2025

- Published 12/18/2025
- Comments due 2/2/2026
- https://www.nerc.com/globalassets/standards/projects/2023-09/white-paper/project-2023-09-risk-management-for-third-party-cloud-services-white-paper_121825.pdf

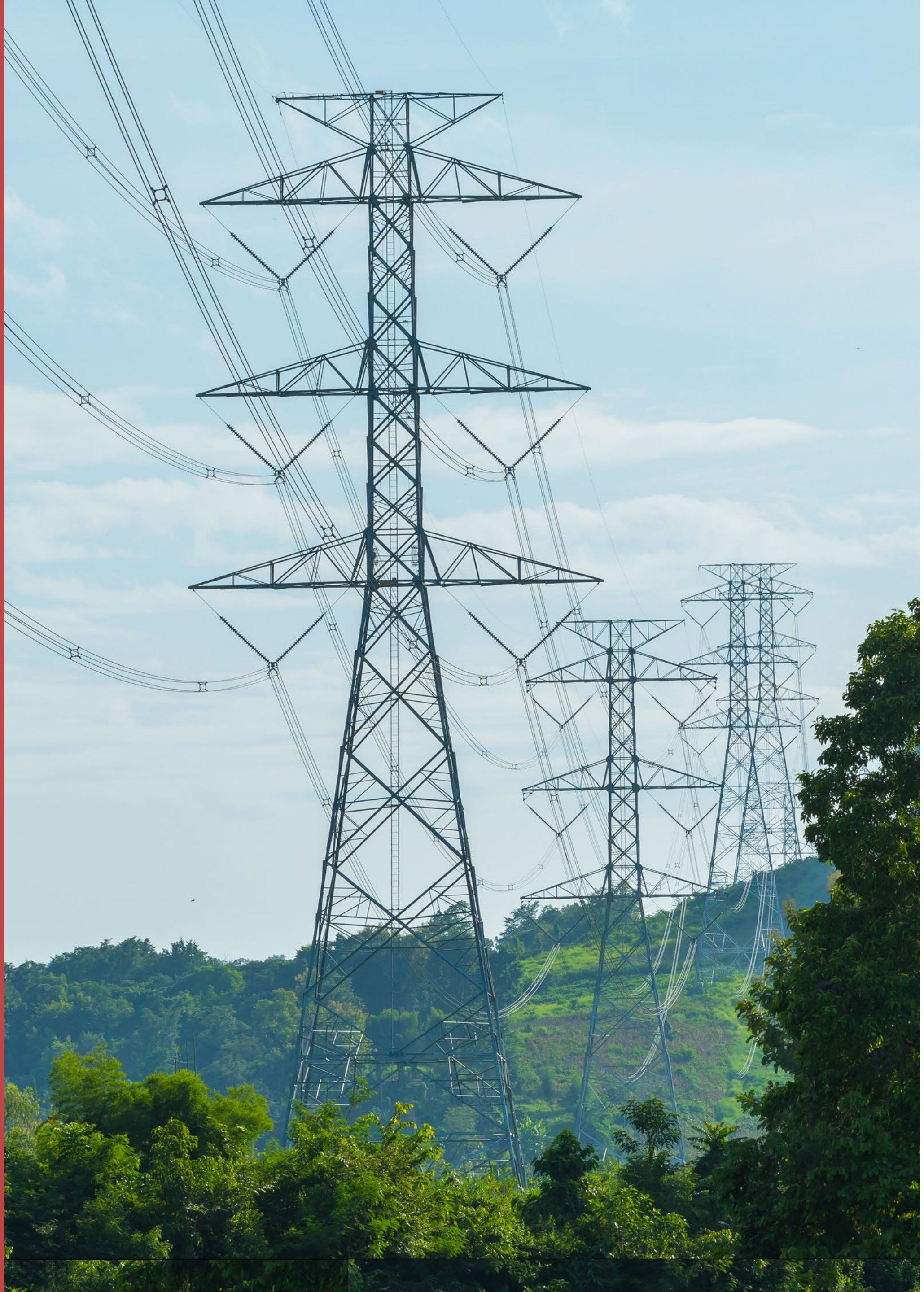
WEBINAR

- The 2023-09 drafting team will conduct a webinar to discuss the white paper
- Scheduled for January 20, 2026, at 1:30 to 3:00 ET
- Watch the NERC web site and the Standards, Compliance, and Enforcement Bulletin for details

REFERENCES

- Project 2023-09 Risk Management for Third-Party Cloud Services
- SITES BES Operations in the Cloud whitepaper
- IEEE Practical Adoption of Cloud Computing in Power Systems- Drivers, Challenges, Guidance, and Real-world Use Cases
- NERC informational filing to FERC in December 2021
- The NIST Definition of Cloud Computing
- Security Guideline for the Electricity Sector – Supply Chain
- Security Guideline BCS Cloud Encryption
- Implementation Guidance: Usage of Cloud Solutions for BES Cyber System Information (BCSI)
- DOD Cybersecurity Reciprocity Playbook

FORWARD TOGETHER RELIABILITYFIRST



QUESTIONS & ANSWERS

Lew Folkerth

lew.folkerth@rfirst.org

A YEAR IN REVIEW: ENFORCEMENT 2025

Marian Kousaie Toney, Counsel

January 12, 2026

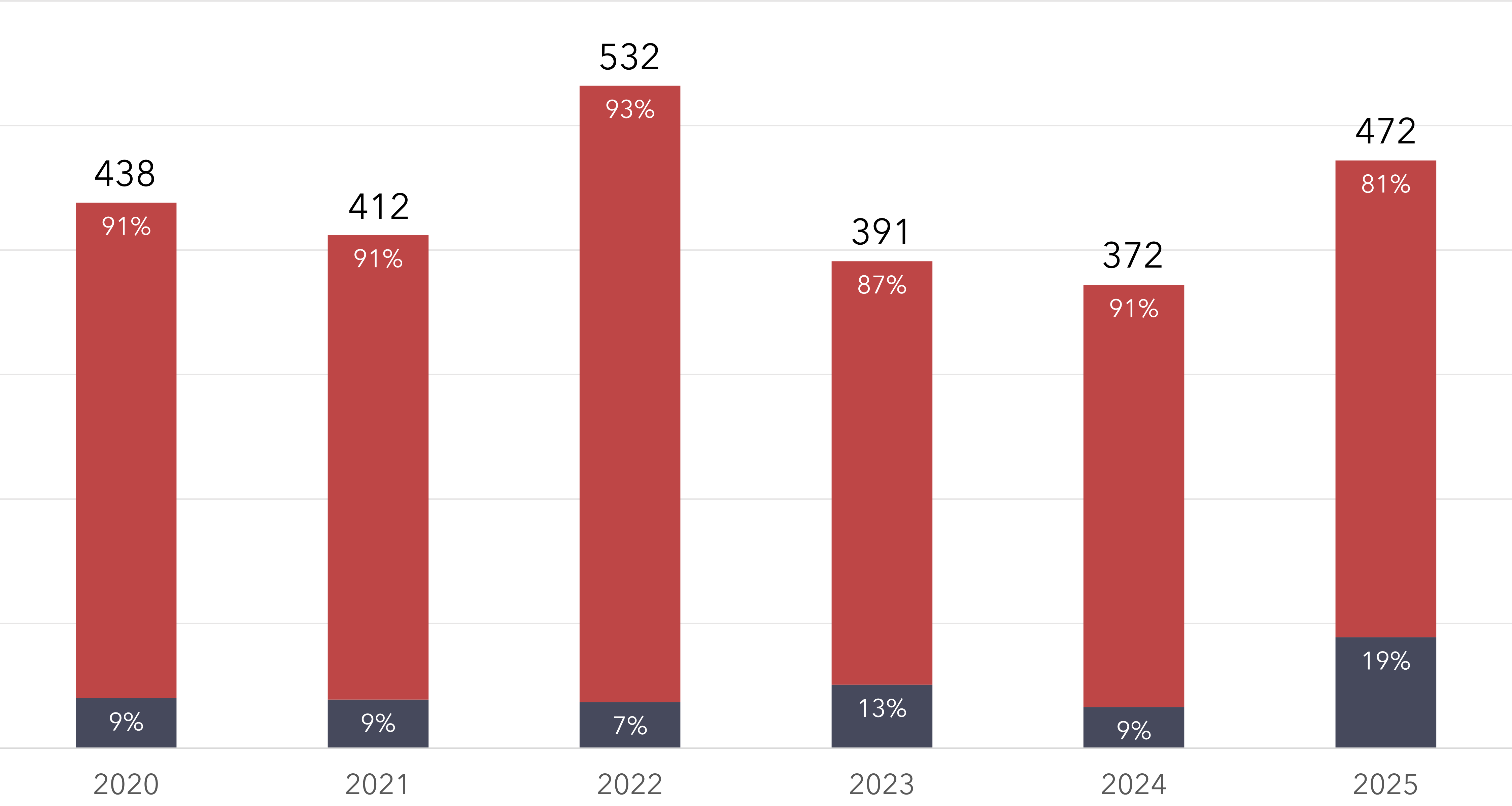
RELIABILITY FIRST

FORWARD TOGETHER RELIABILITYFIRST

AGENDA

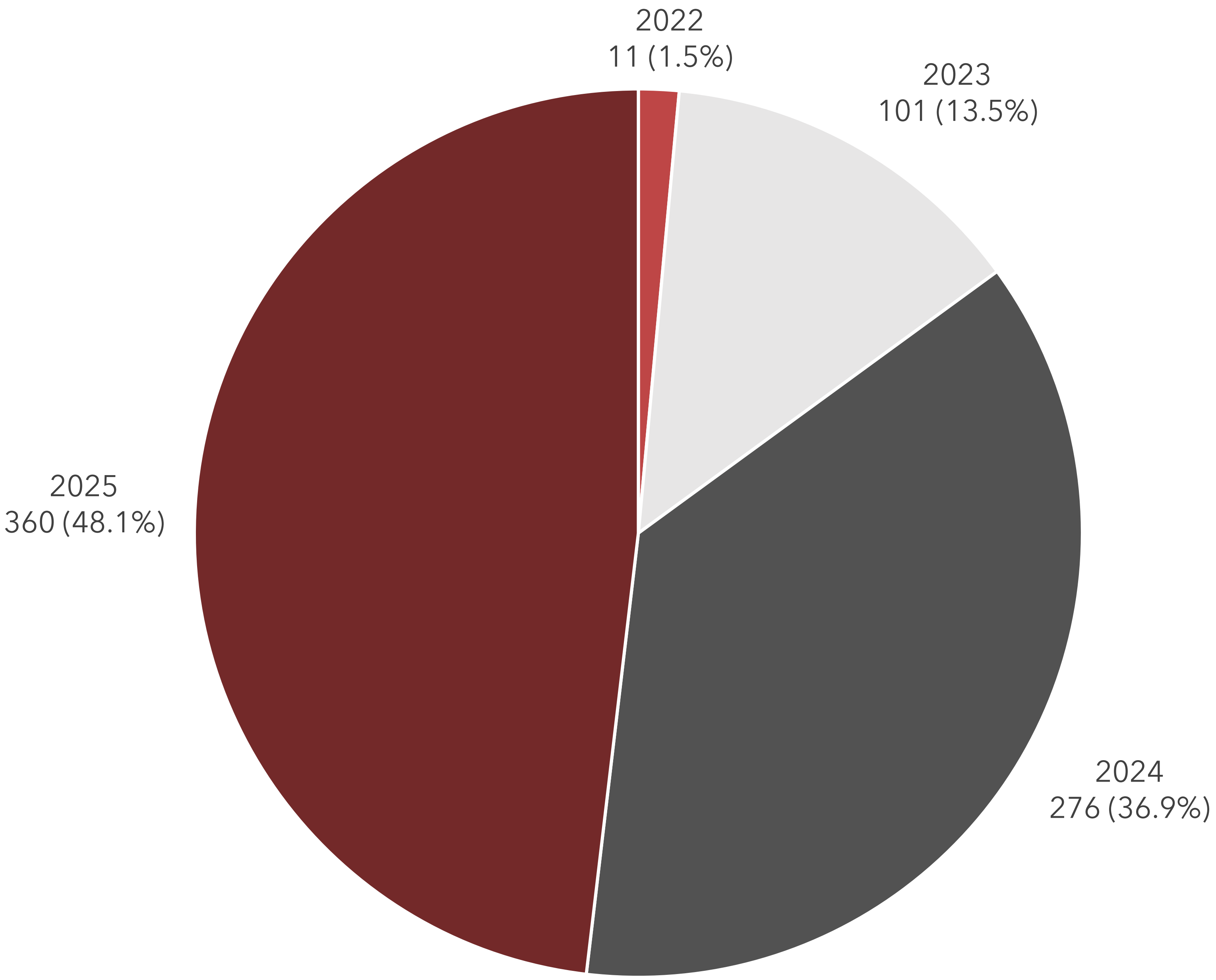
- ANNUAL INTAKE
- CURRENT INVENTORY
- ANNUAL PROCESSING

Annual Intake: Self-Reported v. Monitoring Engagement

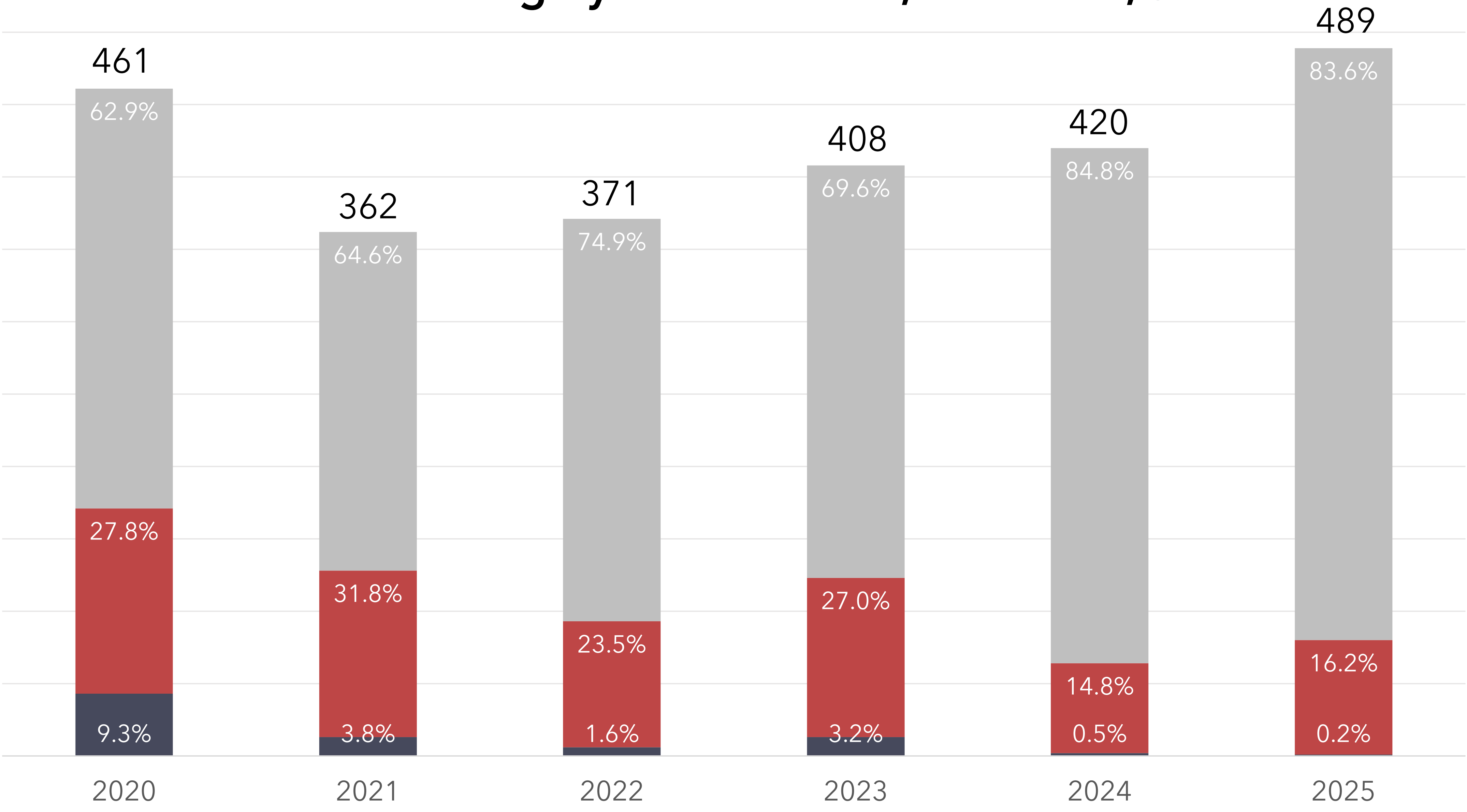


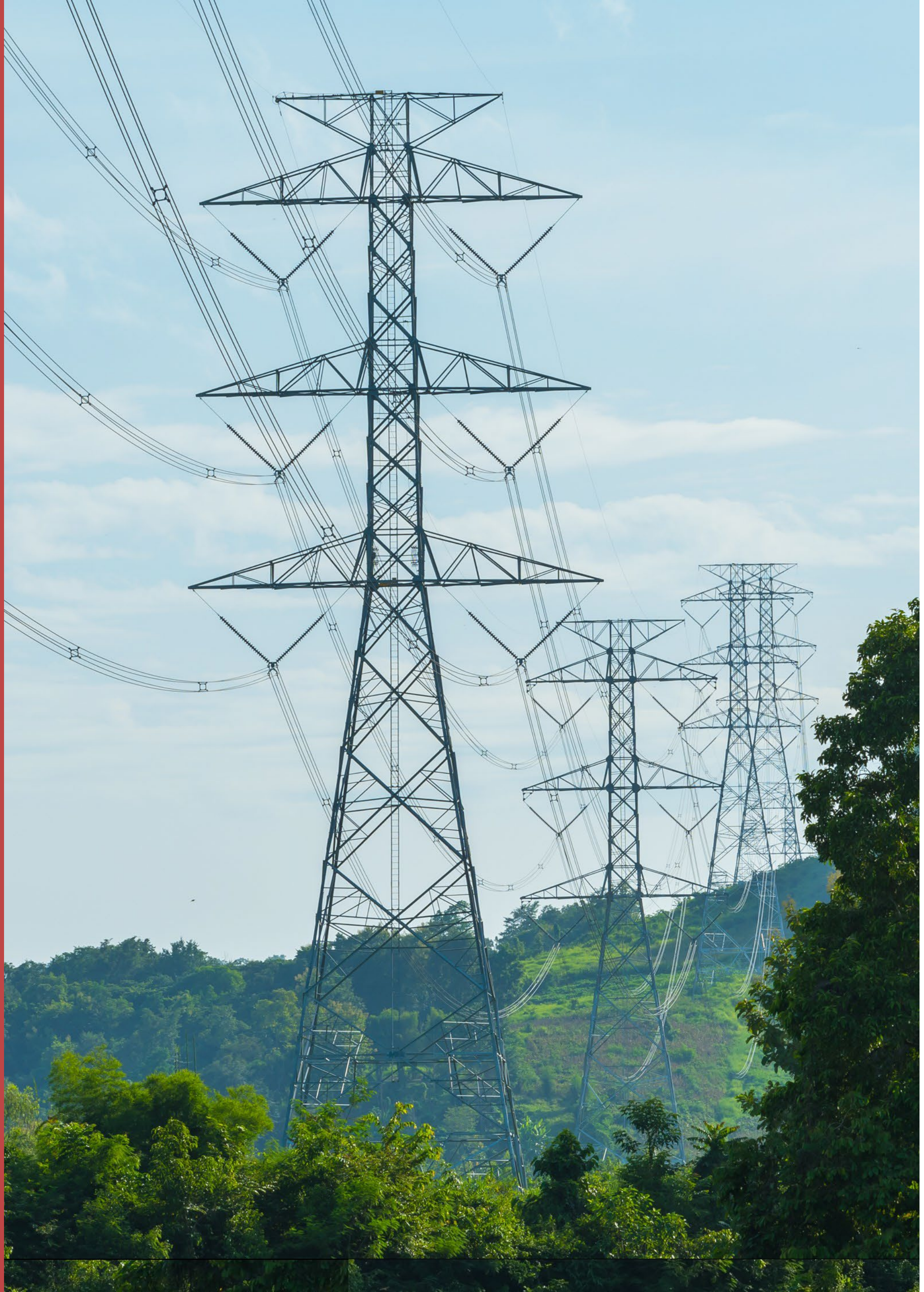
Current Inventory

Year	Intake	Open	Percent Processed
2020	438	0	100%
2021	412	0	100%
2022	532	11	97.93%
2023	391	101	74.17%
2024	372	276	25.81%
2025	472	360	23.73%
Total	**2,617**	**748**	**71.42%**



Annual Processing by Risk: Minimal, Moderate, Serious





QUESTIONS & ANSWERS

CIP-015-1
INTERNAL NETWORK SECURITY MONITORING

Ron Ross, Principal Reliability Consultant, Entity Engagement

Jan. 12, 2026

RELIABILITY FIRST

CIP-015-1

- Internal Network Security Monitoring (INSM)
- To improve the probability of detecting anomalous or unauthorized network activity to facilitate improved response and recovery from an attack
- Goals:
    - Enhance cyber security of Bulk Electric System (BES)
    - Improve visibility within internal networks
    - Detect unauthorized or malicious activity

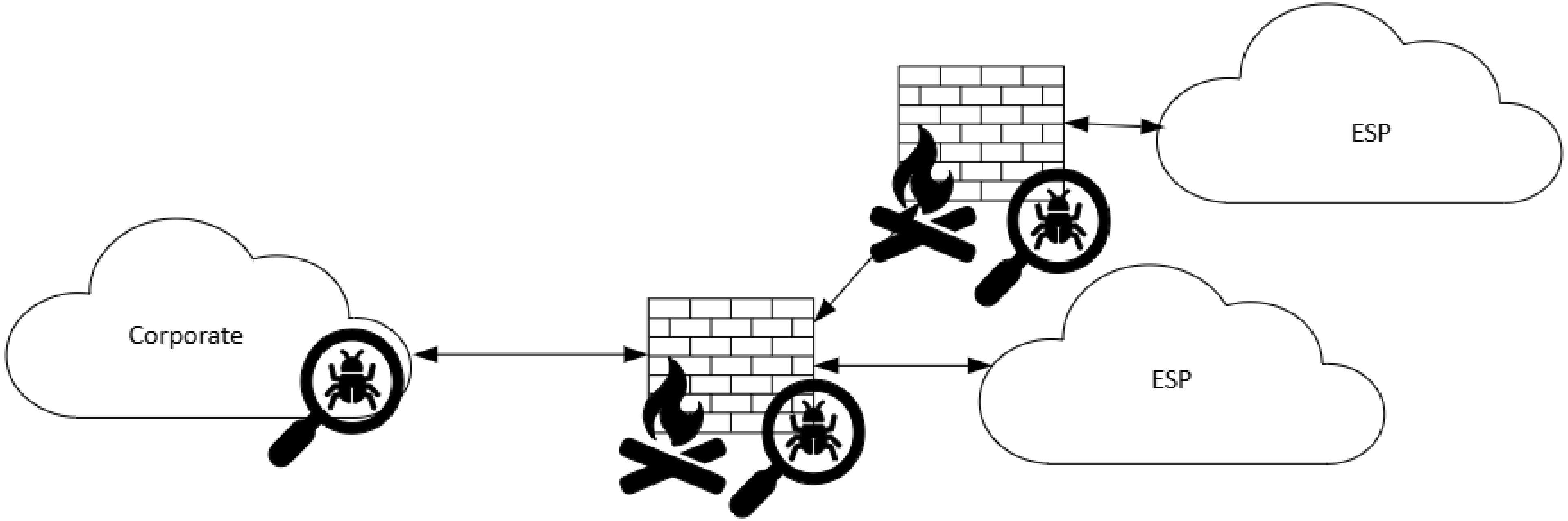
WHY INSM?

- Internal threats are increasing and becoming more sophisticated
  - Supply Chain
  - Insider threats
  - State-sponsored attacks
- Traditional defenses are no longer sufficient

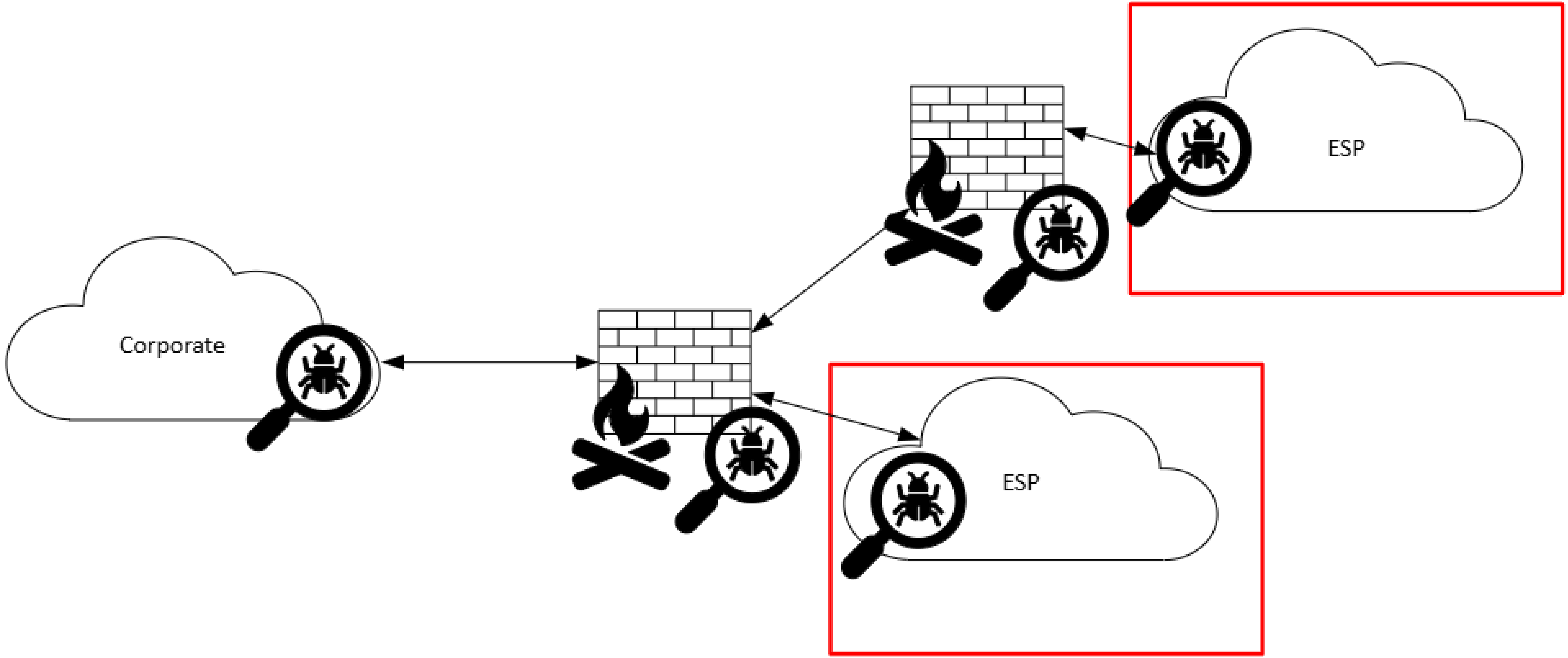
INSM provides:

- Real-time or near-real-time detection of anomalies
- Better network behavior understanding
- Improved incident response capabilities

BEFORE INSM…



AFTER INSM…



Do not edit
How to change the design

Where are you on your Internal Network Security Monitoring implementation?

ⓘ The Slido app must be installed on every computer you’re presenting from

slido

FERC ORDERS

- FERC Order No. 907 (June 2025), and Order No. 907-A (August 2025) approving Reliability Standard CIP-015-1, require Internal Network Security Monitoring (INSM) inside an entity's electronic security perimeter and directing modifications to extend protections to access control systems outside of the electronic security perimeter

CIP-015-1 REQUIREMENTS

R1. [I]mplement one or more documented process(es) for internal network security monitoring of networks protected by the Responsible Entity's Electronic Security Perimeter(s) of high impact BES Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity to provide methods for detecting and evaluating anomalous network activity.

1.1. Implement, using a risk-based rationale, network data feed(s) to monitor network activity; including connections, devices, and network communications.

1.2. Implement one or more method(s) to detect anomalous network activity using the network data feed(s) from Part 1.1.

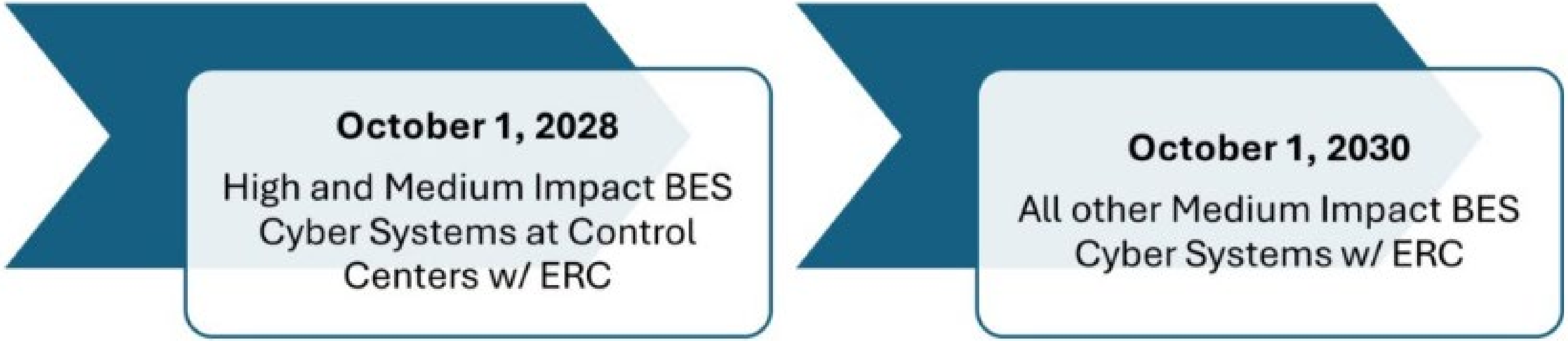
1.3. Implement one or more method(s) to evaluate anomalous network activity detected in Part 1.2. to determine further action(s).

CIP-015-1 REQUIREMENTS

R2. [I]mplement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity at a minimum until the action is complete in support of Requirement R1, Part 1.3.

R3. [I]mplement, except during CIP Exceptional Circumstances, one or more documented process(es) to protect internal network security monitoring data collected in support of Requirement R1 and data retained in support of Requirement R2 to mitigate the risks of unauthorized deletion or modification.

IMPLEMENTATION



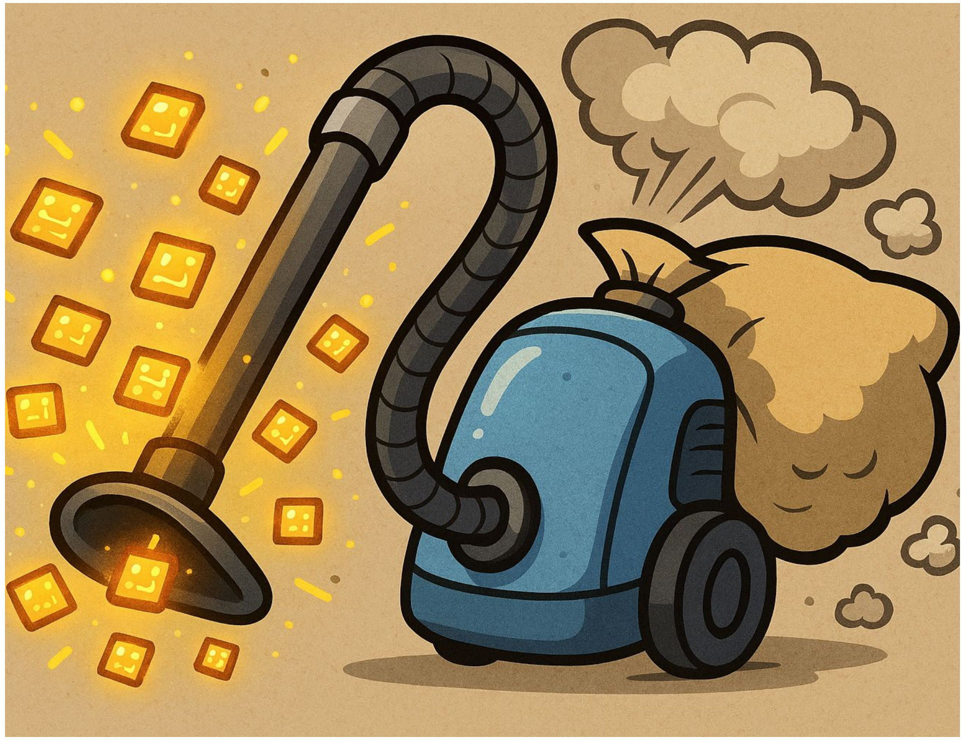
October 1, 2028

High and Medium Impact BES Cyber Systems at Control Centers w/ ERC

October 1, 2030

All other Medium Impact BES Cyber Systems w/ ERC

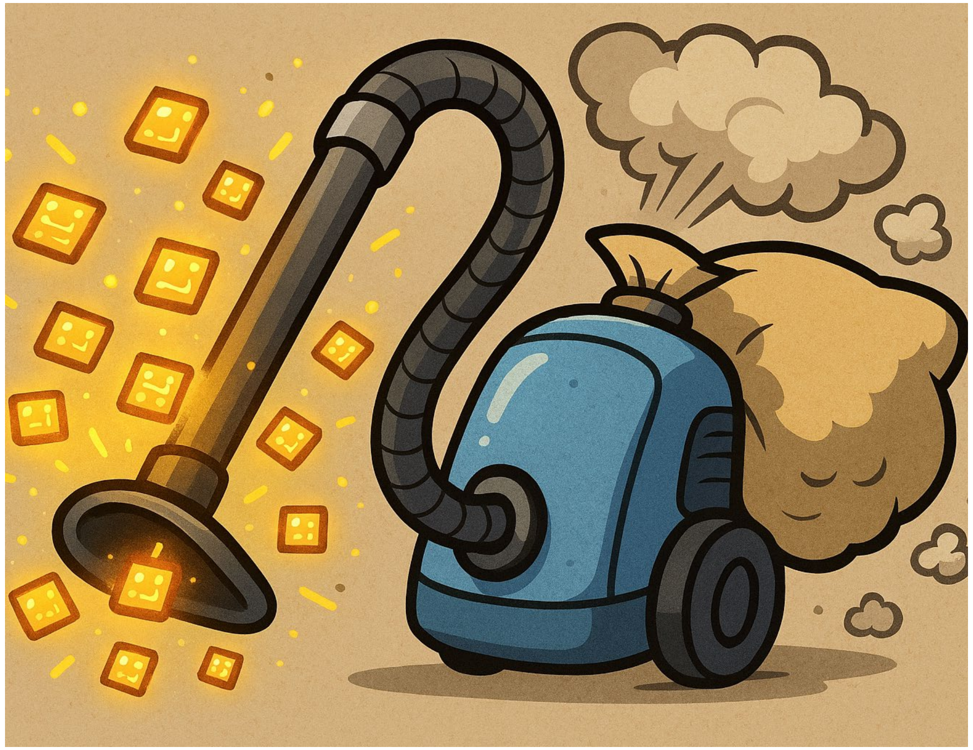
NETWORK MONITORING STRATEGY



If this effort has not been started within your organization, you will need to invest resources and time to:

- Identify what capabilities and information you have in your different environments today e.g. EMS vs. Substation vs. Generation plant

NETWORK MONITORING STRATEGY CONTINUED



- Potentially invest in additional technology, sensors, and storage
- Potentially invest in training or additional personnel to perform INSM
- Develop Baselines of the network to be able to understand “what is anomalous”

POSSIBLE CHALLENGES

Legacy systems may prove difficult to adapt

Lack of visibility for certain systems

Resource constraints – both personnel and equipment

False positive tuning and alert fatigue from defining "normal" network behavior

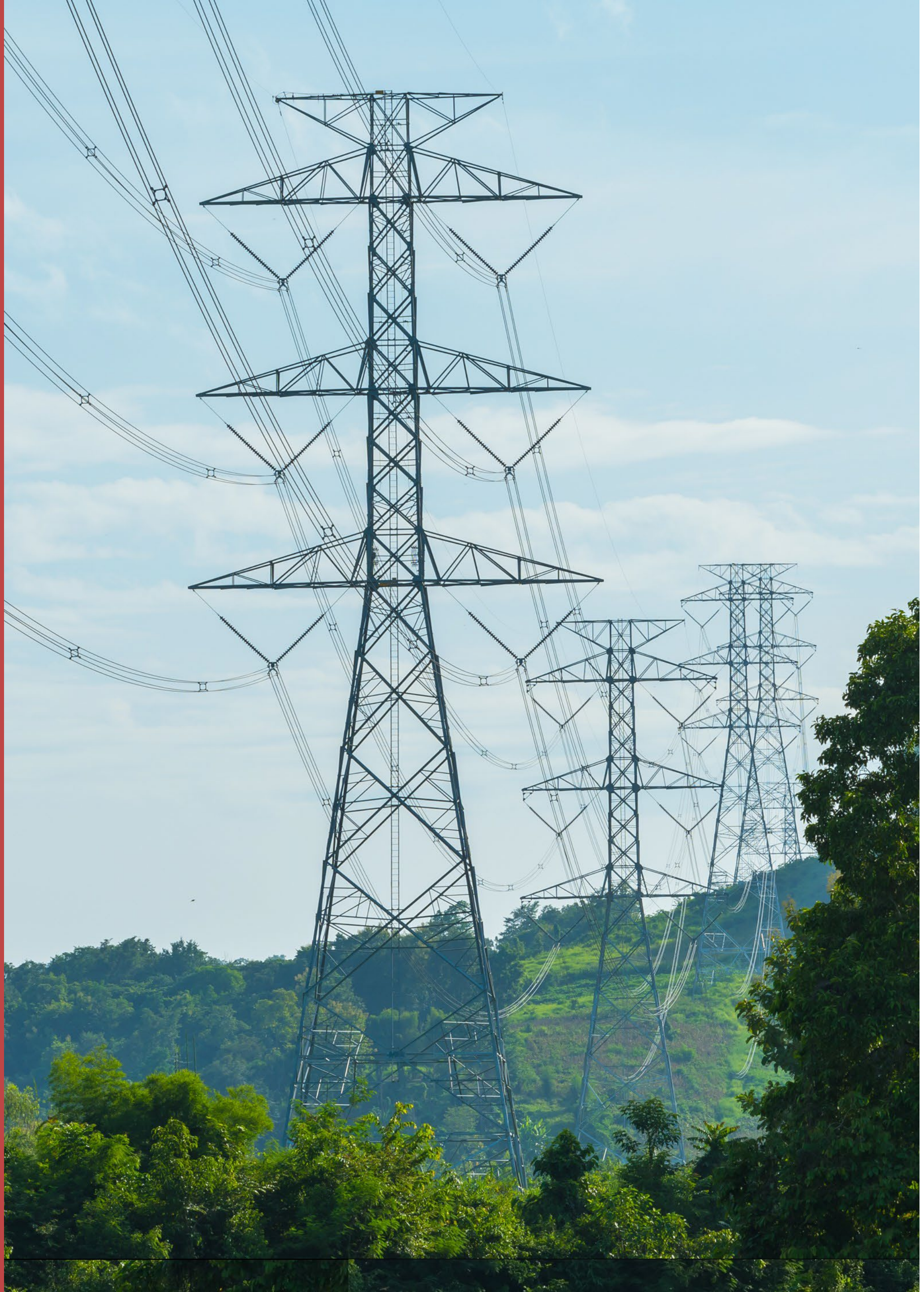
COMPLIANCE CONSIDERATIONS

- Document, document, document
- Maintain up-to-date network diagrams and detection rules
- Document monitoring rules and network flows
- Maintain logs and alerting evidence
- Incident Response Plans – test and update
- Demonstrate that all applicable assets were considered when developing the risk-based monitoring plan
- Start the process/planning early

LINKS

- CIP-015-1
- Project 2023-03 Internal Network Security Monitoring (INSM)
- Implementation Plan
- FERC Order 907
- FERC Order 907-A
- MRO Article: Reliability Standard CIP-015-1 and the Internal Network Security Monitoring (INSM) Journey (September 30, 2025)
- SRP's Journey for INSM: Johnson-Barbier, M., & Heyen, B. (2024, October 10) Internal Network Security Monitoring (INSM). Vimeo

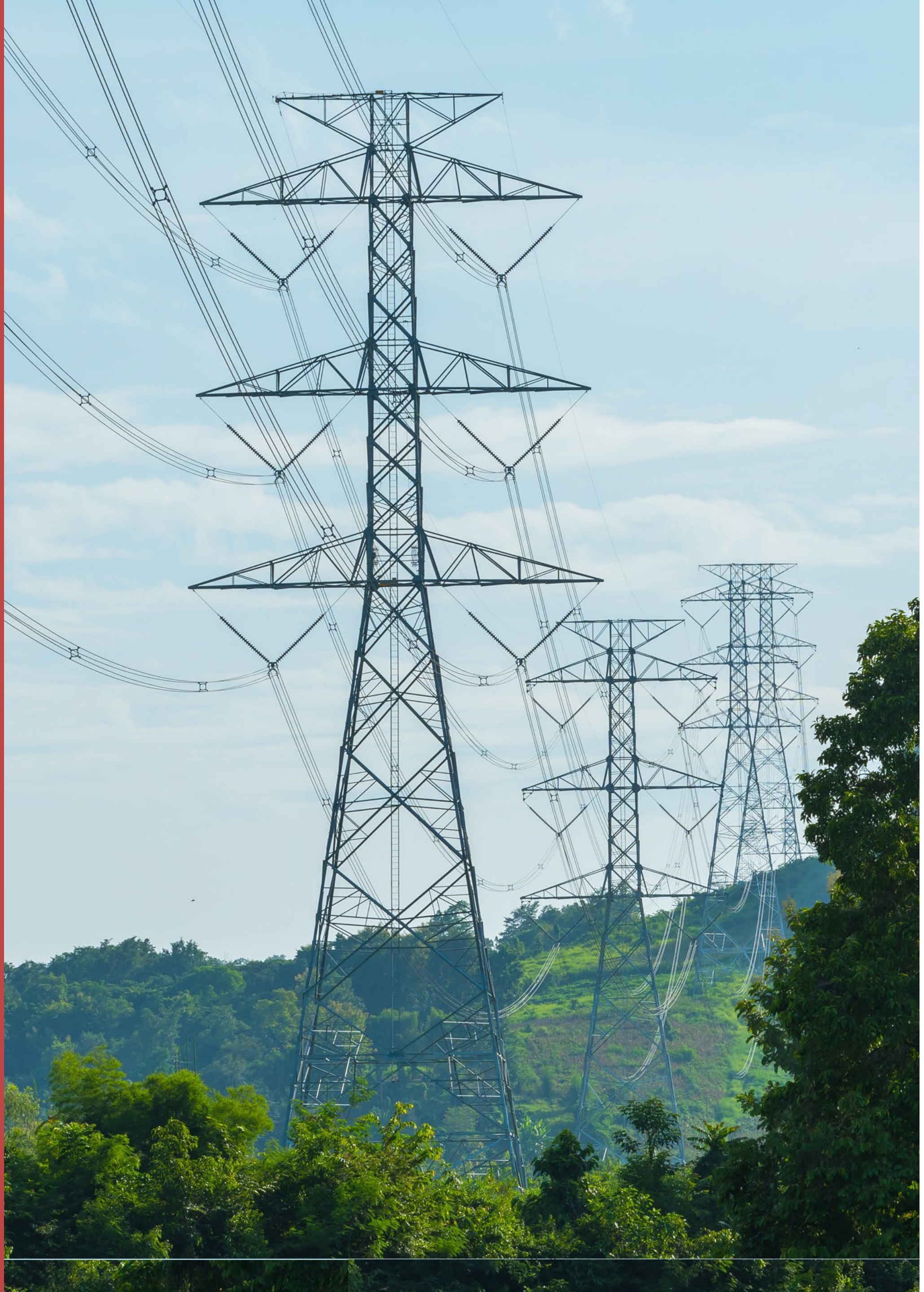
FORWARD TOGETHER RELIABILITYFIRST



QUESTIONS & ANSWERS

Ron Ross

ron.ross@rfirst.org



THANK YOU

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

Webinar Link

Join the conversation at SLIDO.com

#TechTalkRF