

WELCOME TO TECHNICAL TALK WITH RF

September 9, 2024





TECHNICAL TALK WITH RF

Join the conversation at

[SLIDO.com](https://www.slido.com)

#TechTalkRF

TECHNICAL TALK WITH RF

Follow us on



[Linkedin.com/company/reliabilityfirst-corporation](https://www.linkedin.com/company/reliabilityfirst-corporation)

A screenshot of the ReliabilityFirst Corporation LinkedIn profile. The header features a banner image of power lines at sunset. The profile name is "ReliabilityFirst Corporation" with a notification bell icon. Below the name is the tagline "RF works to maintain the reliability, security and resilience of the electric grid in the Mid-Atlantic region" and the location "Utilities · Cleveland, OH · 3,970 followers · 101 employees". A section indicates "Brian & 85 other connections work here" with buttons for "Following", "Invite", and "More". Navigation tabs include "Home", "My Company", "About", "Posts", "Jobs", and "People". The "Posts" tab is active, showing a post from "ReliabilityFirst Corporation" with 3,970 followers, dated "2d". The post text reads: "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 w...see more". The post includes two images: one of a group of staff posing in front of a brick building, and another of staff working on a garden bed.

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](#):

- [2024 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 V8.1 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 [2023 Impact Report](#)




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.

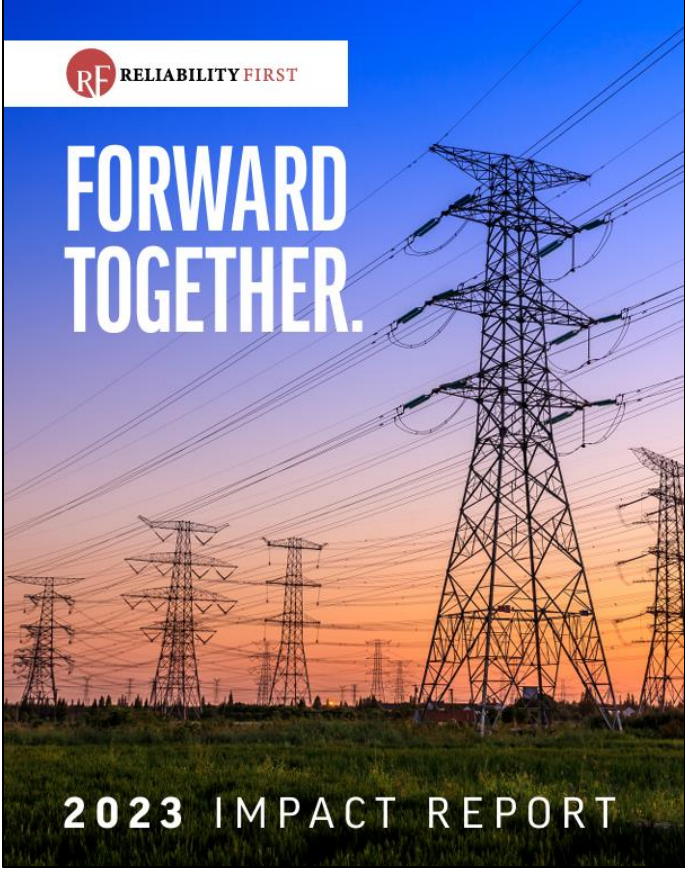
[Click here to read more](#)

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](#)



FORWARD TOGETHER.

2023 IMPACT REPORT

WELCOME TO TECHNICAL TALK WITH RF

September 9, 2024



TECH TALK ANNOUNCEMENT



2024 Interregional Transfer Capability Study Phase 1 2024 ITCS Phase 1 Assessment

NERC published the second in a series of three draft documents that will be merged into the final Interregional Transfer Capability Study (ITCS), which is being produced in response to the congressional directive in the Fiscal Responsibility Act of 2023. The study will be filed with the Federal Energy Regulatory Commission (FERC) by December 2, 2024, and will be followed by a FERC public comment period.



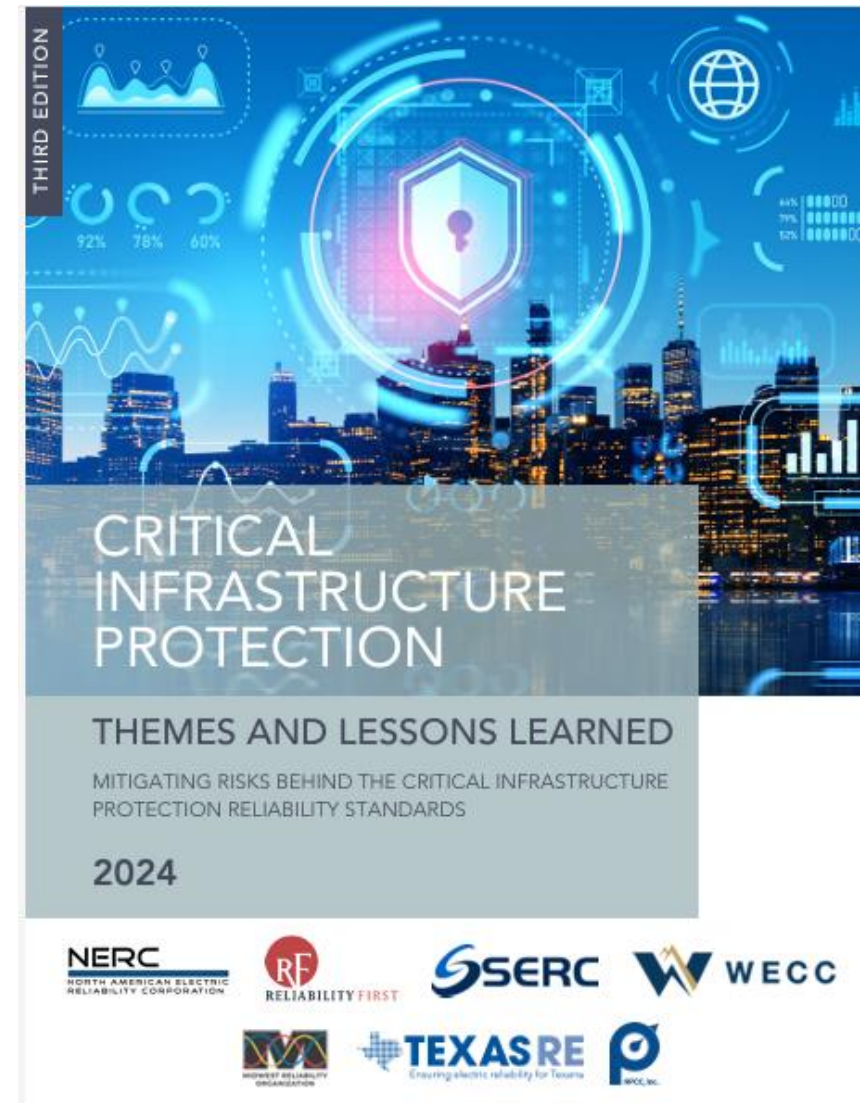
TECH TALK ANNOUNCEMENT



Critical Infrastructure Protection Themes And Lessons Learned

[CIP Themes Report](#)

NERC and the six Regional Entities (collectively the ERO Enterprise) have identified four risk themes that have made it difficult for some entities to mitigate risks associated with the NERC Critical Infrastructure Protection (CIP) Reliability Standards. To communicate these themes and possible resolutions to them, the ERO Enterprise developed the ***2024 Critical Infrastructure Protection Themes and Lessons Learned*** report.



TECH TALK ANNOUNCEMENT



Physical Security Regional Workshop

[Registration](#)

September 25, 8:30-5:00 PM CT

E-ISAC is partnering with ReliabilityFirst, EPRI, ComEd, Edison Electric Institute, the National Rural Electric Cooperative Association and the American Public Power Association to host this regional physical security workshop. In response to the evolving physical threat environment impacting the electric industry, we invite you to join a free discussion about the current threat landscape, mitigation strategies, and lessons learned.

Registration is free and is open to utilities, select government and law enforcement partners. This is an in-person only event, travel and accommodations are not included in participant registration. Lunch will be provided. This workshop is not open to the media.

If you have questions, please contact memberservices@eisac.com

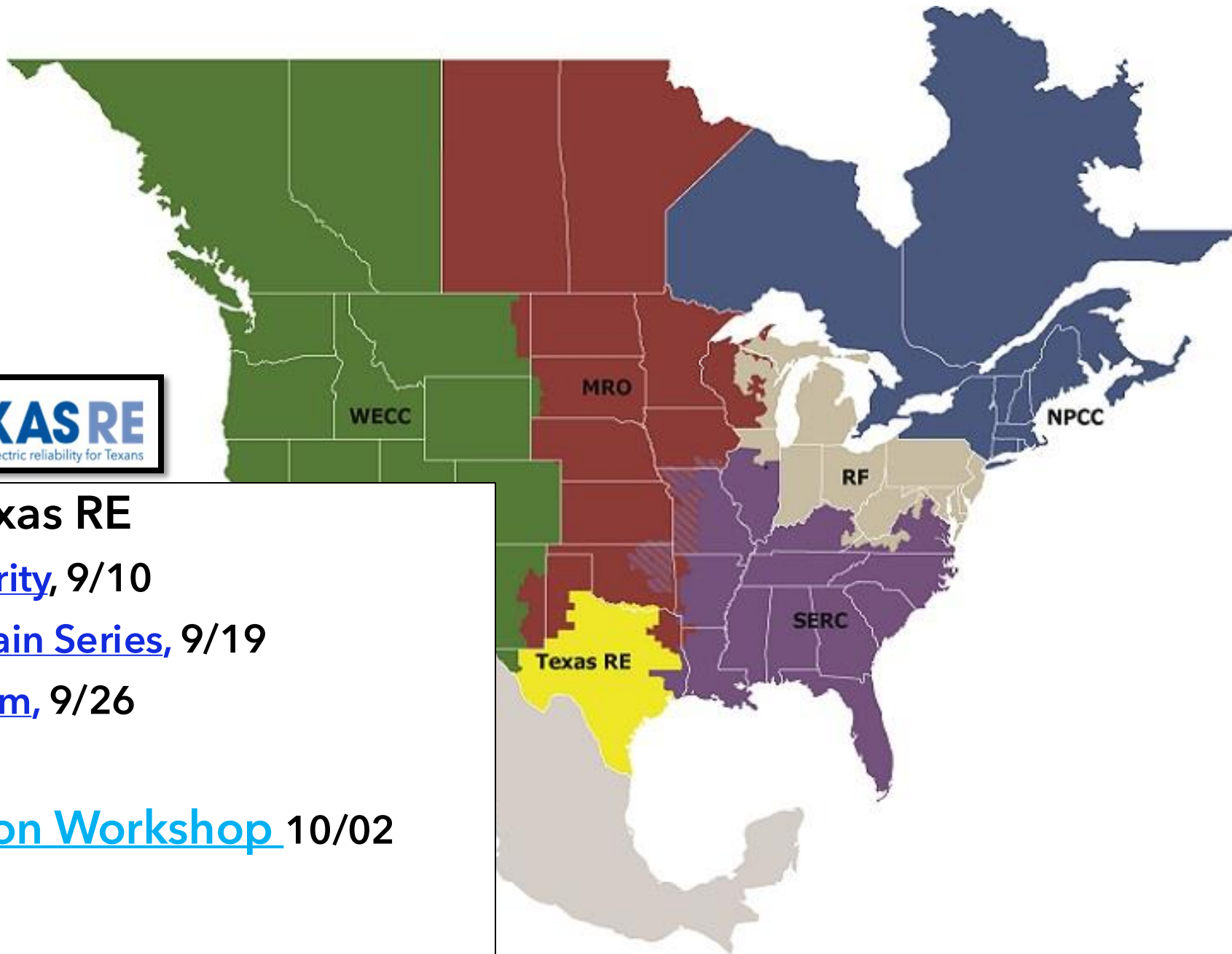




Talk with Texas RE

- [Cybersecurity](#), 9/10
- [Supply Chain Series](#), 9/19
- [Policy Forum](#), 9/26

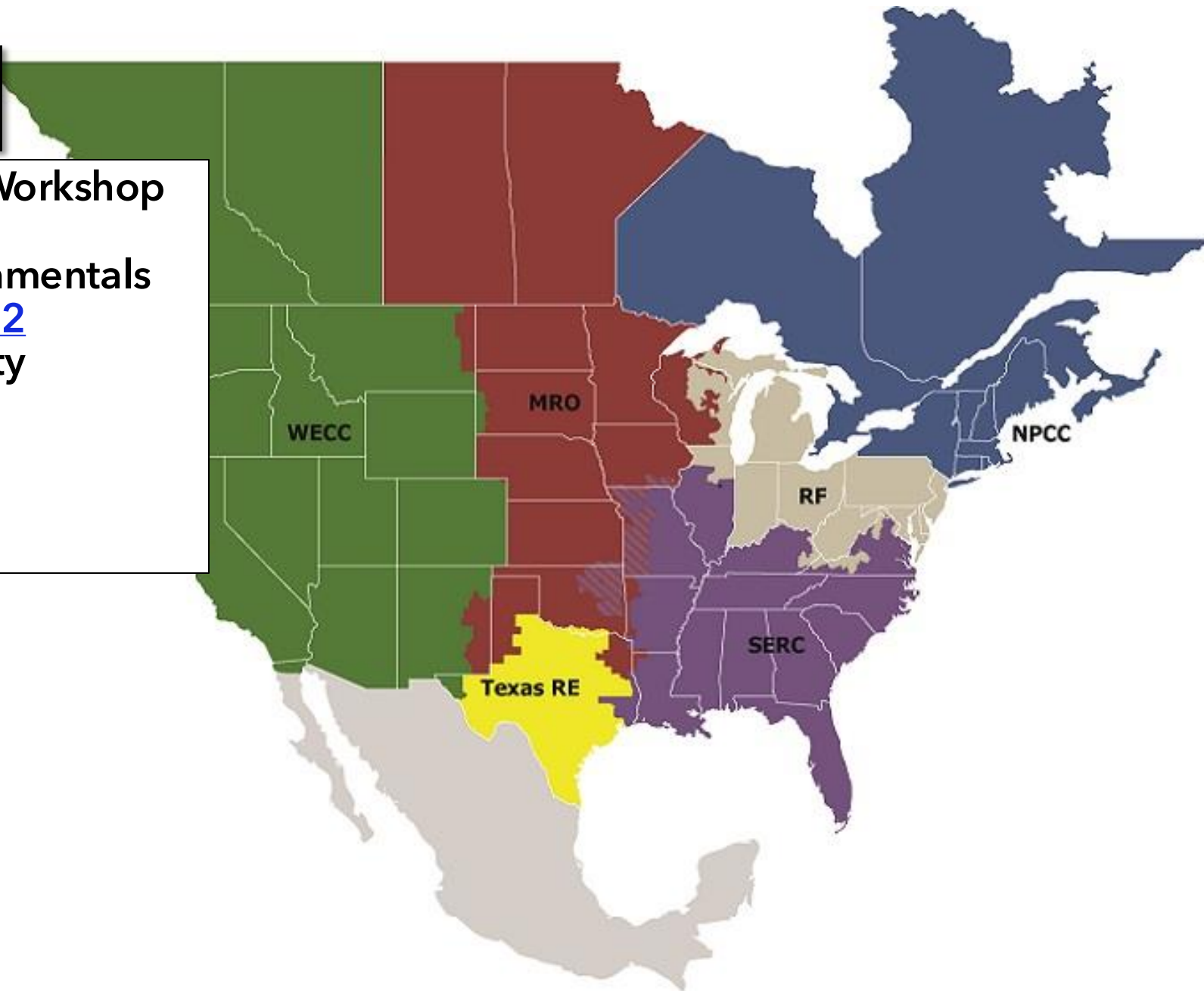
[Winterization Workshop](#) 10/02





Winter Readiness Workshop

- [September 10](#)
Enforcement Fundamentals
- [September 11-12](#)
Reliability & Security
Oversight Update
- [September 19](#)



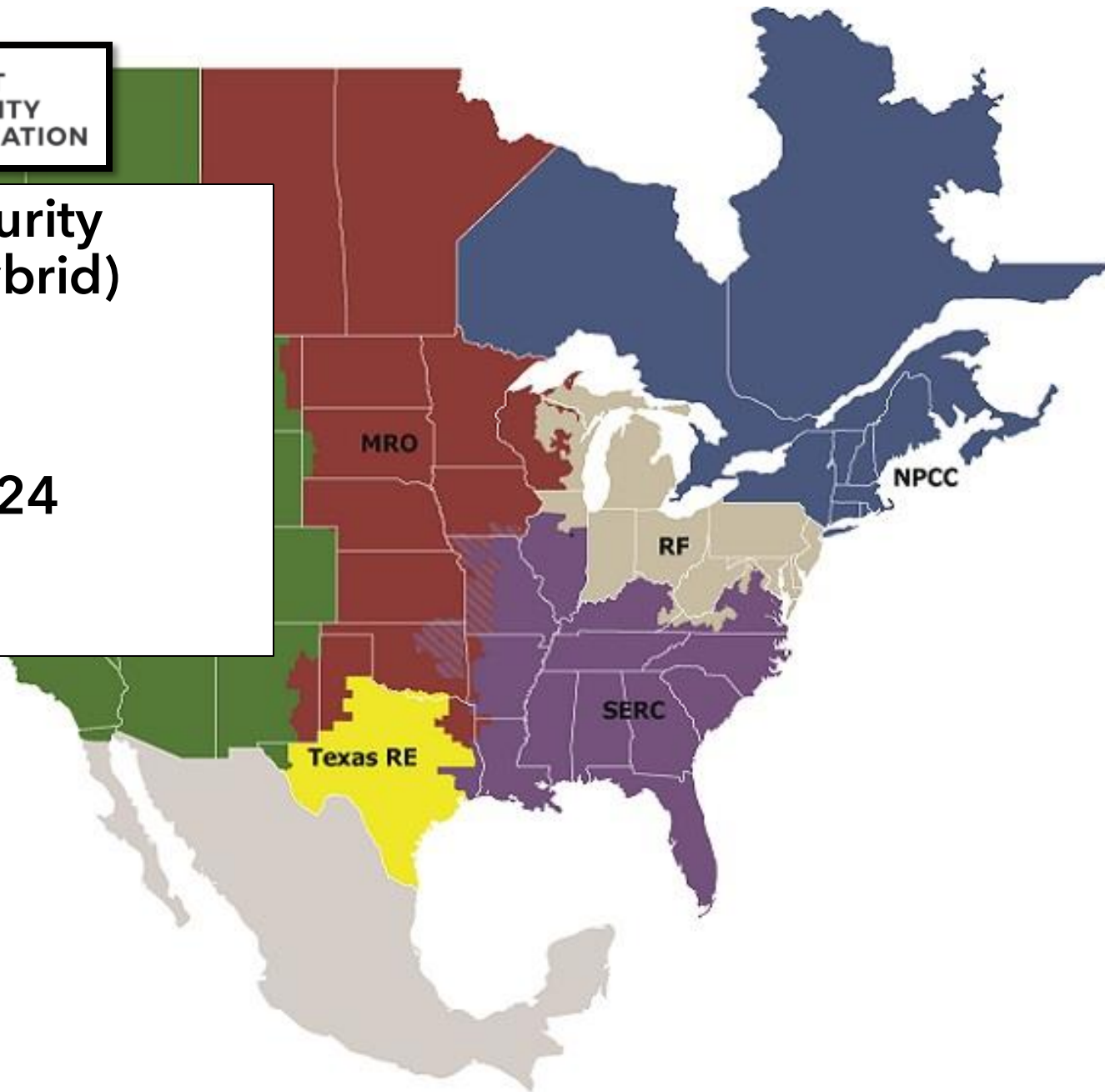


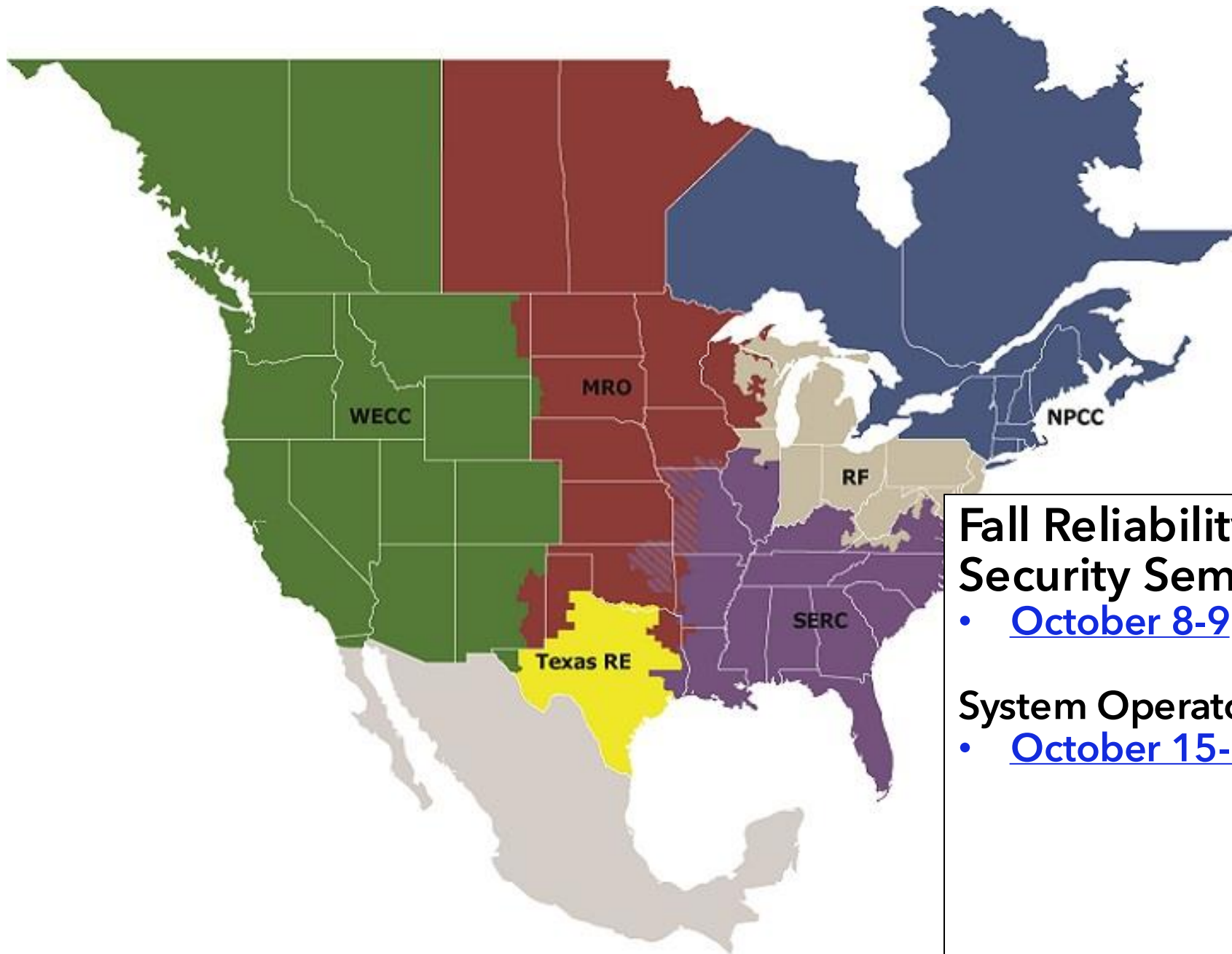
2024 MRO Security Conference (Hybrid)

- [October 1-3](#)

GridSecCon 2024

[October 22nd - 25th](#)



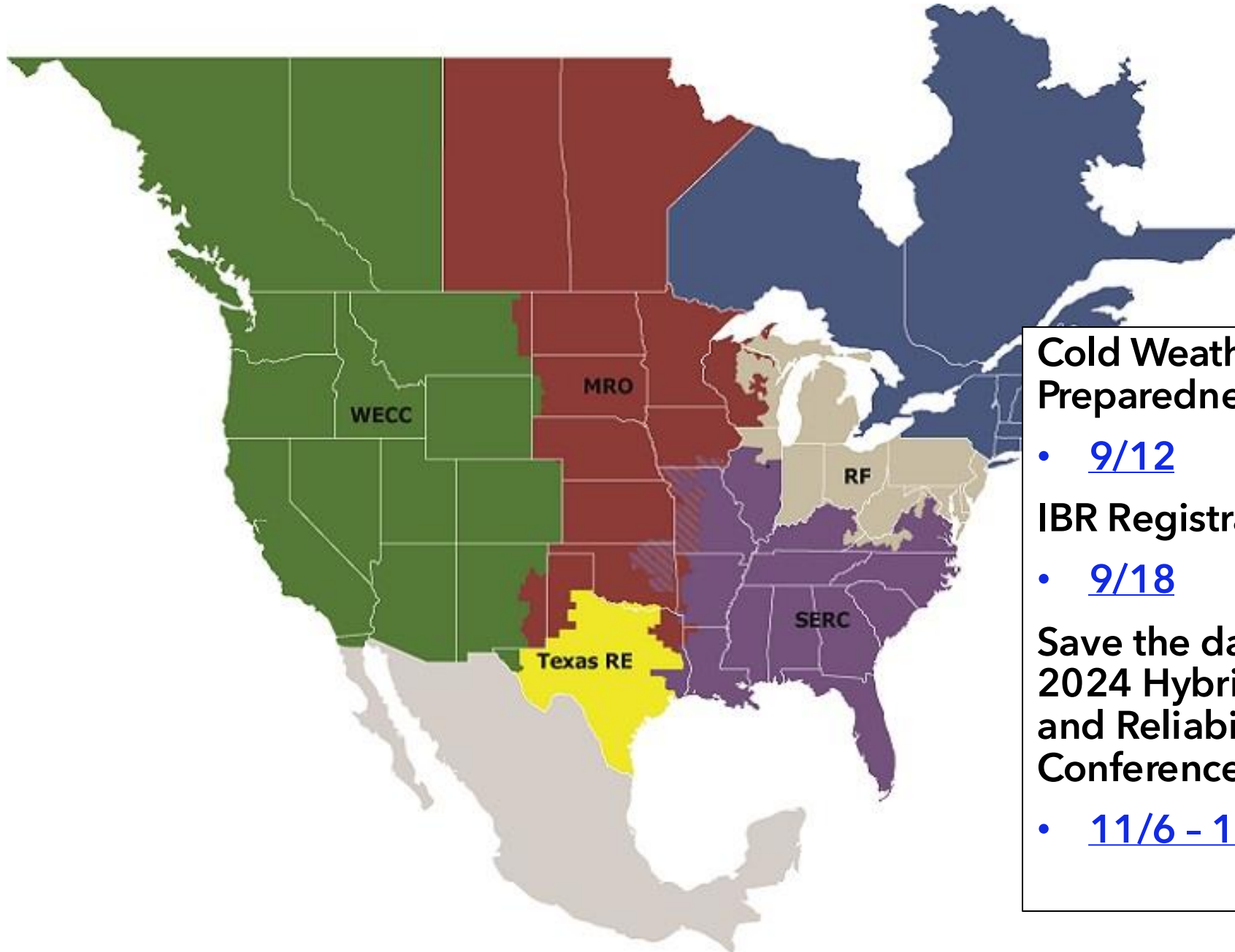


Fall Reliability and Security Seminar

- [October 8-9](#)

System Operator Conference

- [October 15-17](#)



Cold Weather Preparedness Webinar

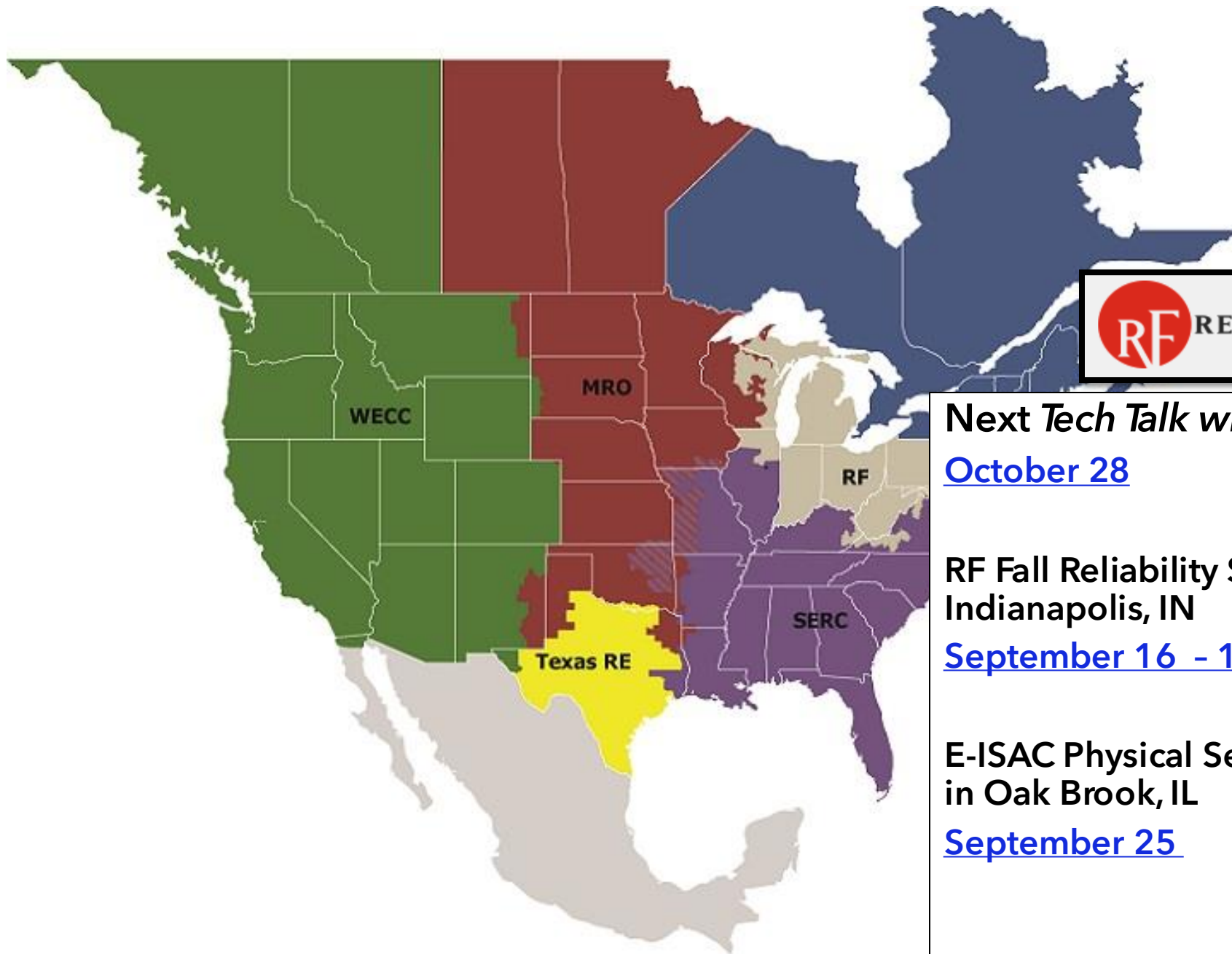
- [9/12](#)

IBR Registration Initiative

- [9/18](#)

Save the date: NPCC Fall 2024 Hybrid Compliance and Reliability Conference

- [11/6 - 11/7](#)



Next Tech Talk with RF
[October 28](#)

**RF Fall Reliability Summit,
Indianapolis, IN**
[September 16 - 18](#)

**E-ISAC Physical Security Workshop
in Oak Brook, IL**
[September 25](#)

TECH TALK ANNOUNCEMENT



FALL RELIABILITY & SECURITY SUMMIT



SEPT. 16-18, 2024



INDIANAPOLIS



Featuring an energy policy legislator panel with:

Brian Feldman
Maryland State Senator



Stephanie Hansen
Delaware State Senator



Eric Koch
Indiana State Senator



Dick Stein
Ohio State Representative



TECH TALK REMINDER

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

CLICK HERE

September 2024

MON
9

September 9 @ 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

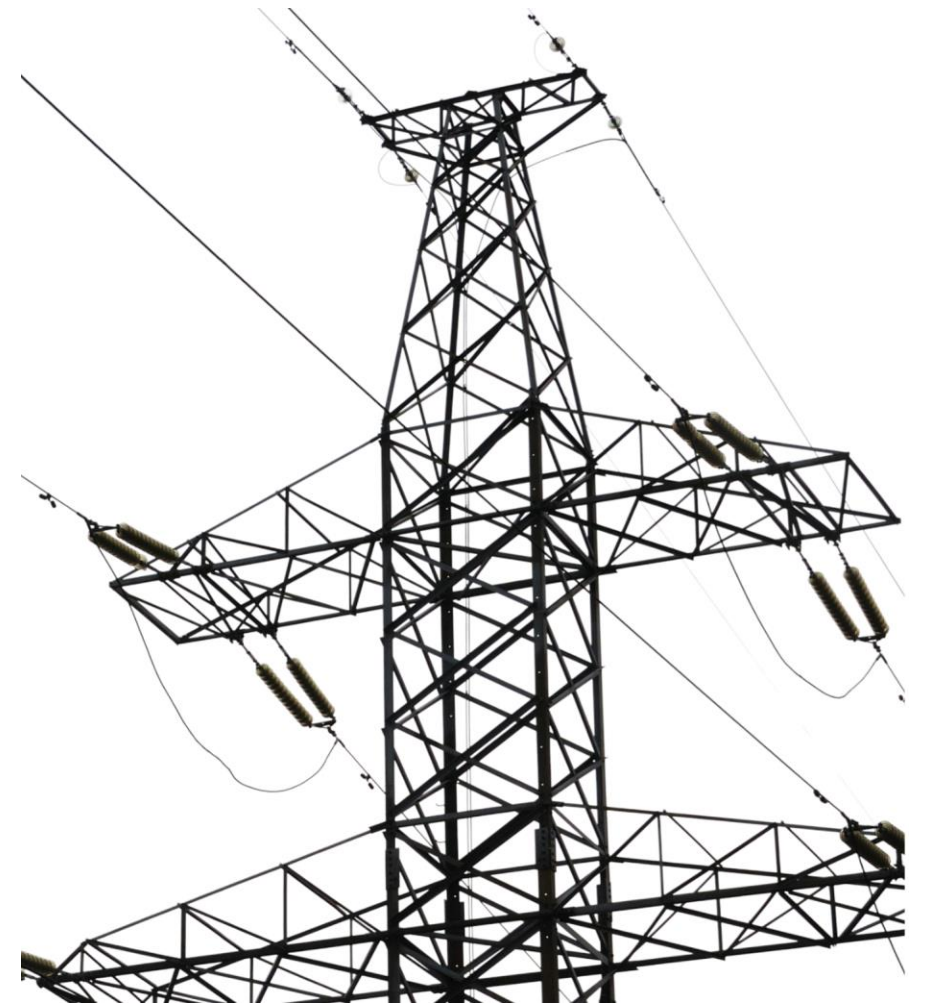
[SLIDO.com](https://www.slido.com)

#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

EVENT ANALYSIS UPDATE

- **DWAYNE FEWLESS**, PRINCIPAL ANALYST, OPERATIONAL ANALYSIS & AWARENESS, RF

RISK ASSESSMENT GUIDELINES OVERVIEW

- **SHAWN BARRETT**, PRINCIPAL ANALYST, RISK ANALYSIS & MITIGATION, RF

EAP V5 AND THE EVENT ANALYSIS PROCESS

Dwayne Fewless, Principal Analyst,
Operational Analysis and Awareness, RF

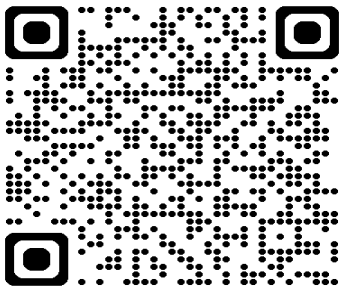
Tech Talk with RF, Sept. 9, 2024



RELIABILITY FIRST

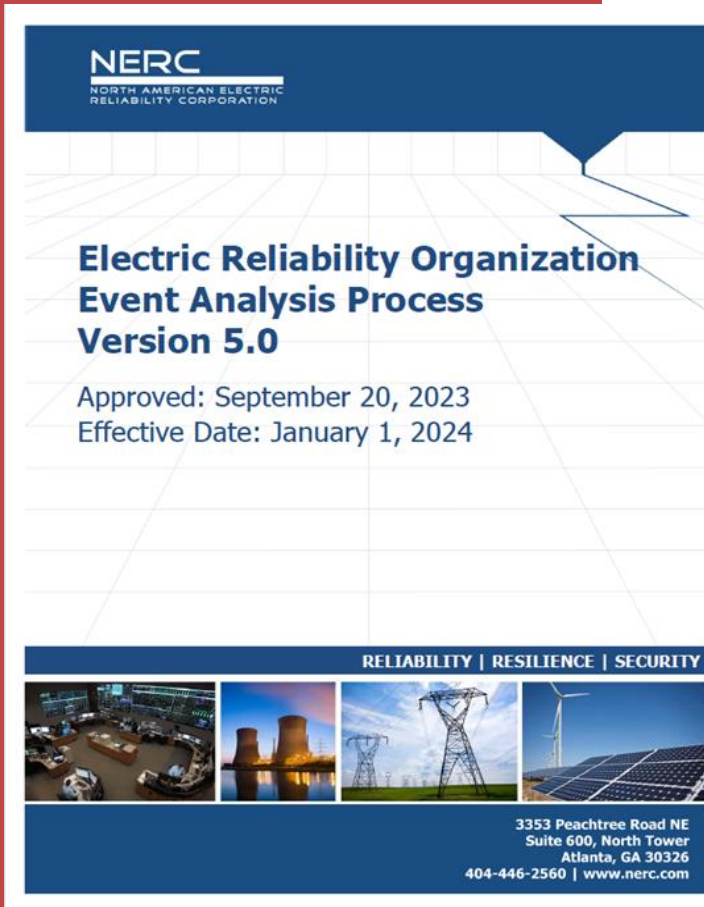
AGENDA

- EAP V5 UPDATE THEMES
- NERC LESSONS LEARNED
- EVENT ANALYSIS AND THE RF REGION

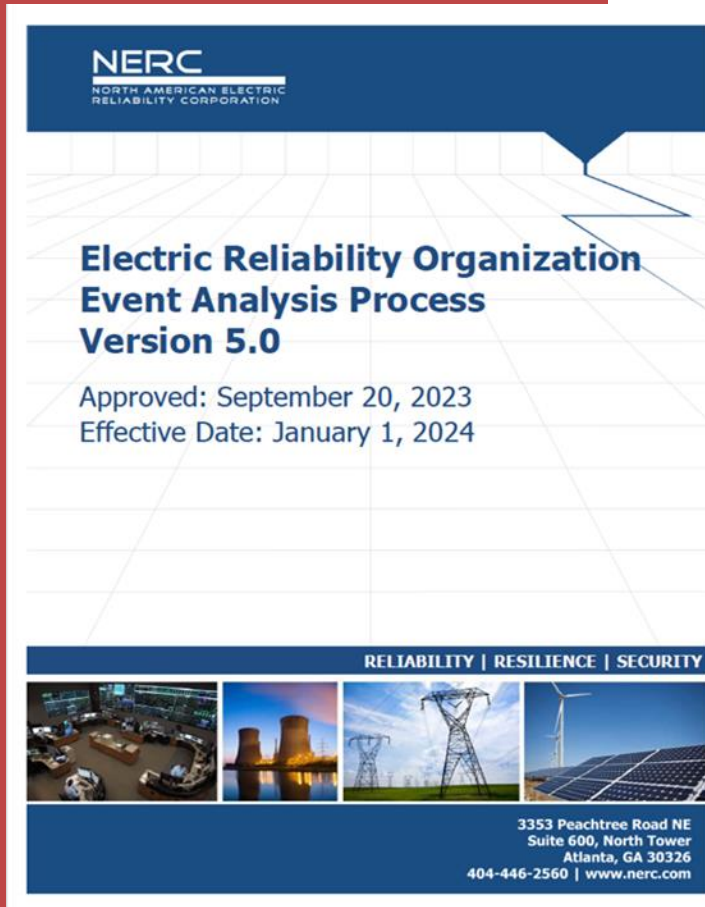


EAP V5 UPDATE THEMES

- Events Analysis Subcommittee (EAS)-Led Periodic Review
- Industry Comment Period
 - April 5 -May 19, 2023
- 57 Comments from 10 different entities

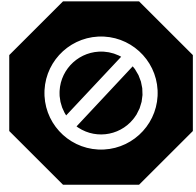


EAP V5 UPDATE THEMES



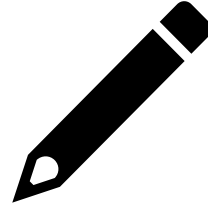
- Update the Introduction section to provide additional background information regarding the Event Analysis Program - “Why”
- Update the Process Overview section to provide additional background information regarding the Event Analysis Process - “How”
- Revise the ERO Event Analysis Process section to provide clarity and describe changes to event categorization definitions that include the following...

EAP V5 UPDATE THEMES



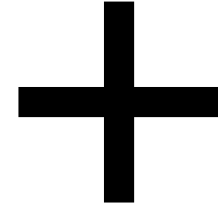
RETIRE

- Retire Category 1b
- Retire Category 1d



REVISE

- Revise Category 1e, 2e, 2f, and 2g definitions to provide clarity
- Revise Category 1h definition in accordance with the recommendation of the EMS Working Group to provide clarity



COMBINE

- Combine Categories 3, 4, & 5 into a single Category 3



EAP V5 SUPPORTING MATERIAL

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

About NERC Career Opportunities Governance Committees Program Areas & Departments Standards Initiatives R

Event Analysis
EA Program
Lessons Learned
Event Reports
Reliability Coordinators
Transmission Loading Relief (TLR) Procedure

Home > Program Areas & Departments > Reliability Risk Management > Event Analysis > EA Program

EA Program

The principal goal of the ERO is to promote the reliability of the bulk power system in North America by performing event analyses in North America. Through the event analysis process, the ERO strives to improve operations, planning, and critical infrastructure protection (CIP) processes. The event analysis process provides guidance by identifying and disseminating valuable information to owners, operators, and users of the system. The process for addressing event analysis, provides a robust lessons learned process, and facilitates communication.

The ERO Event Analysis Process Document - Version 4 was endorsed by the Operating Committee in 2020.

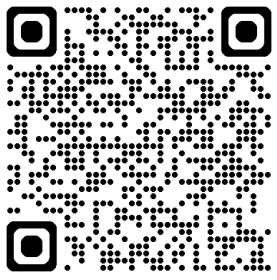
ERO Event Analysis Process Documents	
Type	Title
Current Event Analysis Process Documents (13)	
ERO Event Analysis Process - Version 4 (Effective January 1, 2020) (7)	
ERO Event Analysis Process - Version 5 (Effective January 1, 2024) (6)	

EA Program

Type	Title
Reference Materials for Cause Analysis Methods and Tools (3)	

Previous version,
EAP V4

EAP V5, effective
Jan. 1, 2024



NERC LESSONS LEARNED

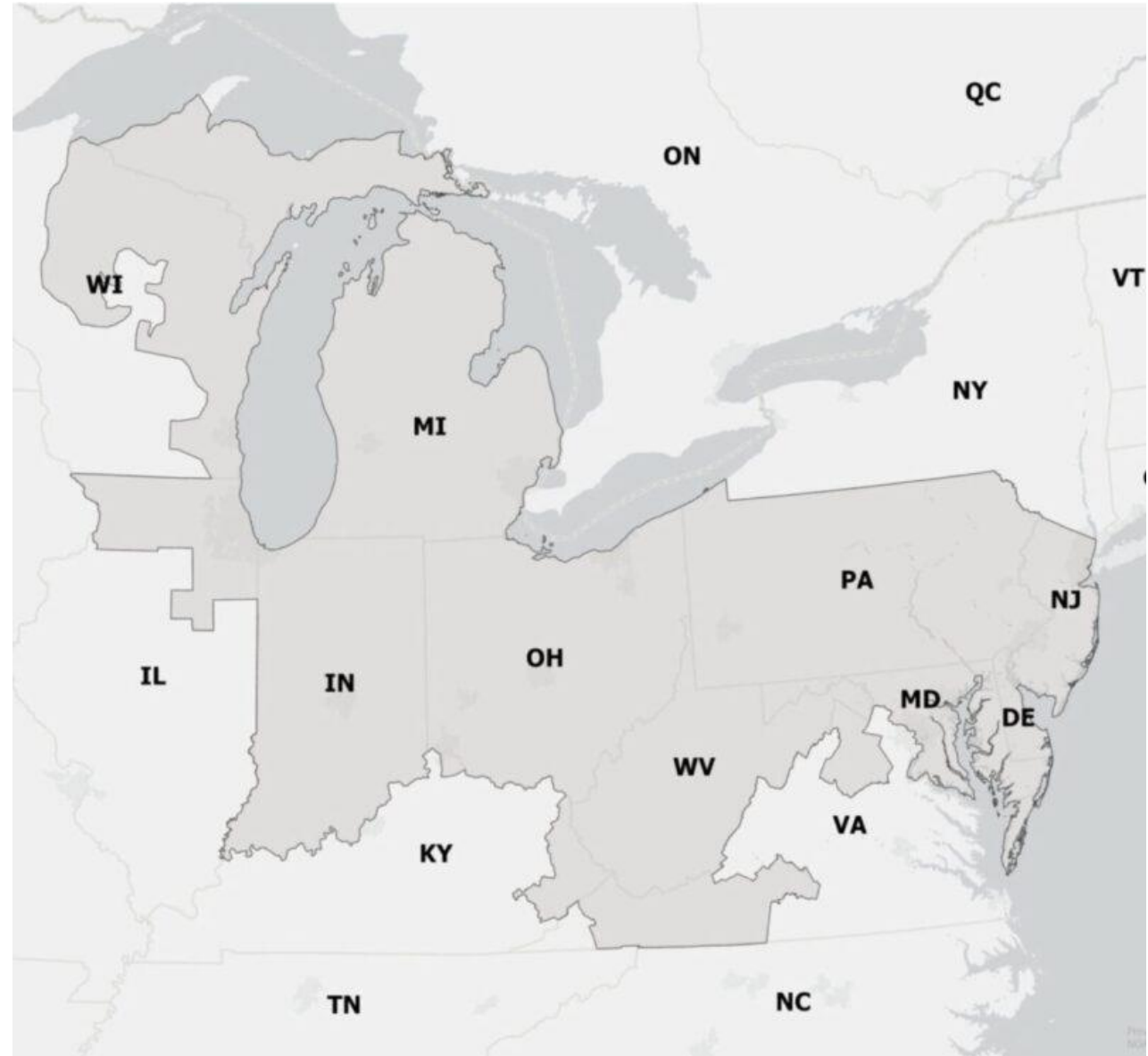
The screenshot shows the NERC website's 'Lessons Learned' page. The header includes the NERC logo and navigation links: About NERC, Career Opportunities, Governance, Committees, Program Areas & Departments, and Standards. The left sidebar lists: Event Analysis, EA Program, Lessons Learned (highlighted), Event Reports, Reliability Coordinators, and Transmission Loading Relief (TLR) Procedure. The main content area shows the breadcrumb path: Home > Program Areas & Departments > Reliability Risk Management > Event Analysis > Lessons Learned. A disclaimer states: 'Disclaimer for Lessons Learned: These documents are designed to convey information and are not intended to be determined based on language in the NERC Reliability Code. For a brief summary of the lessons learned that have been posted, please click on the links below.' Below this is a table with columns 'Type' and 'LL#'. The table lists lessons learned from 2010 to 2024, with counts in parentheses: 2024 (2), 2023 (6), 2022 (13), 2021 (12), 2020 (11), 2019 (11), 2018 (15), 2017 (9), 2016 (13), 2015 (16), 2014 (19), 2013 (14), 2012 (18), 2011 (22), and 2010 (23).

- **NERC Lessons Learned**

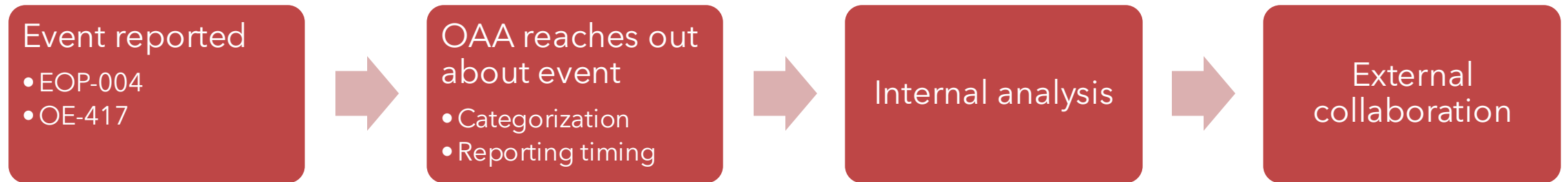
- Events that industry can learn from
- Completely anonymous
- Written as a combined team

EVENTS ANALYSIS AND THE RF REGION

- The process
- The codes
- Inside of RF events



THE PROCESS



ANALYSIS & CAUSE CODING

- **A1** - Design and Engineering
- **A2** - Equipment and Maintenance
- **A3** - Individual Human Performance
- **A4** - Management/Organization
- **A5** - Communications
- **A6** - Training
- **A7** - Other
- **AZ** - Information to determine cause LTA

INSIDE RF EVENTS



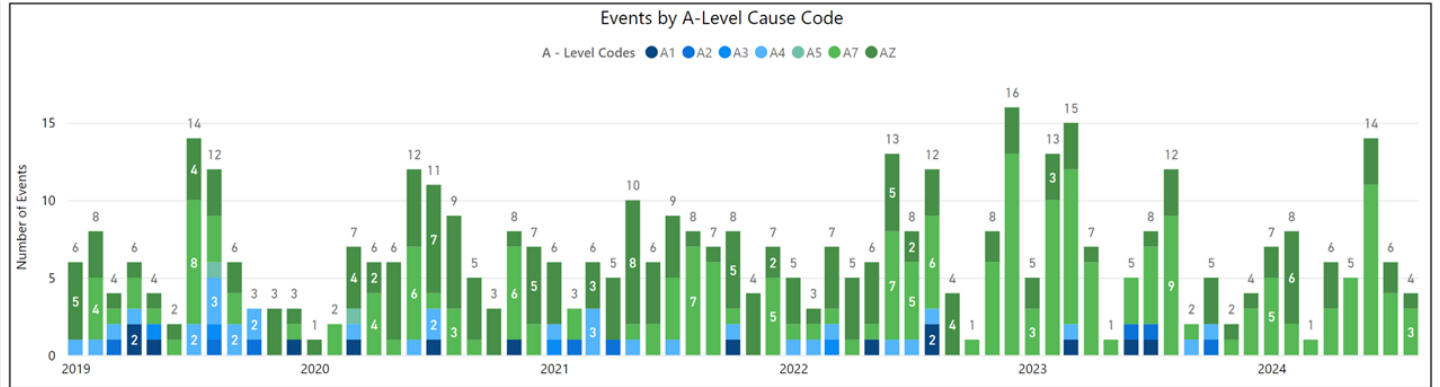
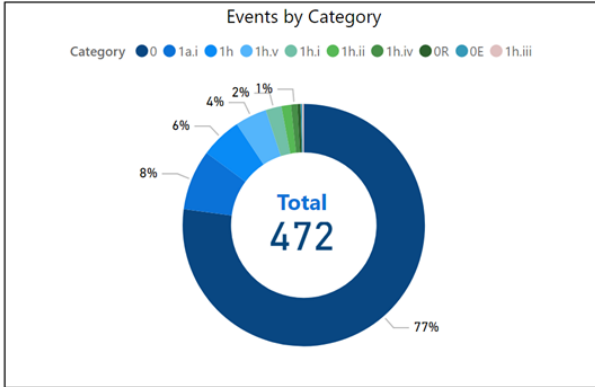
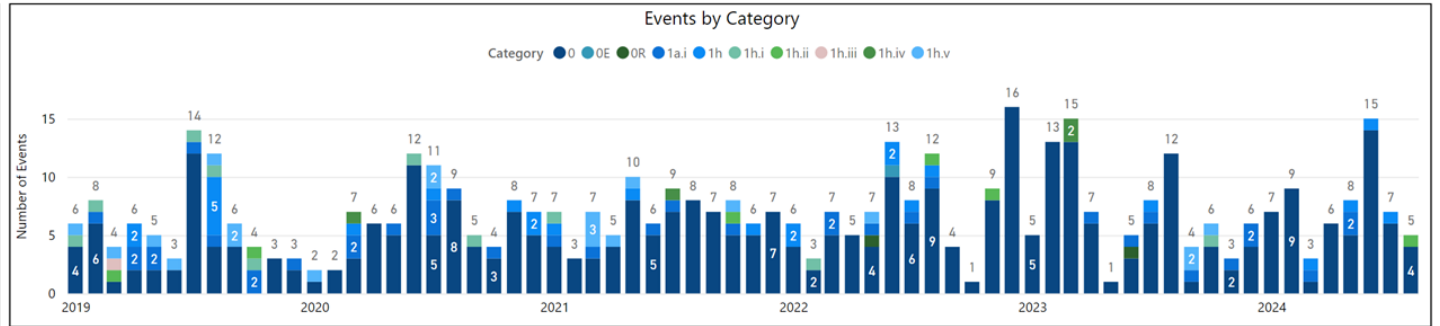
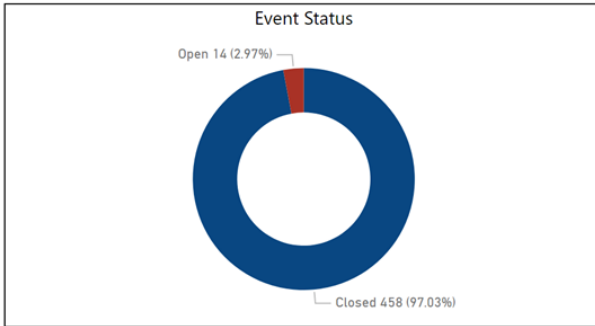
OPERATIONAL ANALYSIS & AWARENESS Events Dashboard

1/1/2019 12/31/2024

Entity Name

14
Open Events

Show Events Details



INSIDE RF EVENTS

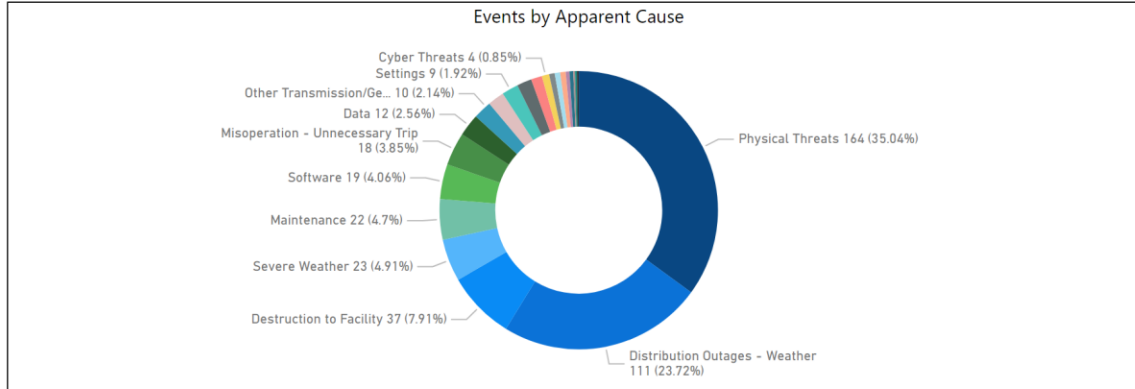


OPERATIONAL ANALYSIS & AWARENESS

Event Characteristics Dashboard

1/1/2019 12/31/2024

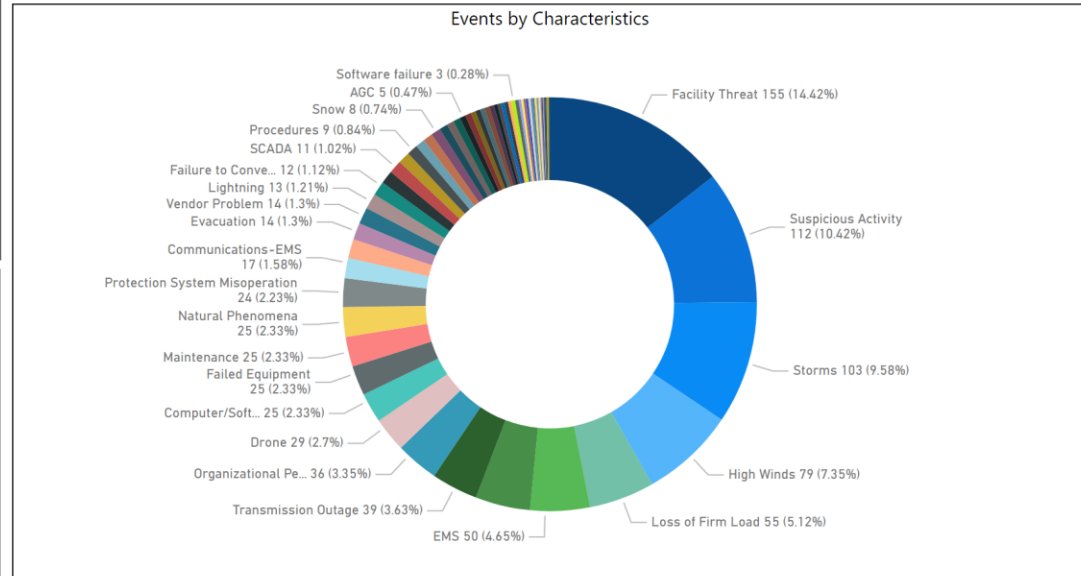
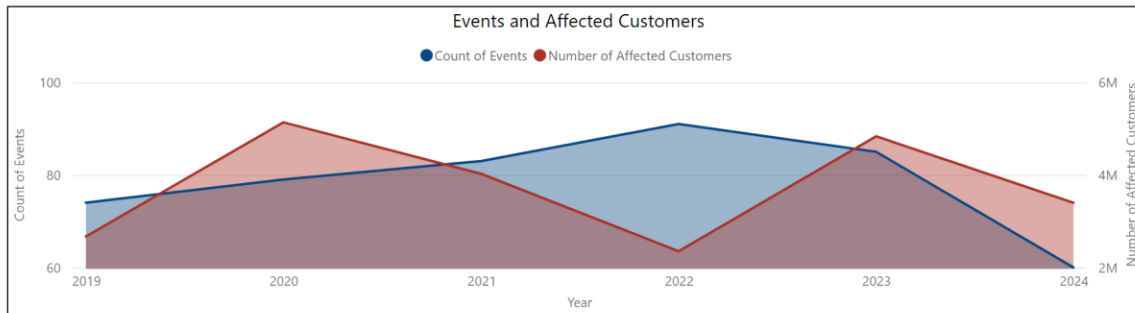
Entity Name



Total Events
472

Affected Customers (As Reported by Entity)
22.41M

EMS Filter
All



"Coming together is a beginning. Keeping together is progress. Working together is success."

-Henry Ford



RF STRATEGY FOR IMPROVEMENT

- COLLABORATIVE ANALYSIS OF EVENTS (EA)
- NERC LESSONS LEARNED
- RF ASSIST VISITS
- RF WORKSHOPS
- NERC SITUATIONAL AWARENESS & MONITORING WORKSHOPS





REPORTING AN EVENT TO RF

- Disturbance mailbox
 - disturbance@rfirst.org
- Unable to email -
 - Business hours - 216.503.0600
 - After hours - 216.503.0646

RF EVENTS ANALYSIS CONTACTS

- Dwayne Fewless - Principal Analyst
 - dwayne.fewless@rfirst.org
 - 216.503.0671
- Darren Schue - Senior Analyst
 - darren.schue@rfirst.org
 - 216.503.0622
- Danielle Daugherty - Analyst
 - danielle.daugherty@rfirst.org
 - 216.503.0602



QUESTIONS & ANSWERS

Dwayne Fewless,

Dwayne.Fewless@rfirst.org

EVENT ANALYSIS LINKS

- NERC EA Program
 - <https://www.nerc.com/pa/rrm/ea/Pages/EA-Program.aspx>
- NERC Lessons Learned:
 - [Lessons Learned \(nerc.com\)](#)
- RF EA guidance Page:
 - <https://www.rfirst.org/events-data-requests/event-reporting/>

RF RISK ASSESSMENT GUIDELINE

Shawn Barrett, Principal Analyst,
Risk Analysis and Mitigation, RF

Sept. 9, 2024

INTRODUCTION

- RISK ASSESSMENT OVERVIEW
- QUALIFIED SUBJECT MATTER EXPERTS
- RISK ASSESSMENT PROCESS
- ASSESSING POTENTIAL HARM
- ASSESSING LIKELIHOOD OF OCCURRENCE
- CONSIDERING MITIGATION
- SUMMARY



RISK ASSESSMENT OVERVIEW

- The North American Electric Reliability Corporation (NERC) requires entities to include a risk assessment with all self-reported potential non-compliances
- Risk assessments are the product of a documented process that consistently analyzes four key considerations:



Threats

&



Vulnerabilities



Potential Harm



Likelihood of harm

QUALIFIED SUBJECT MATTER EXPERTS

- Risk assessments are inherently difficult and imprecise
- It is strongly recommended that trained and experienced SMEs perform the assessments
- Two key areas of training required of SMEs:
 1. Technical training in the equipment and technologies, especially in understanding their vulnerabilities
 2. Training in making estimates



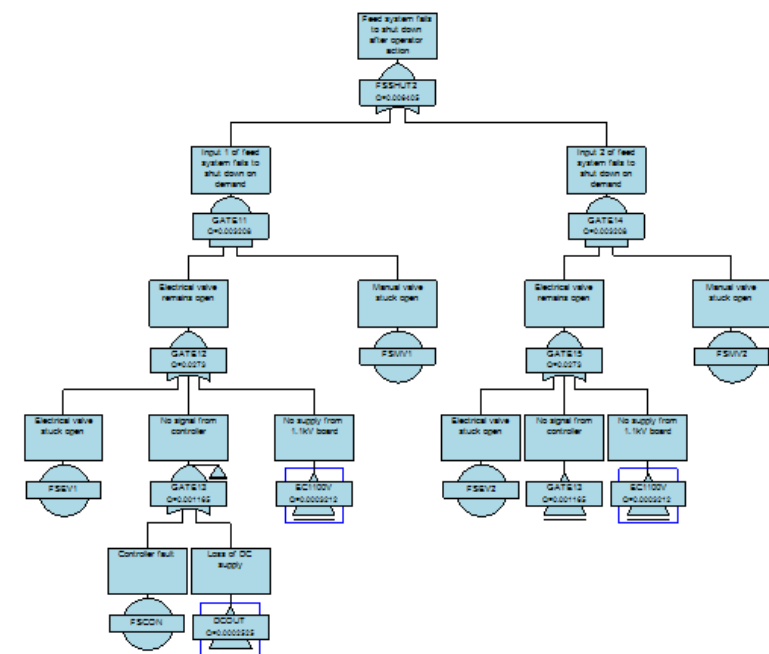
RISK ASSESSMENT PROCESS

- A documented process to assess risk consistently and reasonably accurately
- Needs adequate guidelines on completing an assessment
- Should identify which methodology will be used and when

Qualitative

Potential Harm based on MW lost	> 5k MW	Serious	Moderate	High	High	Extreme	Extreme
	2.5k to 5k MW	High	Moderate	Moderate	High	High	Extreme
	1k to 2.5k MW	Moderate	Minimal	Moderate	Moderate	High	High
	300 to 1,000 MW	Minimal	Minimal	Minimal	Moderate	Moderate	High
	< 300 MW	Negligible	Negligible	Negligible	Minimal	Moderate	Moderate
			Remote	Unlikely	Possible	Likely	Certain
			> 1 in 10,000	1 in 1000	1 in 100	1 in 20	1 in 5
Likelihood of occurrence based on odds							

Quantitative



ASSESSING POTENTIAL HARM

Assessing the adverse impacts as they relate to potential non-compliance normally begins with the assets directly involved.



- However, the assessments must consider interconnected or interrelated systems.



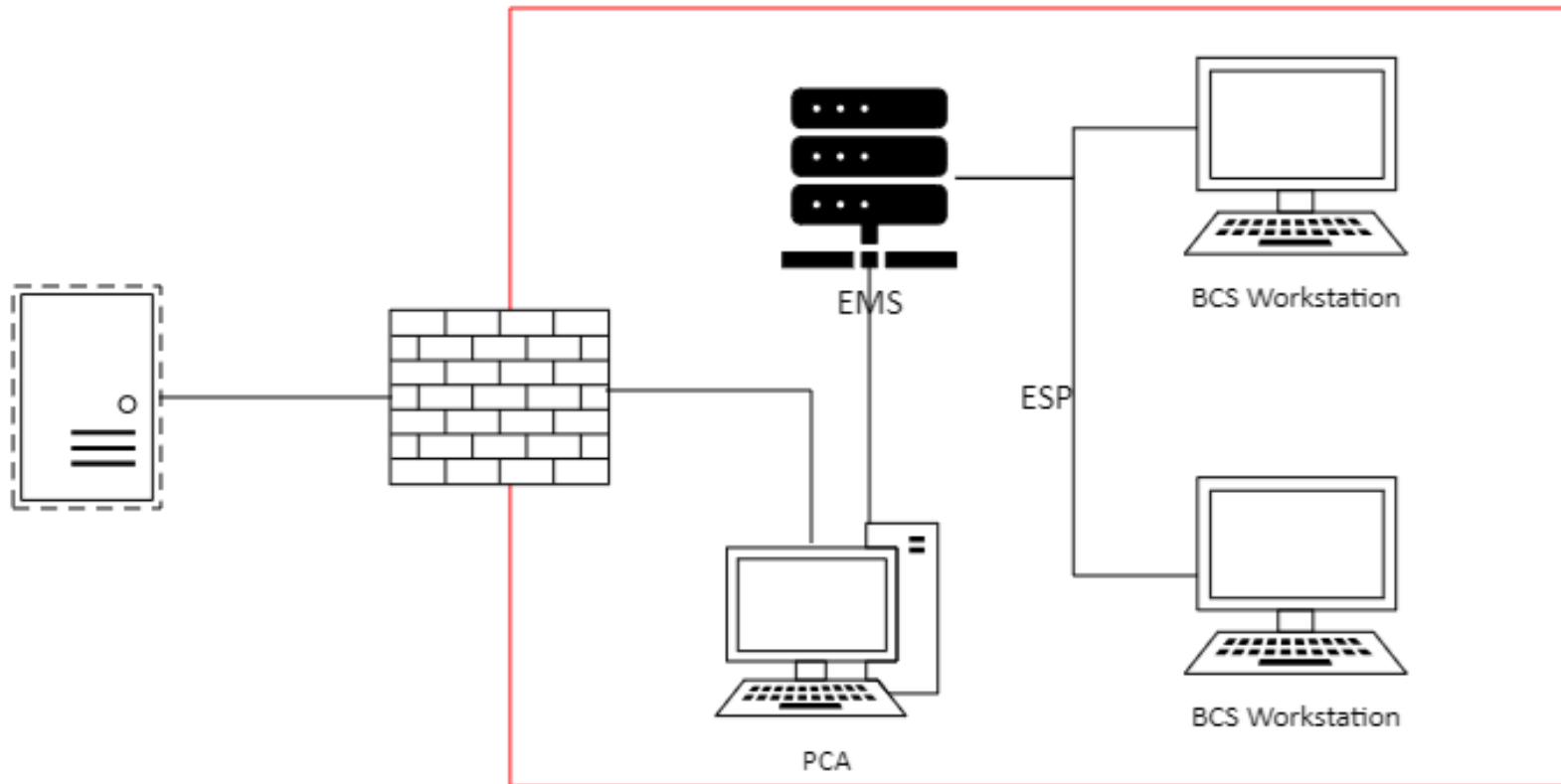
- Likewise, they may also need to include potential adverse impacts on neighboring systems.

NERC has set a minimum list of factors to consider.

- Referenced in the Risk Assessment Guidelines document on the RF site
- Found in Chapter 2, Registered Entity Self-Report and Mitigation Plan (Jan 2021)

FIRST POTENTIAL HARM PITFALL

- Many entities fail to appropriately scope the potential harm



SECOND COMMON PITFALL

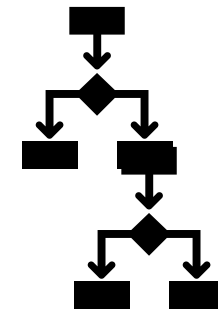
- Entities often consider facts such as:
 - Software security tools
 - Internal controls
 - Infrequency of an adverse event



- These reduce the likelihood of occurrence, not the potential harm
- A system will still catastrophically fail if those mitigating factors are all circumvented

ASSESSING LIKELIHOOD OF OCCURRENCE

- Practical application of estimation
- Two common techniques include:
 - Percentages and odds
- SMEs must consider
 - Vulnerabilities
 - Threats that can leverage the vulnerabilities
 - The likelihood that a threat may compromise the vulnerability
- Biases can play a huge role

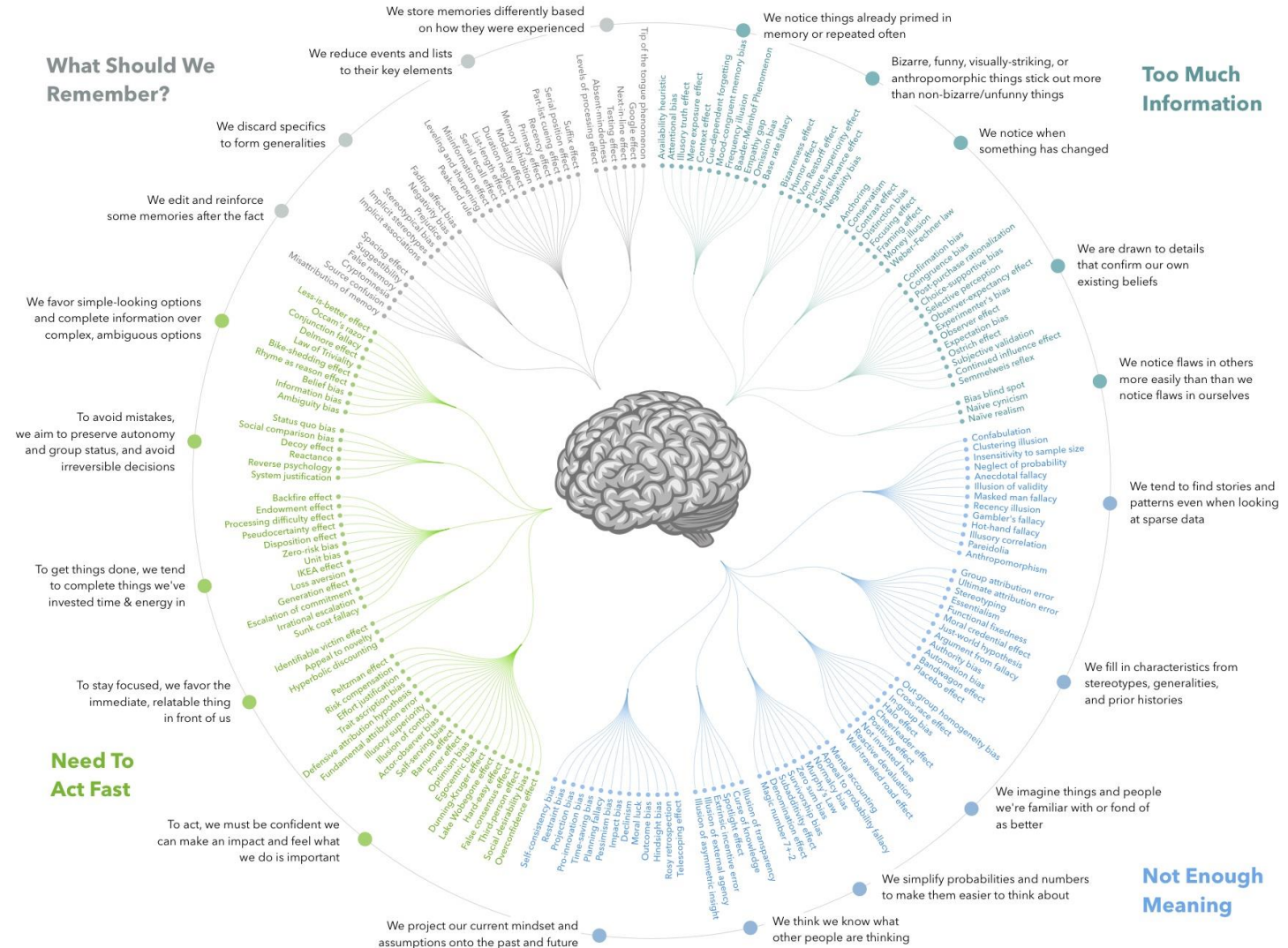


MANAGING BIAS

Common biases

- Overconfidence
- Confirmation
- Anchoring
- Observer expectancy
- Suggestibility

COGNITIVE BIAS CODEX



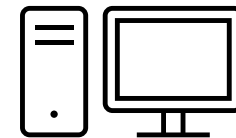
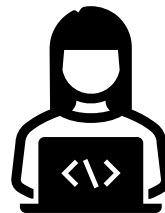
REDUCING & AGGRAVATING FACTORS

- Here is where the second common pitfall of harm assessment can apply
 - What software tools (log analytic tools) installed
 - What Internal controls (baseline monitoring) are in place
 - Are there active attacks in the wild
- Aggravating factors to consider
 - Overlapping issues with other security controls
 - Interdependent systems



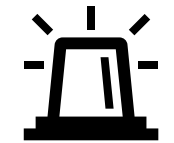
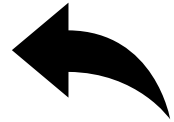
CONSIDERING MITIGATION

- Mitigation steps can be implemented during the assessment or afterward
- Mitigation steps are actions that fix or remediate the issue
- They also include actions to reduce occurrence of an issue by preventing, detecting, or correcting future issues (Internal Controls)



FIVE ALIGN MITIGATION ACTIONS:

- **Remediating Action:** An action taken to return to compliance
- **Preventive Control Action:** Creation of an internal control designed to avoid an unintended event or consequence.
- **Detective Control Action:** Creation of an internal control designed to identify errors or deviations from the norm.
- **Corrective Control Action:** Creation of an internal control designed to fix a problem that may arise.
- Other...



INTERNAL CONTROLS

- Can be technical, procedural, or a combination of the two
- Technical controls are automated systems that work without human initiation
- Procedural controls are policies, procedures and checklists
- Some technical controls rely on a procedural controls



PRACTICAL EXAMPLE

Consider a scenario where an employee's CIP training date is entered into an electronic record, specifically a data entry field.

In this scenario the entity could establish at least two procedural and two technical internal controls

Employee Training Deadlines Alert

 Alert@entity.com
To physical.security@entity.com
Retention Policy 18 Month Delete (1 year, 6 months)

 Reply  Reply All  Forward  

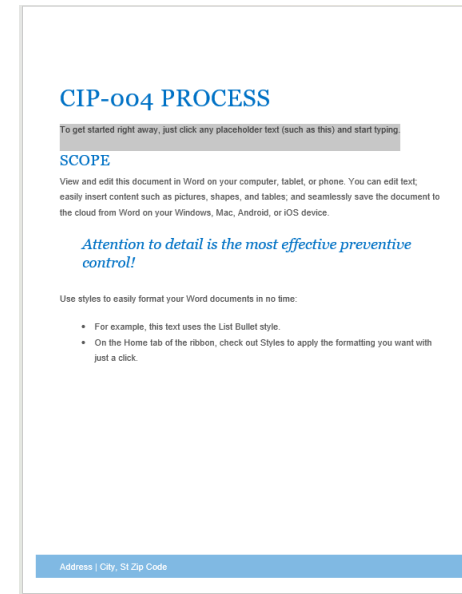
Fri 8/9/2024 12:07 PM

Expires 2/7/2026

This is an automated alert. The following employee last training date completion was over 12 months ago:

John Doe: Operations, john.doe@entity.com, op.mgr@entity.com
Jane Wonde: IT Security, jane.wonde@entity.com, itsec.mgr@entity.com
Sean Bea: [DASales](mailto:dasales@entity.com), sean.bea@entity.com, dasales.mgr@entity.com

Please review the CIP-004 Process document for next steps to initiate the next training cycle.



CIP-004 DATA ENTRY CHECKLIST

- Do this first
- Do this second
- Check the data
- Open the application
- Enter the data
- Confirm the data is entered correctly
- Save the information



SOURCES

- [RF Risk Assessment Guideline](#)
- [NERC Rules of Procedure, Appendix 4C, effective 5/19/22](#)
- [NERC Self-Logging Program User Guide, Chapter 2, dated 11/27/2018](#)
- [NERC Registered Entity Self-Report and Mitigation Plan, Chapter 2, dated January 2021](#)
- [NIST Special Publication 800-30, Revision 1, Guide for Conducting Risk Assessments, Appendix G](#)
- [Cognitive Bias Codex](#)

QUESTIONS & ANSWERS

Shawn Barrett

shawn.barrett@rfirst.org



THANK YOU

***Join us for our next Tech Talk -
October 28th***

[Webinar Link](#)

***Fall Reliability Summit -
September 16th - 18th***

