

WELCOME TO TECHNICAL TALK WITH RF

November 18, 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, it states "RF works to maintain the reliability, security and resilience of the electric grid in the Mid-Atlantic region" and "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" (3,970 followers, 2d) with the text: "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: a group photo of staff in front of a building and a photo of staff working on a roof.

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.

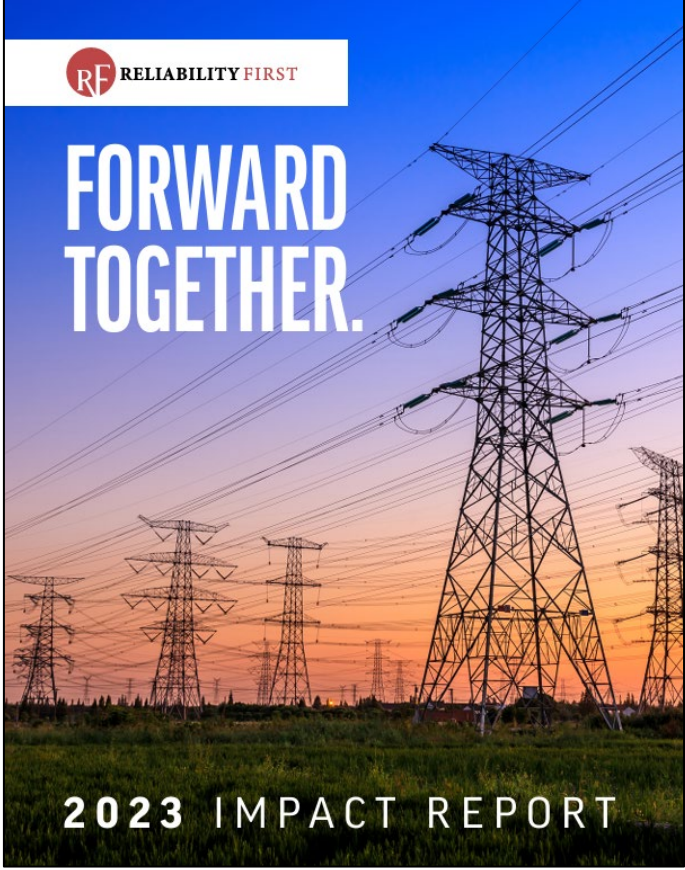
[Click here to read more](#)

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

November 18, 2024



TECH TALK ANNOUNCEMENT



Milestone 3 Projects

Highlighting and Addressing Scope of Issues Related to Current State of Model Quality | October 30, 2024

In response to FERC Order No. 901, NERC is actively developing key Reliability Standards projects to enhance IBR planning and ensure reliable grid reliability. NERC's Order No. 901 work plan includes four milestones designed to meet FERC's directives within the specified timeframes. **Milestone 3** focuses on developing and filing standards that enhance data sharing and model validation for all IBRs. This milestone has a filing deadline of November 4, 2025, with a full implementation target of January 1, 2030.

NERC's [Milestone 3 Summary](#) provides a high-level overview of its associated projects—[Project 2020-06 - Verifications of Models and Data for Generators](#), [Project 2021-01 - System Model Validation with IBRs](#), [Project 2022-02 - Uniform Framework Model Framework for IBR](#), and [Project 2022-04 - Electromagnetic Transient Modeling](#).



TECH TALK ANNOUNCEMENT



Third ITCS Document Published

November 4, 2024

NERC published Prudent Additions Recommendations (Part 2) and Meet and Maintain Recommendations (Part 3), the third in a series of three draft documents that will be merged into the final Interregional Transfer Capability Study (ITCS).

The document provides an energy margin analysis and resulting recommendations for increases to the transfer capability between Transmission Planning Regions to improve energy adequacy during extreme weather events. It also recommends how to meet and maintain transfer capability as enhanced by these technically prudent additions.

The complete ITCS will be filed with the Federal Energy Regulatory Commission (FERC) by December 2, 2024, and will be followed by a FERC public comment period.

ITCS Parts 2 and 3

The third document in the ITCS series, addresses Part 2 (Prudent Additions Recommendations), and Part 3 (Meet and Maintain Recommendations) of the ITCS mandate.

Part 2 provides an energy margin analysis and technically prudent recommendations for transfer capability increases, while Part 3 discusses how to meet and maintain transfer capability as enhanced by these technically prudent additions.

CONTEXT

ANALYSIS

RECOMMENDATIONS

The graphic features three document covers on the right side, each with the NERC logo and the title 'Interregional Transfer Capability Study (ITCS) Strengthening Reliability Through the Energy Transformation'. The top cover is titled 'Overview of Study Need and Approach June 2024'. The middle cover is titled 'Transfer Capability Analysis (Part 1) August 2024'. The bottom cover is titled 'Recommendations for Prudent Additions to Transfer Capability (Part 2) and Recommendations to Meet and Maintain Transfer Capability (Part 3) November 2024'. The background of the graphic shows a power transmission tower against a sunset sky.

TECH TALK ANNOUNCEMENT



NERC-NATF-EPRI Annual Transmission Planning and Modeling Workshop

November 19-20, 2024 | [Register](#)

Register now for the 2024 virtual annual transmission planning and modeling seminar featuring industry experts sharing valuable insights, best practices, and innovative strategies to address the evolving challenges in the field of electric power transmission.

The event will be held virtually, 1:00 pm to 5:00 pm eastern each day.



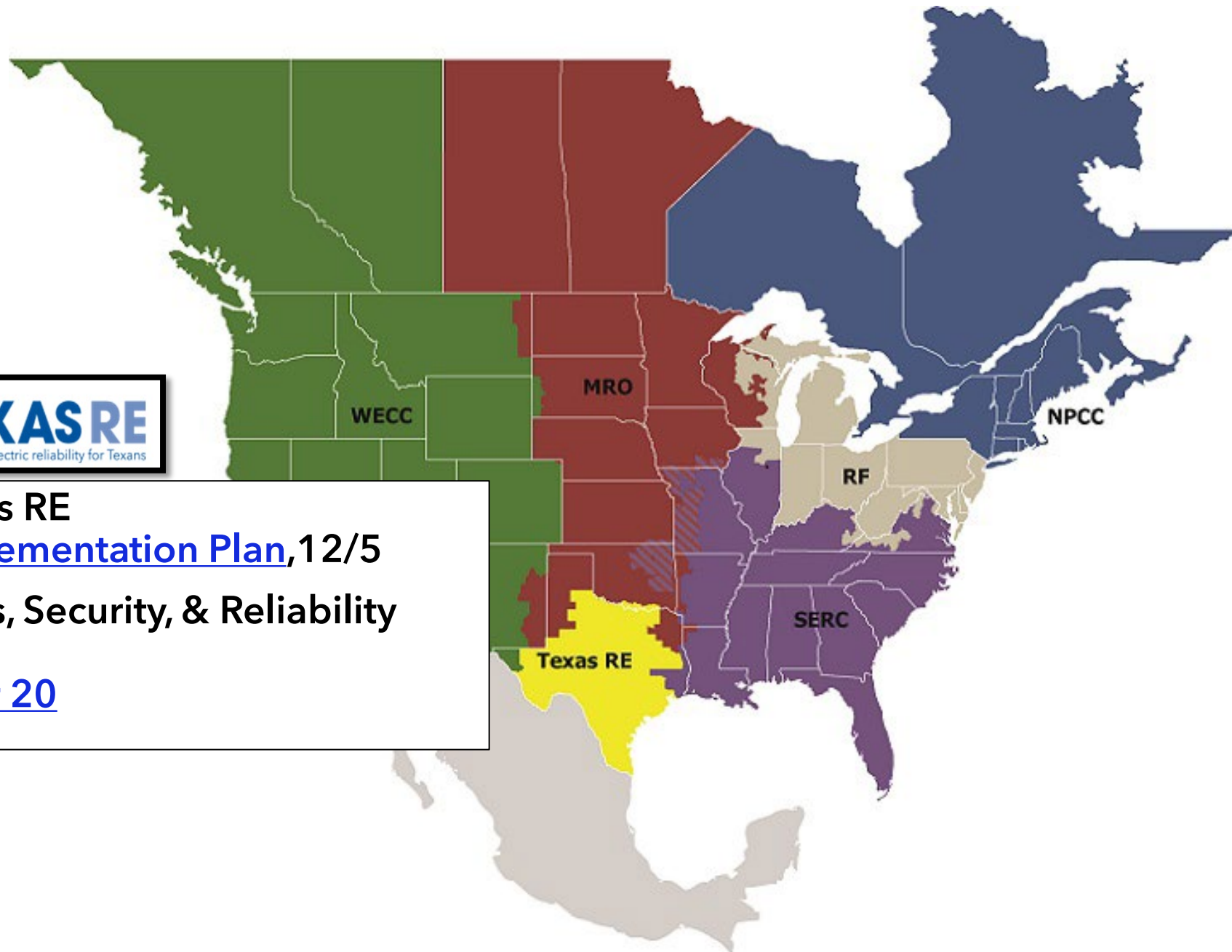


Talk with Texas RE

- [2025 Implementation Plan, 12/5](#)

Fall Standards, Security, & Reliability Workshop

- [November 20](#)



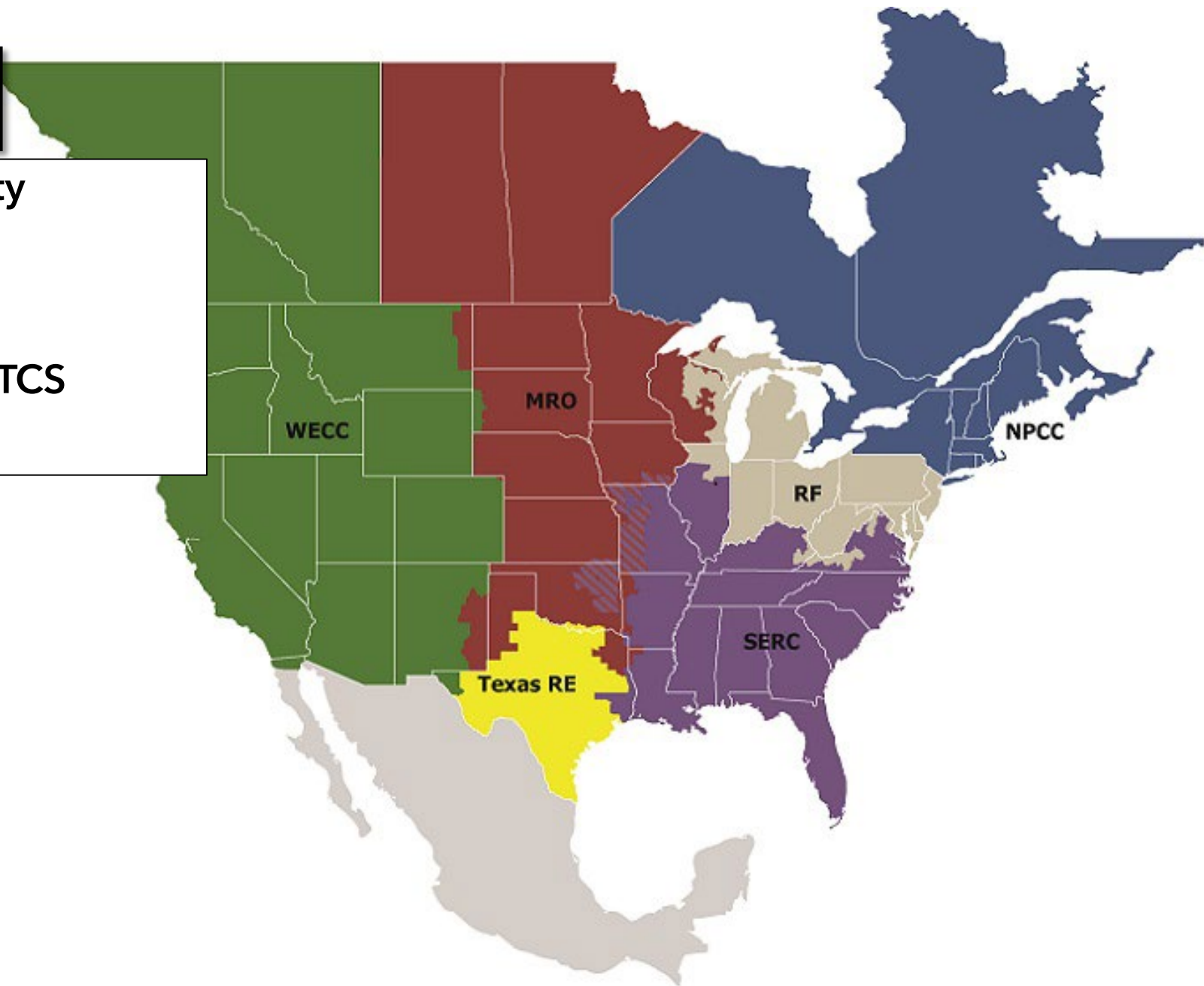


Reliability & Security Oversight Update

- [November 21](#)
- [December 19](#)

Technical Session: ITCS

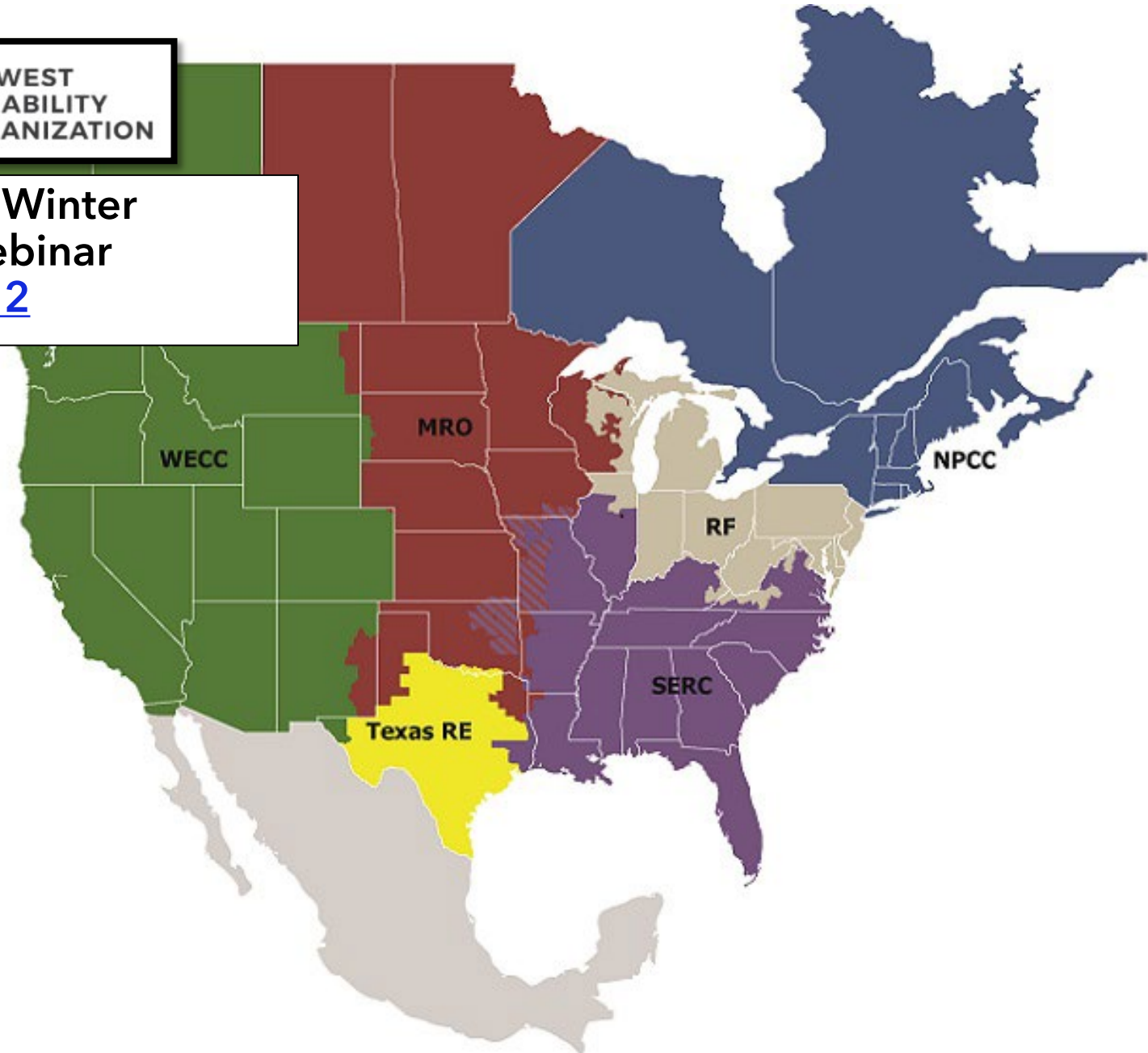
- [December 10](#)

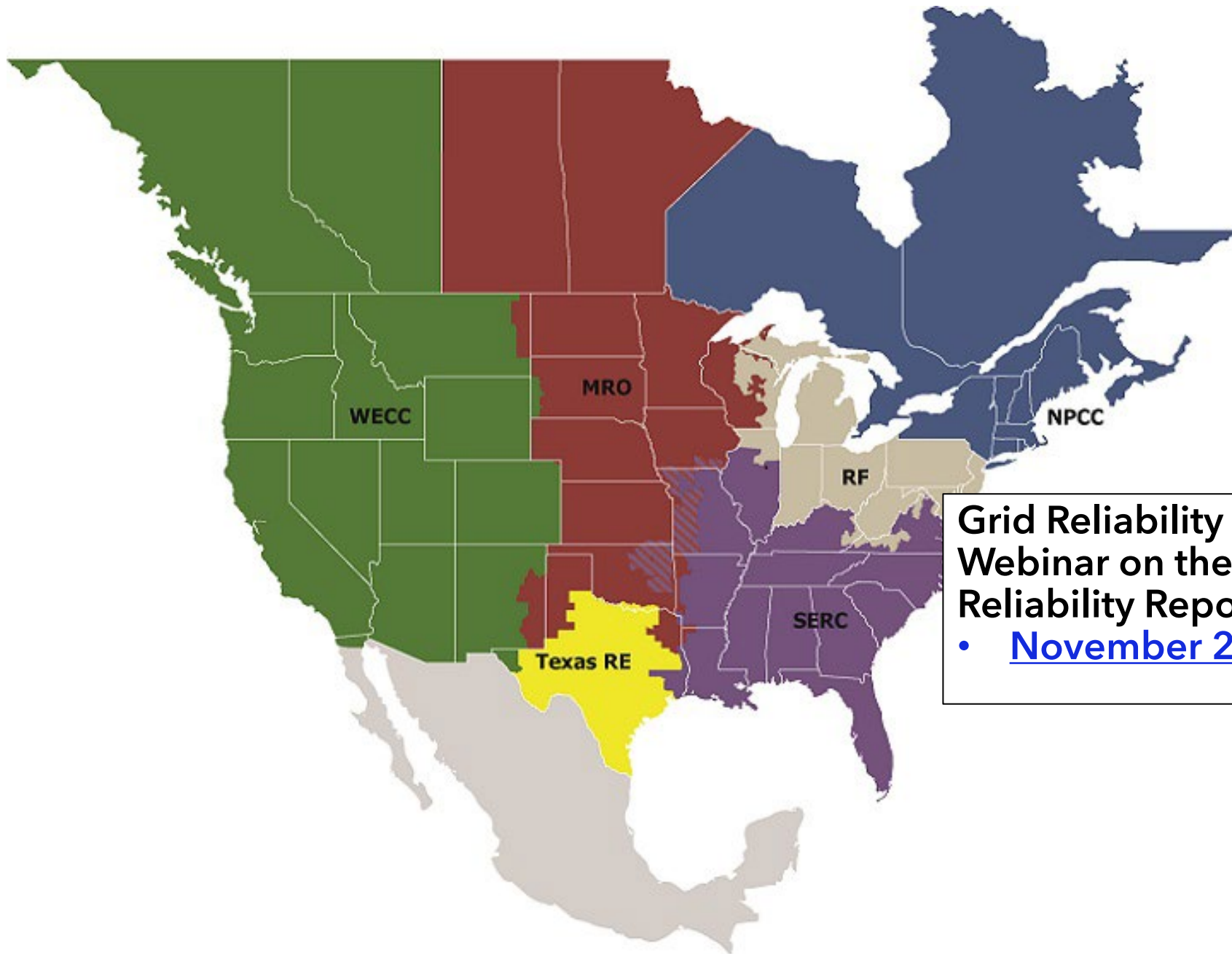




2024 Regional Winter Assessment Webinar

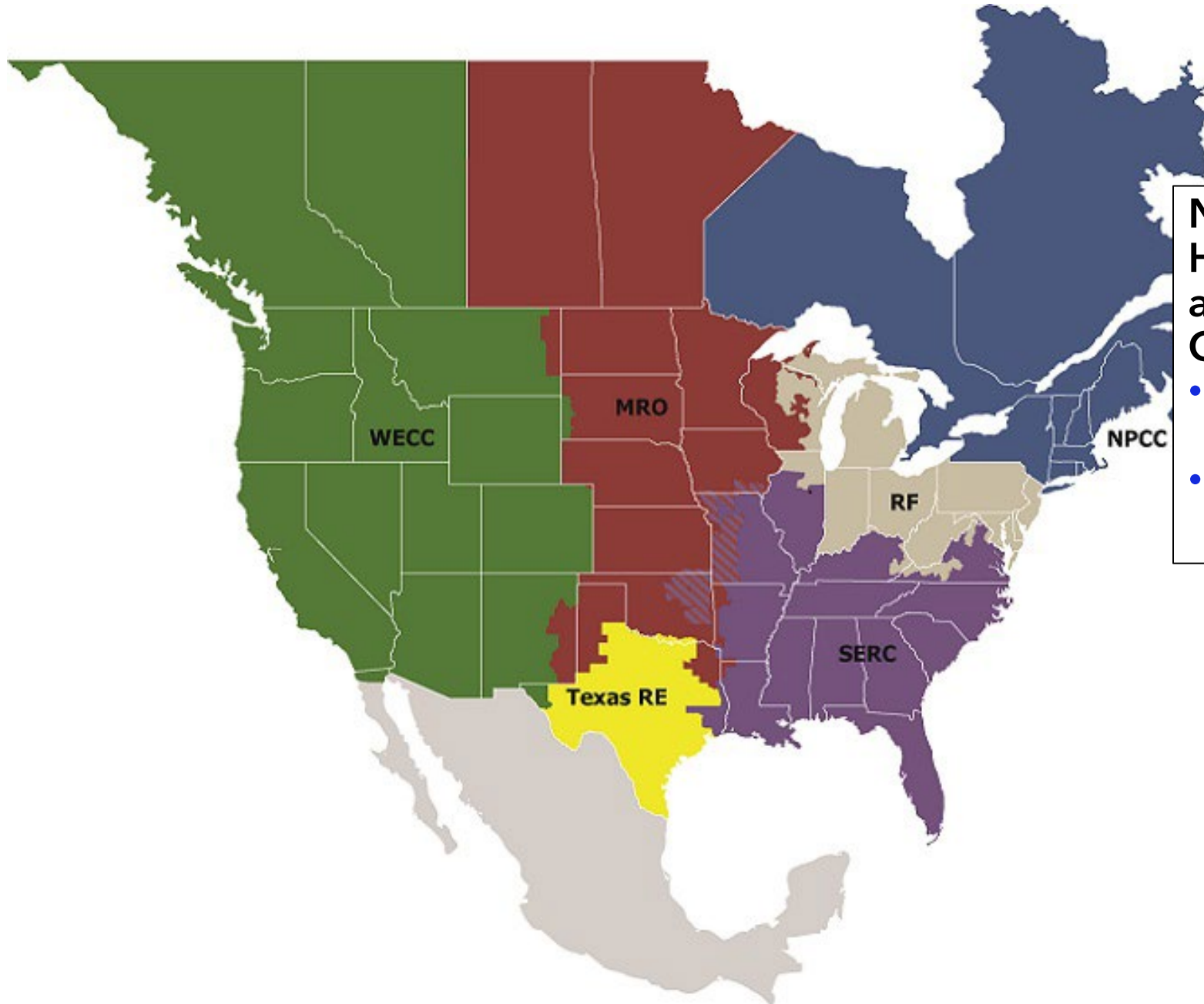
- [December 12](#)





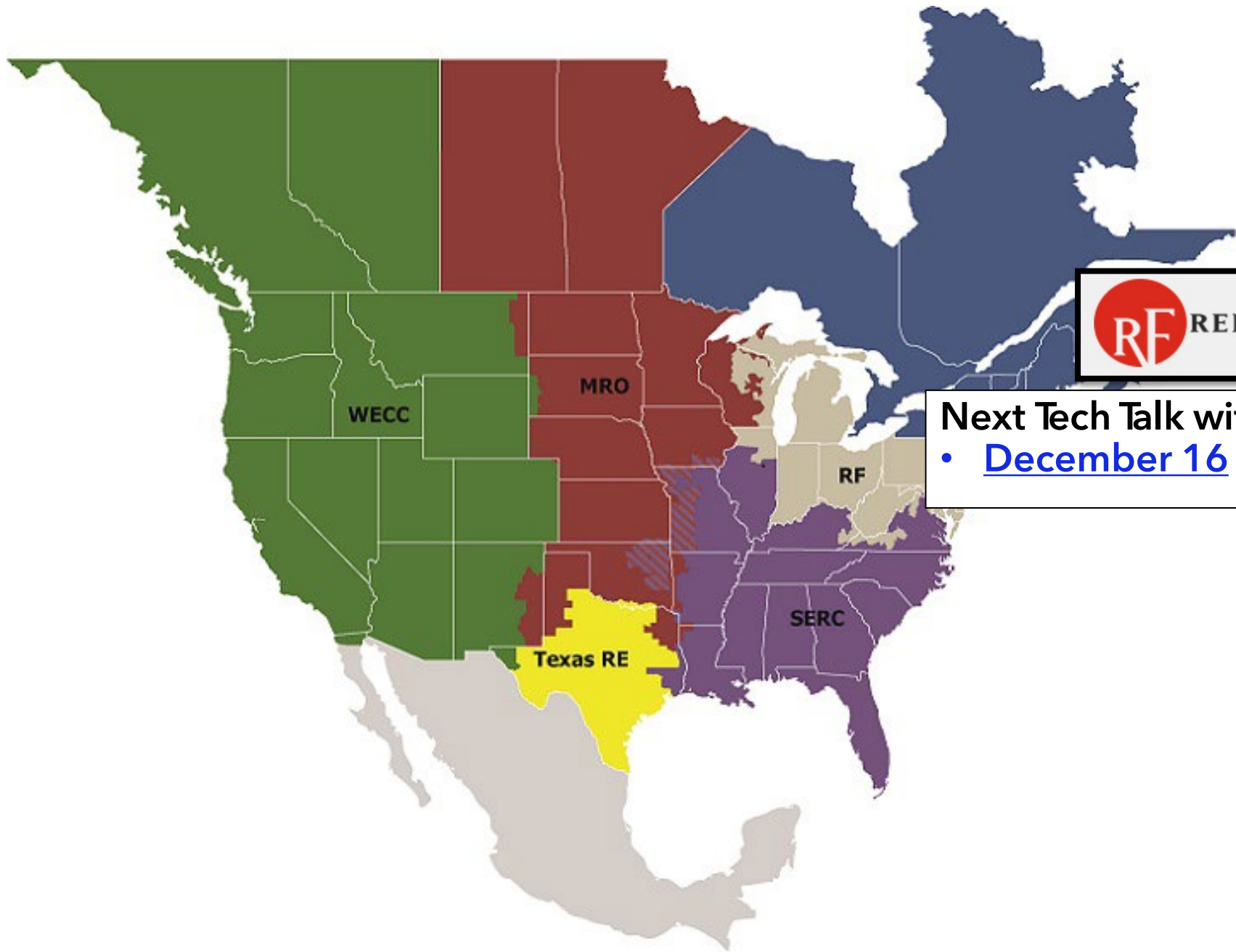
**Grid Reliability for States
Webinar on the 2024 State of
Reliability Report**

- [November 21](#)



**NPCC Fall 2024
Hybrid Compliance
and Reliability
Conference**

- [November 6 Slides](#)
- [November 7 slides](#)



Next Tech Talk with RF
• [December 16](#)

TECH TALK REMINDER

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

CLICK HERE

MON
18

November 18 @ 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

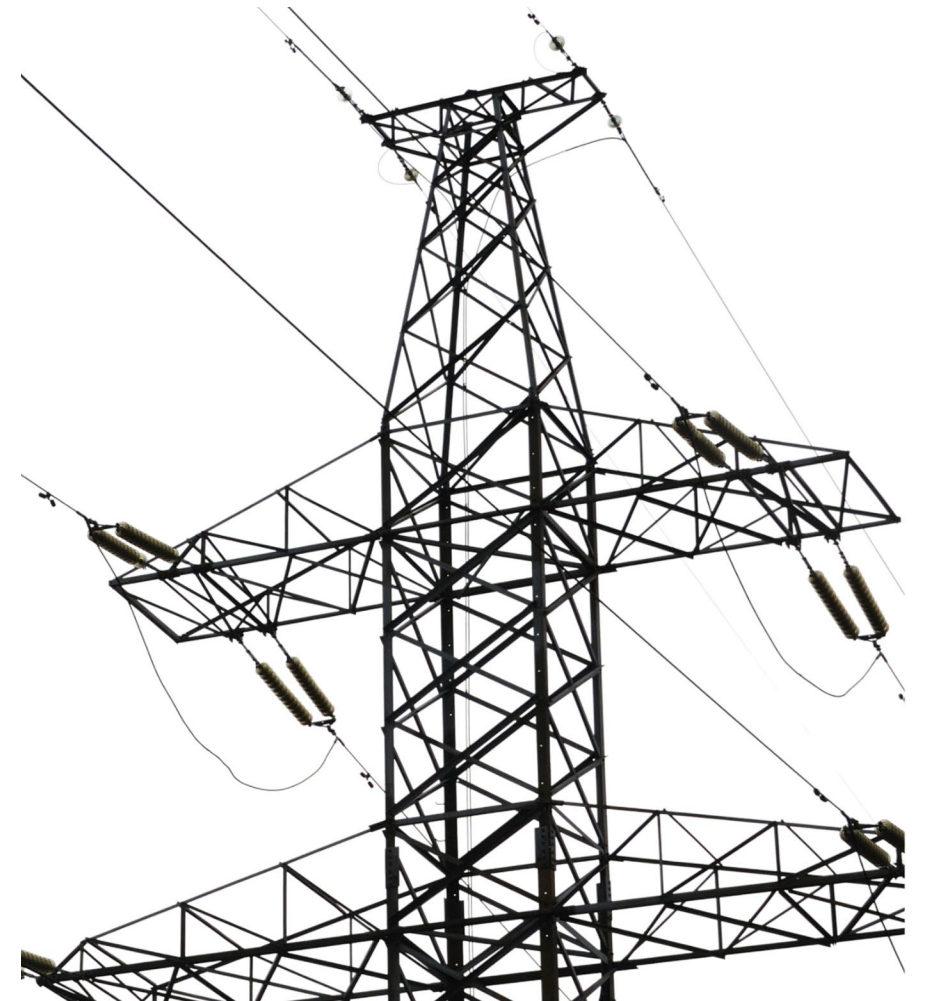
[SLIDO.com](https://www.slido.com)

#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

EXELON'S PHYSICAL SECURITY BEST PRACTICES AND LESSONS LEARNED

- **MIKE MELVIN**, DIRECTOR CORPORATE PHYSICAL SECURITY, EXELON

CERTIFICATION PROCESS AND TIMELINE CONSIDERATIONS

- **SAM CICCONE**, PRINCIPAL RELIABILITY CONSULTANT, RELIABILITYFIRST



November 18, 2024

ReliabilityFirst Tech Talk - Physical Security Best Practices and Lessons Learned

Mike Melvin, Director, Exelon Corporate Physical Security

Agenda

1. Overview of the Exelon Corporation
2. Executive Summary
3. Changing Threat Landscape
4. Significant Programs to Mitigate Threat Landscape
5. Next Steps

Exelon's Family of Companies

Transmission and Delivery



- Exelon Corporation (Exelon) is a Fortune 250 company focused on transmission and distribution of electricity and gas. As the nation's largest utility company, Exelon had revenues of \$21.03 billion in the 12 months ending September 30, 2023, with 11.65% growth year over year.
- Serving more than 10 million customers across Delaware, Illinois, Maryland, New Jersey, Pennsylvania and the District of Columbia through its six fully regulated transmission and distribution utilities—ACE, BGE, ComEd, DPL, PECO, and Pepco— Exelon is recognized as an industry leader with best-in-class operations.
- Exelon's more than 19,500 employees have driven ACE, BGE, ComEd, DPL, PECO, and Pepco to achieve top quartile or better performance in customer satisfaction, reduce outage frequency, and provide faster service restoration for the benefit of their customers. This strong record of reliability and customer satisfaction is reinforced by substantial infrastructure investments across the fleet.

Who is Exelon?

6 T&D-only utilities

Operate within seven regulatory jurisdictions

4 major metro areas served

Chicago, Philadelphia, Baltimore, and Washington D.C.

19,100

Employees across our operating companies

10.6 million⁽¹⁾

Electric and gas customers served across our service territories

25,600

Square miles of combined service territory across our jurisdictions

183,540

Circuit miles of electric and gas distribution lines

11,140

Circuit miles of FERC-regulated electric transmission lines

\$19.1 billion

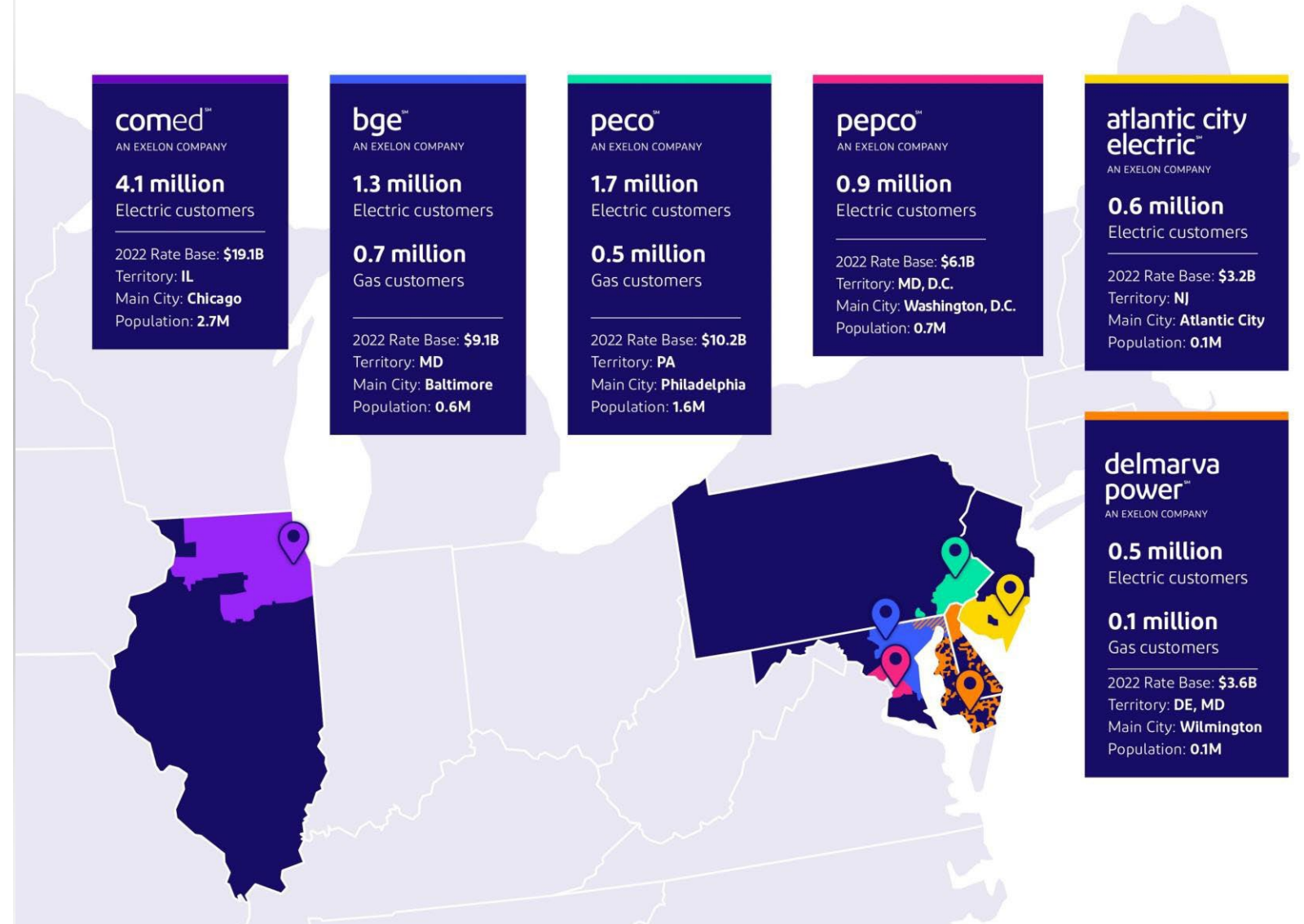
Operating revenues recorded at our utilities in 2022

\$56.2 billion

Rate base estimate for 2023

\$31.3 billion

Projected capital investment over 2023 through 2026



(1) Customer count reflects the sum of Exelon's total gas and electric customer base; Exelon consolidated customer count may not sum due to rounding
Privileged and Confidential

Executive Summary

Threat Landscape has Changed

- The U.S. threat environment has or is changing in ways that require new levels of attention. Critical infrastructure is both in the geopolitical battle space and the target of extensive criminal activities.
- Exelon operates in territories that have experienced violent crime rates of concern, employees are rarely targeted because of their profession or employer; however, they can be targets of opportunity or unintended victims in violent incidents.

Best Practices

- Exelon's utilizes a risk-based approach to physically protect assets through our Facility Enhancement Program (FEP) and Office & Support Facilities (O&SF) program.
- Exelon's Personnel Security Protection Programs are designed to provide security support to field personnel and have been considered best practice by industry counterparts. Exelon has shared program strategies, such as developing Security Awareness Areas based on crime reporting data, with industry and non-industry partners who deploy personnel in the field.

Focus of Protection Programs

- Execution of the multi-year FEP and O&SF programs in a risk-based fashion (i.e., higher tiered sites completed first).
- Education to field personnel to increase utilization of security support available to proactively ensure their safety/security.

Changing Threat Landscape

Problem Statement: The threat landscape for the Physical Security of our most important asset, our personnel, and our critical infrastructure assets, has advanced.

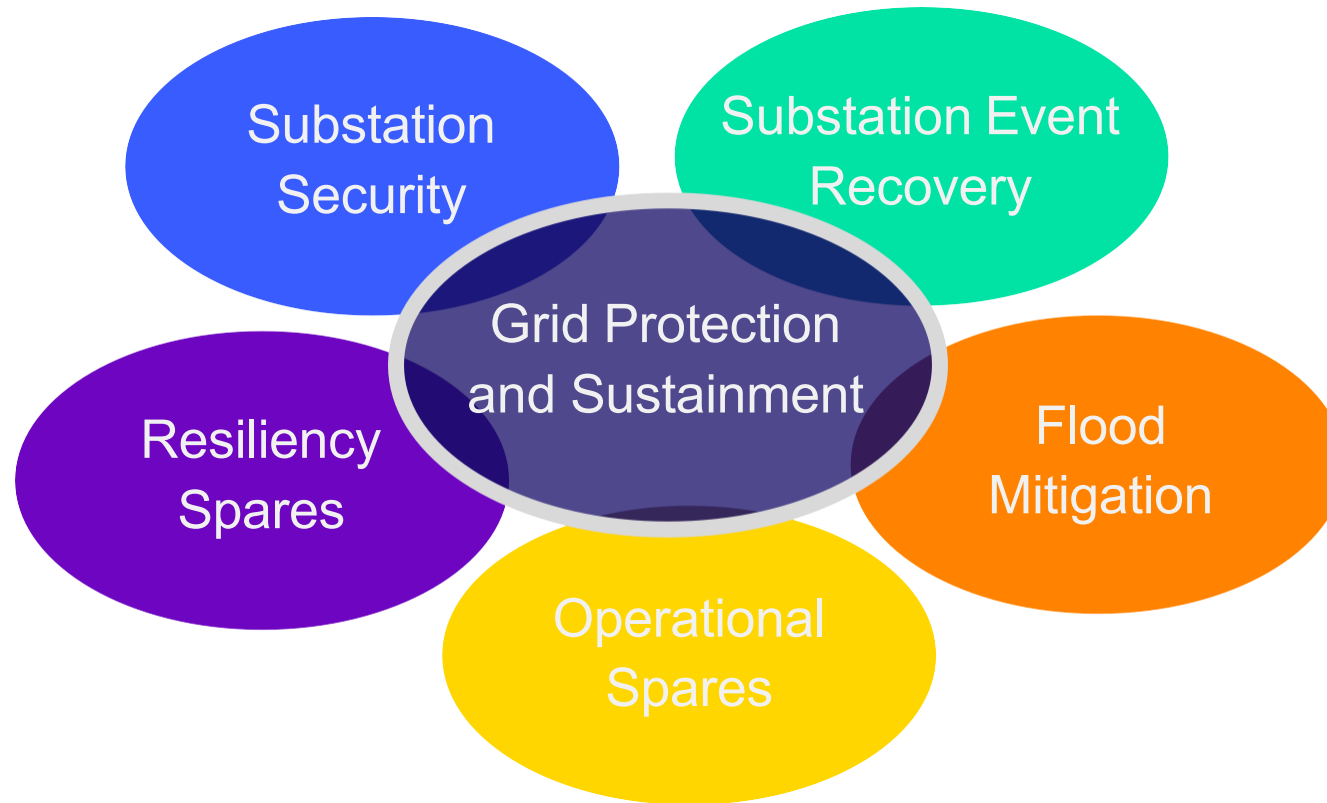
- July 2022: A post on the Telegram Channel "National Anarchist Ecoposting" promoted a coordinated attack to cause a "national blackout"
 - Listed several substations as critical components including two operated by ComEd.
 - Post has resurfaced a handful of times since.
 - Corporate Physical Security Intelligence believes this will likely continue.
- February 6, 2023: Two charged with conspiracy to destroy an energy facility.
 - Suspects accused of planning attacks on BGE Substations.
 - Motive: Racially/Ethnicly extremists "planned to lay Baltimore to waste".
 - Suspect Sarah Clendaniel pled guilty on May 14, 2024; prosecutors are seeking 18-year prison sentence with potential for \$75 million in damage.
 - Suspect Brandon Russell's trial scheduled to begin on November 12, 2024.
- August 21 & 28, 2024: 4chan postings called for the destruction of PEPCO power plants in Charles County, MD, within the context of a hypothetical civil war.
 - Corporate Physical Security met with PHI and other OpCo Security teams to collaborate on response, public sector partners were notified.
 - The situation is continuing to be closely monitored.
- Exelon, as well as the greater utility sector has seen an uptick in threats and assaults on field crew members.
 - Employees frequently work in areas that experience increased levels of violent crime. Though rarely targeted because of their role in Exelon, they have been unintended victims of those behaviors.
 - Corporate Physical Security Intelligence assesses it is likely that threats will increase.



Significant Programs to Mitigate Threat Landscape

- **Facility Enhancement Program (FEP):** The multi-year program for installing standard physical security protection measures at Exelon's electric transmission and distribution substations (including facilities or buildings within a substation and standalone microwave buildings or relay point locations in a substation), gas plants, gas gate stations, gas regulator stations and gas system critical valves, based on the tier level of the asset.
 - In response to the changing threat landscape, in 2023 Exelon completed a reevaluation of our physical security standards. Additional security measures to improve our security posture were identified and are being implemented into FEP.
- **Office & Support Facilities (O&SF):** The multi-year program for installing standard physical security protection measures at Exelon's Office & Support Facilities (including conference centers, data centers, fleet buildings, headquarters, legislative offices, office buildings, payment centers, reporting centers, service buildings, training centers and warehouses) based on the tier level of the asset.
- **Personnel Security Protection Programs (PSPP):** Coordinated by Business Unit (BU) Security Departments at each Exelon Operating Company (OpCo) for the development, coordination and implementation of a Protection Program to provide field personnel with readily available security support, which includes armed guards, when performing work in areas identified as Security Awareness Areas. These Security Awareness Areas are based off an analysis of Uniformed Crime Reporting Part I Violent Crimes.
- **Business Continuity:** Serves to integrate the disciplines of Emergency Preparedness/Response, Crisis Management, Disaster Recovery and individual Business Continuity function/location plans.

Exelon - Grid Protection and Sustainment Initiatives



Adequate mitigation of potential threats includes more than physical barriers

- There is no “one size fits all” approach
- Requires a resiliency strategy that supports system recovery

Exelon - Grid Protection and Sustainment Initiatives

Goals

- Withstand a shock from any hazard with no loss of critical functions
- Prevent a power disruption from cascading into interconnected systems
- Minimize the duration and magnitude of power outages through rapid recovery strategies
- Mitigate future risks by incorporating lessons from past disruptions, simulations and exercises, and sound risk assessment processes



Initiatives

- Align multiple “Resiliency” efforts across all Exelon Utilities
- Coordinated approach based on engineering studies of the transmission systems
- Establish common goals and objectives but account for local system differences
- Develop plans and processes to mitigate and recover from events
- Do not create additional critical substations
- Reduce the number of existing critical substations
- Prevention/Protection is also part of this integrated effort that goes beyond CIP-014 critical substations to include other electric and gas facilities across all the Exelon Utilities

Tiering Assets Based on Operational Criticality

Exelon developed a tiering process for all electric and gas assets in 2014

- Tiering is conducted every three years by operations/planning/engineering representatives from Transmission and Distribution (for Electric) and Gas. OpCo COOs approve final tiering results.
- Each asset is assigned a Tier (0 - 4) and is based on the operational criticality of the facility.
- Many factors such as customer count, critical customers served, direct/indirect connect to nuclear, feeder number and type, etc.

Exelon developed security standards for all assets based on their tier level

- Threat Basis: Implement physical security measures that reduce vulnerability associated with unauthorized access to personnel, equipment, systems, and material at critical sites utilizing a defense in depth strategy.
- Standards are for all tiered electric & gas assets across Exelon.
 - Exelon standards ensure all sites are designed & built with the same protection and monitoring criteria.
- Specific standards and tier levels are protected and proprietary information and not distributed to others without a need to know.
- Designed to accomplish the following objective: **Deter/Detect/Delay/Assess/Communicate/Respond**.
 - This approach follows the NERC CIP-014 Standard approach.
- The initial strategy was reviewed with Nuclear Security and third-party consultants.
 - Program continues to be benchmarked with industry peers.

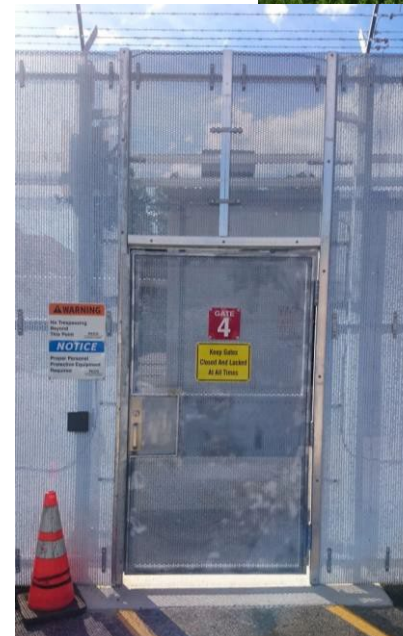
Facility Enhancement Program (FEP)

Exelon Facilities After FEP Enhancements

- FEP Security Standards can include the following measures based on the tier assigned to the facility:
 - Perimeter fencing materials and perimeter/fencing detection
 - Gate installation
 - Roof protection
 - Lock and chain installations
 - Signage postings
 - Camera installation at the perimeter, gate, building and critical infrastructure
 - Alarm points
 - Access Controls (both mechanical and manual)
 - Video recording and storage
 - Reactive lighting
 - Underground pathways
 - Law enforcement engagement



Exelon Substation



Exelon Pedestrian Gate



Exelon Vehicle Gate

Next Steps

- Pursue continuous improvement opportunities to our security posture with an appropriate methodical and flexible approach to address the evolving threat landscape.
- Conduct challenge sessions on security plans developed ahead of election and other major events for lessons learned, collaboration, and opportunities for improvement.
- Continue R&D to identify new technologies to effectively and efficiently protect critical assets.
- Strengthen relationships with federal, state, and local law enforcement to promote bi-directional information sharing.
- Enhance monitoring of online activity for new and emerging threats to Exelon's infrastructure and personnel.
- Proceed with strengthening Business Continuity program and concepts into all aspects of the business.





Appendix

Substation after security enhancements



Substation after security enhancements



Vehicle gate before/after security enhancements

BEFORE



AFTER

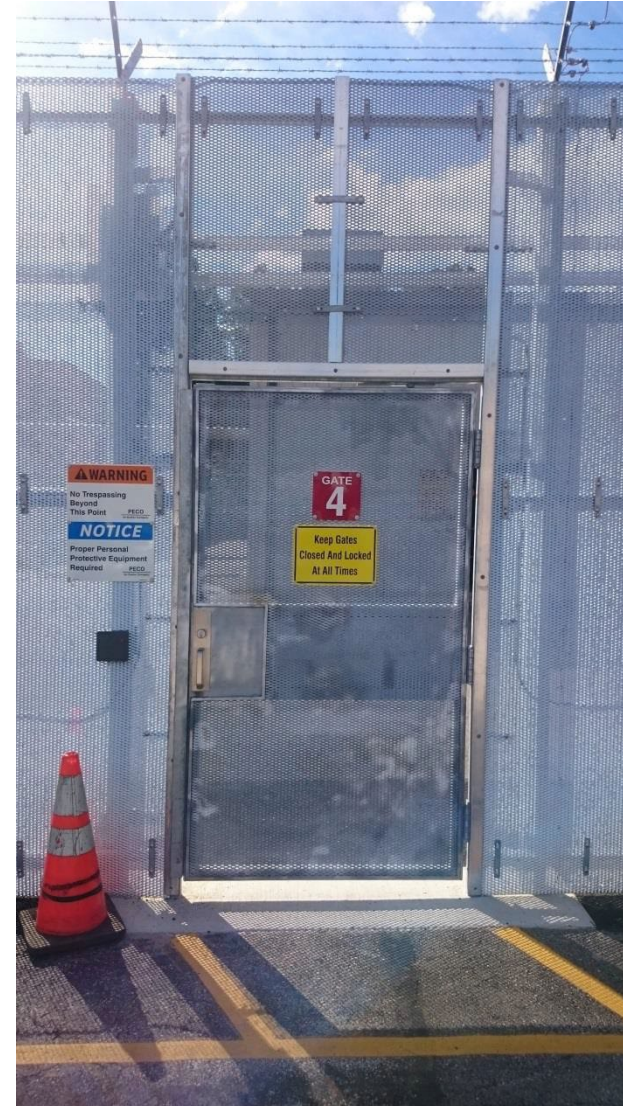


Pedestrian gate before/after security enhancements

BEFORE



AFTER



CERTIFICATION PROGRAM

Sam Ciccone

**Principal Reliability Consultant,
Entity Engagement, RF**

Technical Talk with RF

Nov. 18, 2024



AGENDA

CERTIFICATION INTRODUCTION AND TYPES

CERTIFICATION REVIEWS TRIGGERS

CERTIFICATION PROCESS

CERTIFICATION PROCESS TEMPLATES

PROCESS TYPICAL TIMELINE

FERC ORDER 881

RESOURCES

QUESTIONS



CERTIFICATIONS



NERC RULES OF PROCEDURE (ROP)



Section 500 and Appendix 5A governs Certifications

- ROP Appendix 5A Section IV addresses Certifications for new TOPs, BAs and RCs
- ROP Appendix 5A Section V addresses Certification Review Activities
 - Mandated when certified entities (i.e., TOP, BA, RC) make certain operational changes.

**** Note:** TOs in the PJM footprint are also required to notify RF when making certain operational changes.

(ROP says: "For an entity that is not required to be certified but performs tasks associated with a RC, TOP, or BA shall consult with the Registered Entity regarding the applicability of a "capability verification" or "readiness evaluation" regarding those tasks."

CERTIFICATION ACTIVITY TYPES

- **Full Certification**
 - Certification of newly registered TOP, BA, and/or RC
- **Certification Review**
 - Review of changes made by registered TOP, BA, and RC
- **Readiness Evaluation**
 - They are like Certification Reviews
 - Intended for “an entity that is not required to be certified but performs tasks associated with a RC, TOP, or BA in accordance with Section IV” (ROP Appendix 5A Sec. V)
 - Example is PJM TOs
 - Matrix of requirements pared down further for only those requirements delegated to the entity
- **Lesser Activity**
 - No ROP process steps that must be used (optional)
 - Defined by Regional Entities
 - Touchpoint meetings, RFIs, Summary Report, etc.

CERTIFICATION REVIEW TRIGGERS



FOOTPRINT CHANGE

Changes to registered entity's footprint⁸ (including de-certification changes to existing JRO/CFR assignments or sub-set list of requirements):

- i. The review of changes to an already registered and operational entity's footprint is primarily concerned with ensuring the gaining functional entity has the tools, training, and security in place to reliably operate with new responsibilities. Changes to an entity's footprint can be characterized by new metered boundaries associated with the integration or disassociation of existing electrical areas of the BPS (Reliability Coordinator Area, Transmission Operator Area, or Balancing Authority Area).

⁸ This includes changes in ownership of BPS facilities, changes in the applicability of the BES Definition to a Facility, and newly installed BPS facilities.

What should you expect from this review?



CONTROL CENTER RELOCATION

- i. Fundamental to the reliable operation of the interconnected transmission network are the control centers that continuously monitor, assess, and control the generation and transmission power flows on the BES. Of interest are impacts to the functionality provided within these facilities for continued reliable operations of the BES that affect:
- Tools and applications that system operators use for situational awareness of the BES
 - Data exchange capabilities
 - Interpersonal (and alternate) communications capabilities
 - Power source(s)
 - Physical and cyber security
- ii. The impact of the relocation of the control center on the entity's ability to perform the functions for which the entity is registered under normal and emergency conditions should be explored and documented to understand the manner in which the control center continues to support the reliable operations of the BES.



What should you expect from this review?

EMS MODIFICATION

Modification of the Energy Management System (EMS) which is expected to materially affect CIP security perimeters or the System Operator's:

- 1) situational awareness tools,
- 2) functionality, or
- 3) machine interfaces.



What should you expect from this review?

SUMMARY OF ITEMS TO REVIEW

Operator ability to monitor, assess, and control the grid

- Inspect and walk through any ESP, EAP, PSP changes
- Review security and physical plan changes
- Operator training depending on the extent the changes affect operator functions
- Data exchange capabilities and communications with their RTO and neighbor
- Tools operators use for situational awareness
- Demonstration of EMS/SCADA functionality and screens that may have changed
- Review changes to backup control center functionality and CIP assets and processes
- New metered boundaries associated with integration or disassociation of existing areas
- Review all policies/procedures impacted by the change

CERTIFICATION PROCESS



CERTIFICATION ACTIVITY PROCESS INITIATION


Application/Questionnaire

RFirst.org Certification page: Certification - ReliabilityFirst

To request a certification, certification review, or readiness evaluation, please complete the “RF Certification Notification and Preliminary Questionnaire” form in the Resources section below.

If you wish to send in a Certification Notification and Preliminary Questionnaire, or if you have any questions, please send your request to **entityengagement@rfirst.org**. 

Documents

- **Certification Annual Reminder to RF Entities**
- **RF Certification Notification and Preliminary Questionnaire** 

CERTIFICATION ACTIVITY PROCESS INITIATION

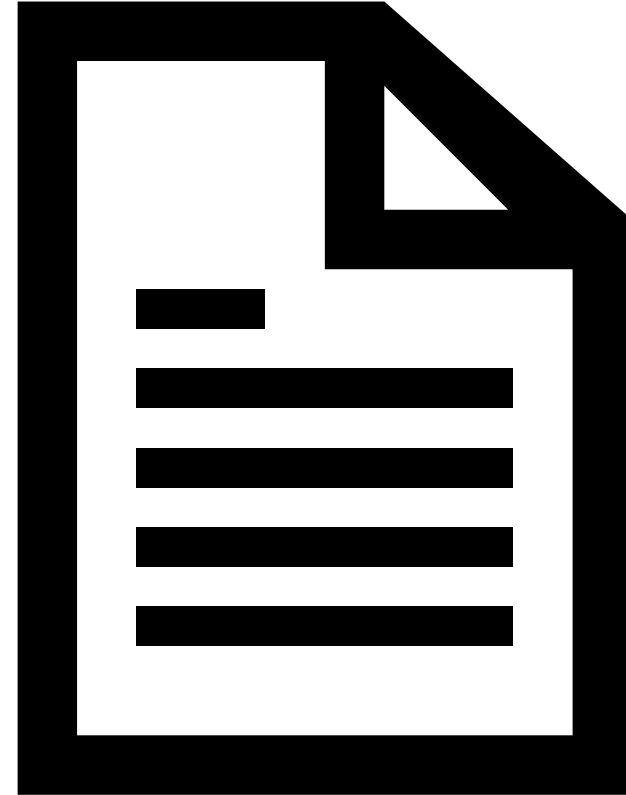
- **Entity notifies RF's Entity Engagement** group regarding changes per the "triggers" mentioned previously
 - Ideally at least 1 year before implementation of the change
- **Entity provides RF an overview of the changes**, including timeline for implementation
 - Entity is asked to provide an application (if not already complete)
 - RF touchpoint with entity to ask questions and get more/clarify information from the application
- **RF consults with NERC** to confirm the need and proposed approach for a review
 - Once confirmed with NERC, RF will start the process with the entity



HIGH-LEVEL PROCESS STEPS

- **RF assembles the review team**
- **RF scopes the applicable standards and creates and sends certification package to entity**
 - Includes matrix of requirements relevant to the changes being made
 - Note: Certifications are a forward-looking engagement and may look at standards that have recently become enforceable or will soon become enforceable
- **Request for Information (RFI) and documentation reviews from entity supplied to review team**
 - Review team reviews responses and documentation and closes out those that require no further action
- **On-site (or virtual) visit to entity for control room tours, interviews, and demonstrations**
 - Address open items
 - Record positive observations and recommendations
- **RF issues final report and letter**





















CERTIFICATION TEMPLATES



CERTIFICATION TEMPLATES

The NERC Organization Certification program page is found at: [Organization Certification](#)

- You will see some example Certification Reports
- You will also see various templates we will use throughout the process under Certification Process Documents

Certification Process Documents (26)	
	01 Certification Review Checklist v1
	02 CT Leader Training Record
	03 CT Member Training Record
	04 Conflict of Interest for Non ERO Employees
	05 ERO Enterprise NDA
	06 Sample CT Composition Approval Letter
	07 RC Pre-Certification Questionnaire
	08 BA Pre-Certification Questionnaire
	09 TOP Pre-Certification Questionnaire
	10 Neighboring Entity Pre-Certification Questionnaire
	11 Certification Master Matrix
	12 Sample Certification Schedule
	13 Sample On-Site Agenda Certification
	14 Full Certification Opening Presentation
	15 Certification Review Opening Presentation
	16 Full Certification Closing Presentation
	17 Certification Review Closing Presentation
	18 Entity Certification Feedback Form
	19 CT Member Feedback Form
	20 Certification Final Report
	21 Certification Review Summary Report
	22 Example RE Full Certification Approval Letter
	23 Example Full NERC Certification Approval Letter
	24 NERC Certification Certificate
	25 Example RE Certification Review Approval Letter
	26 Example NERC Certification Review Approval Letter

EXAMPLE CERTIFICATION OPS MATRIX

		Certification Team Columns in blue				Applicant Response in orange			
Standard	Req #	Text of Requirement	In-Scope?	Request for Initial Documentation/Information (RFI) or Onsite Actions (Onsite)	RFI and/or Onsite Actions (Yes, No, or Bot)	Applicant Response: (process, procedure or tool)	Evidence Provided	Follow Up Questions and/or Onsite Actions	Applicant Response to Follow Up Questions
PER-005-2	1.4.	Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall conduct an evaluation each calendar year of the training program established in	Yes	See above main requirement	RFI			See follow-up RFI for R1	
PER-005-2	R3.	Each Reliability Coordinator, Balancing Authority, Transmission Operator, and Transmission Owner shall verify, at least once, the capabilities of its personnel, identified in Requirement R1 or Requirement R2, assigned to perform each of the BES company-specific Real-time reliability-related tasks identified under Requirement R1 part 1.1 or Requirement R2 part 2.1.	Yes	How was/will the effectiveness of the training of the new EMS be verified? Are there new reliability-related tasks that have been identified and how/when were they trained on?	RFI	Trainees were verified by instructors on their ability to complete tasks during training, or utilized workbooks to show completion. No new tasks were identified as part of this rollout.		RFI: Please provide documents that show this verification was signed by both the trainer and trainees.	
PER-005-2	3.1.	Within six months of a modification or addition of a BES company-specific Real-time reliability-related task, each Reliability Coordinator, Balancing Authority, Transmission Operator, and Transmission Owner shall verify the capabilities of each of its personnel identified in Requirement R1 or Requirement R2 to perform the new or modified BES company-specific Real-time reliability-related tasks identified in Requirement R1 part 1.1 or Requirement R2 part 2.1.	Yes	See above main requirement	RFI			See follow-up RFI for R3	
PER-005-2	R5.	Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall use a systematic approach to develop and implement training for its identified Operations Support Personnel on how their job function(s) impact those BES company-specific Real-time reliability-related tasks identified by the entity pursuant to Requirement R1 part 1.1.	Yes	What was the approach for identifying the training/tasks needed for implementing the new EMS and the cross-coverage?	RFI	Surveys were utilized as part of a DIF analysis to determine areas of focus for training outside of basic navigation and use of the tool.		RFI: Please provide some example surveys for review.	
TOP-001-6	R8.	Each Transmission Operator shall inform its Reliability Coordinator, known impacted Balancing Authorities, and known impacted Transmission Operators of its actual or expected operations that result in, or could result in, an Emergency.	Yes	Have these procedures been modified or updated, related to the new EMS? (If so, please provide.)	RFI	Entity's process by which it informs its Reliability Coordinator, known impacted Balancing Authorities, and known impacted Transmission Operators of its actual or expected operations that result in, or could result in, an Emergency has not changed. How Entity monitors for actual or potential Emergencies is changing based on the use of the new EMS/SCADA system.		Onsite: Please demonstrate the change in how Entity monitors for actual or potential Emergencies on the new EMS/SCADA system.	
TOP-001-6	R9.	Each Balancing Authority and Transmission Operator shall notify its Reliability Coordinator and known impacted interconnected entities of all planned outages, and unplanned outages of 30 minutes or more, for telemetering	Yes	Have these procedures been modified or updated, related to the new EMS? (If so, please provide.)	RFI	Entity's process for notifying its Reliability Coordinator and known impacted interconnected entities of all planned outages, and unplanned outages of 30 minutes or more, for telemetering and control equipment, monitoring and assessment capabilities, and			
TOP-001-6	R10.	Each Transmission Operator shall perform the following for determining System Operating Limit (SOL) exceedances	Yes	Walk through onsite.	Onsite			Onsite: Demonstration for determining SOL exceedance	
TOP-001-6	10.1.	Monitor Facilities within its Transmission Operator Area;	Yes	See R10.	RFI			See R10	

EXAMPLE READINESS EVALUATION OPS MATRIX

Standards	Req #	Text of Requirement	A/S	Assigned or Shared Member TO Tasks	In Scope? (Y/N)	Request for Initial Documentation/Information (RFI) or Onsite Actions (Onsite)	RFI and/or Onsite Actions	Applicant Response: (process, procedure or tool)	Evidence Provided
EOP-008-2	Purpose	Ensure continued reliable operations of the Bulk Electric System (BES) in the event that a control center becomes inoperable.							
EOP-008-2	R1	Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall have a current Operating Plan describing the manner in which it continues to meet its functional obligations with regard to the reliable operations of the BES in the event that its primary control center functionality is lost. This Operating Plan for backup functionality shall include: <i>[Violation Risk Factor = Medium] [Time</i>	A	Each Member TO shall have a current Operating Plan describing the manner in which the Member TO will continue to meet functional obligations with regard to the reliable operations of the BES in the event that the Member TO's primary control center functionality is lost.	Y	For each of the new control centers, provide the new/revised Operating Plan (based on the control center relocations) and demonstrate that the new/revised Operating Plan includes what is required per the Parts of R1 within the scope of this Readiness Evaluation.	RFI	Entity TSO have been combined into one plan for evacuating to their Backup Control Center, (xxx will go to xxx, and vice-versa) as described in xxxxxx - TSO Loss of Control Center Functionality, Rev 0 dated 5/1/24.	• xxxxx - TSO Loss of Control Center Functionality, Rev 0 dated 5/1/24
PER-005-2	R4.	Each Reliability Coordinator, Balancing Authority, Transmission Operator, and Transmission Owner that (1) has operational authority or control over Facilities with established Interconnection Reliability Operating Limits (IROLs), or (2) has established protection systems or operating guides to mitigate IROL violations, shall provide its personnel identified in Requirement R1 or Requirement R2 with emergency operations training using simulation technology such as a simulator, virtual technology, or other technology that	S	Each Member TO shall provide its personnel identified in Requirement R1 with emergency operations training using simulation technology such as a simulator, virtual technology, or other technology that replicates the operational behavior of the BES through participation in PJM training or an equivalent as required by Manual 40.	Y	If Entity does not have (1) operational authority or control over Facilities with established Interconnection Reliability Operating Limits (IROLs), or (2) has established protection systems or operating guides to mitigate IROL violations, simply state this. If Entity has the referenced authority/control over Facilities with established IROLs or has established protection systems or operating guides to mitigate IROL violations, provide documentation that Entity provided new Control Center System Operators (based on the Control Center relocations) with the	RFI	All operators have already received this training for all applicable operating companies. Entity does not have new Control Center System Operators (based on the Control Center relocations) that require the referenced training. Entity provides all its new and current operators with system restoration training using Entity's Operator Training Simulator (OTS).	
TOP-001-5	Purpose	To prevent instability, uncontrolled separation, or Cascading outages that adversely impact the reliability of the Interconnection by ensuring prompt action to prevent or mitigate such occurrences.							
TOP-001-5	R20	Each Transmission Operator shall have data exchange capabilities, with redundant and diversely routed exchange infrastructure within the Transmission Operator's primary Control Center, for the exchange of Real-time data with its Reliability Coordinator, Balancing Authority, and the entities it has identified it needs data from in order to perform its Real-time monitoring and Real-time Assessments.	S	Each Member TO shall have data exchange capabilities, with redundant and diversely routed exchange infrastructure within the Member TO's primary Control Center, for the exchange of Real-time data with PJM and, if applicable, those entities where the Member TO exchanges Real-time data directly with another entity, to allow the Member TO and PJM to perform Real-time monitoring and Real-time Assessments.	Y	Provide documentation that Entity have data exchange capabilities with redundant and diversely routed exchange infrastructure per the PJM shared task.	Either or Both	Entity has data exchange capabilities, with redundant and diversely routed exchange infrastructure, for the exchange of Real-time data with PJM. Entity's routed exchange infrastructure to PJM is described in Entity procedure xxxx, Real-Time Monitoring and Loss of Data Communications (R20.A)	R20.A) xxxx Real-Time Monitoring of Data Communications Revision 4 8/18/23Pages 20-27, Attachment xxxxxEntity

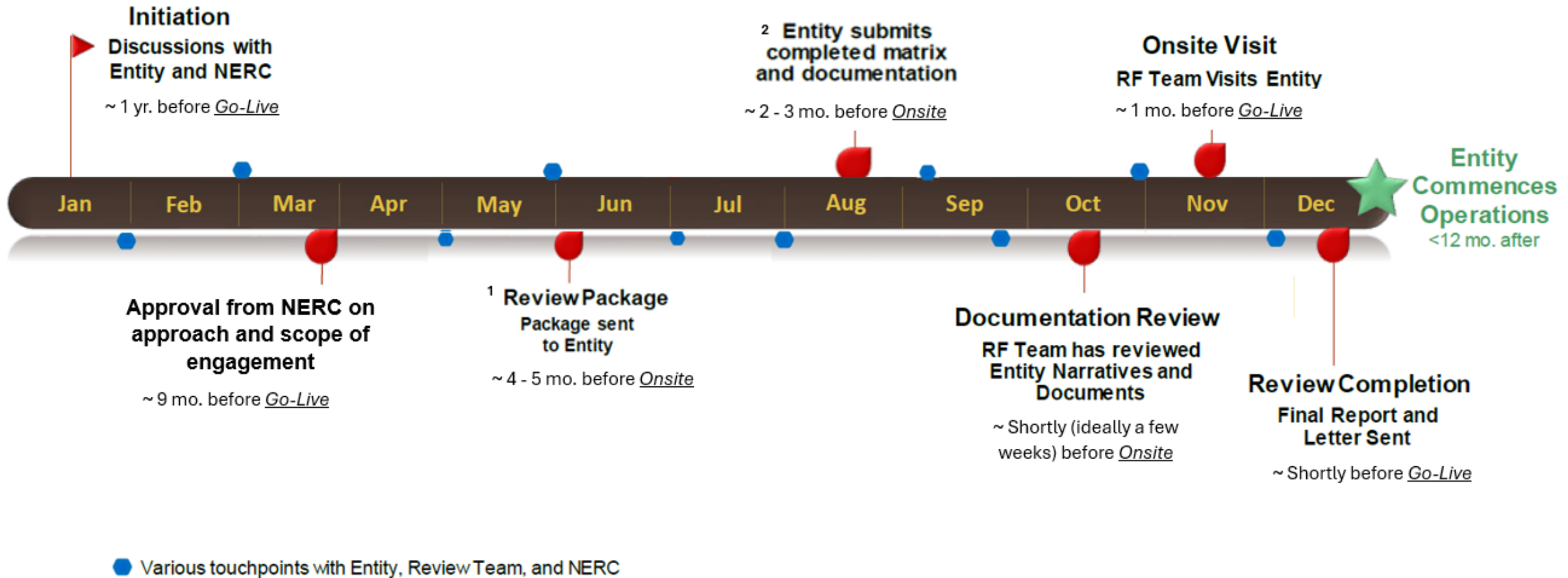
EXAMPLE CERTIFICATION CIP MATRIX

Standard	Req #	Text of Requirement	In-Scope?	Request for Initial Documentation/Information (RFI) or Onsite Actions (Onsite)	Applicant Response: (process, procedure or tool)	Evidence Provided	Follow Up Questions	Applicant Response to Follow Up
CIP-002-5.1	R1.	iii.Generation resources; iv.Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements; v.Special Protection Systems that support the reliable operation of the Bulk Electric System; and vi.For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.	Yes	and BES Facilities is required and critical to BPS reliability. Failure to correctly identify and track items may result in gaps and compromise the integrity and reliability of the BPS. RFI: Please provide the new BES Cyber System list for review. Especially those changes due to new hardware and virtual instances being installed in the new CC and infrastructure update.	Please see the narrative response in file RFI_CIP-002-5.1_R1_V2_Clean, within the CIP-002 folder for further detail.	High Impact BCA List: CIP-002 R1 P1.1 High Impact BCS Device List for in scope xxxxxx Devices: CIP-002 R1 P1.1 High Impact BCS (1).pdf Updated: xxxxxx Device Inventory.pdf	Cyber System Assets types that were provided for CIP-007 baselines (firewalls, network devices, and servers (no workstations). This might require some rework of the documentation provided as either the CIP-002 documentation is correct and we would need new baselines for network devices and workstations or the CIP-007 baseline documentation is correct and we would need additional workstation baselines and a new CIP-002 documentation including the other devices that are in the CIP-007 documentation.	Resolved on 5/1 call regarding file references.
CIP-005-7	R1.	Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-005-7 Table R1 – Electronic Security Perimeter.	Yes	Identity Management and Access Control- Entities must develop controls to prevent or mitigate malicious or unintentional access to BES Cyber Assets. Failure to develop controls may compromise the integrity and operability of the BPS. RFI: Will any ESPs and associated EAPs be changed (i.e. firewall refresh/changes)? Please provide logical/virtual and physical network diagrams for review.	Please refer to the narrative in the document RFI_CIP-005-7_R1_Final.docx within the CIP-005-7>R1 Folder on the site.	Narrative: xxxxxx_R1_Final Process: xxxxxx Evidence: xxxxxx_CIP_Protected_Draft.pdf	5/2 Is this the final diagram before go live? Please provide the latest diagram if possible.	
CIP-007-6	R1.	Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R1 – Ports and Services.	Yes	Identity Management and Access Control- Entities must develop controls to prevent or mitigate malicious or unintentional access to BES Cyber Assets. Failure to develop controls may compromise the integrity and operability of the BPS. Asset/System Management and Maintenance- BPS reliability depends on an entity's success in tracking, managing, and maintaining significant amounts of data, components, assets, and systems. The scope and complexity of this effort require programs to ensure that the entity effectively performs these activities. Failure to execute these programs can result in various types of lapses and may compromise the integrity and reliability of the BPS. RFI- RFI: With the new CC, will there be new baselines for ports and	Please see the narrative RFI_CIP-007_R1.1_RFI_Clean in the CIP-007-6>R1 Folder	Narrative: RFI_CIP-007_R1.1_RFI_Clean Procedure: xxxxxx NERC CIP Ports and Services Procedure (1).pdf Evidence: xxxxxx Sample Devices Port Baseline - CIP Protected.pdf UPDATED 4/30: 20240429 xxxxxx Sample Devices Port	5/1 See CIP-002 Follow Up questions- While reviewing the new version of the CIP-007 baseline document 20240429 xxxxxx Sample Devices Port Baseline - CIP Protected.pdf There were some questions about some of the ports and services identified on some of the baselines. Cisco - How is snmp setup and used within the environment? The justification seems a bit confusing. is snmp setup to allow for configuration of devices? Open Gear - It was noted that the same justification was repeated	Received 5/1.

CERTIFICATION ACTIVITY TIMELINE



CERTIFICATION TIMELINE RECOMMENDED BY RF



¹ ROP requires the certification package be sent no later than 90 days prior to onsite visit

² ROP requires entity to submit matrix and documentation no later than 4 weeks prior to onsite visit

AMBIENT ADJUSTED RATINGS

**FERC ORDER 881 –
MANAGING TRANSMISSION
LINE RATINGS**

FERC ORDER 881

Per FERC Order 881, transmission providers are required to use ambient adjusted ratings (AARs) as the basis for evaluating near-term transmission service to increase the accuracy of near-term line ratings.

- The deadline is July 12, 2025.

When no certification activity is required for AAR implementation

- Entities do not need to submit a certification application/questionnaire to RF for tweaks or adjustments to their Energy Management Systems (EMS) that are specific to the implementation of AARs per FERC Order 881.
 - The purpose of certifications is to allow Regional Entities (like RF) to work with entities to ensure they are ready and able to perform requirements as a newly registered Transmission Operator (TOP), Reliability Coordinator (RC), and/or Balancing Authority (BA), and in some cases when entities make changes to their footprint, control centers, or EMS. ***However, they are generally not designed to prepare entities to comply with NERC Standards, or in this case, a FERC Order.***



NO ACTION
REQUIRED

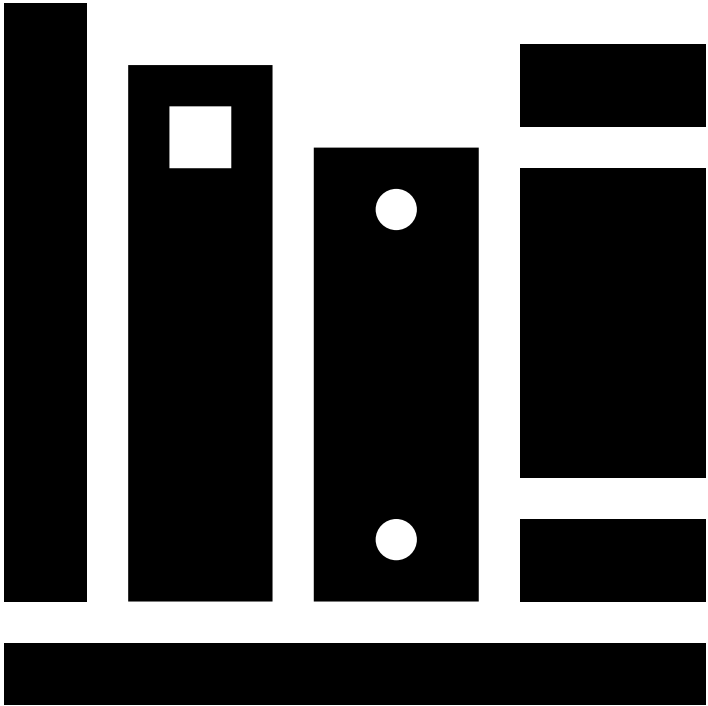
FERC ORDER 881

When certification activity may be needed during AAR implementation

- When your organization's integration of AARs involves additional updates in addition to those required for AAR implementation, such as:
 - When a complete EMS replacement ***goes beyond just minor updates*** of your EMS or SCADA system or a major system upgrade (e.g., going from EMS Version 1.1 to version 2.3 with all new functionality and significantly different operator screens/situational awareness, virtualization changes/implementation, installation of new hardware, etc.), a certification review (or ***lesser certification activity***) may be necessary.
 - In these instances, please complete the RF Certification Notification and Preliminary Questionnaire found on our website at [RF Certification Notification and Preliminary Questionnaire](#).



RESOURCES



HELPFUL RESOURCES

Certification Activities

- [RF Certification Notification and Preliminary Questionnaire](#)
 - ***Email Notification and Preliminary Questionnaire to:*** entityengagement@rfirst.org
- [NERC ROP Sec. 500, App. 5A, Sections IV and V](#)
- [NERC Organization Certification site](#)

FERC Order 881 Activities

- [RF newsletter article: When updates to ambient adjusted ratings \(to comply with FERC Order 881\) require a certification review](#)
- [PJM presentation: FERC Order 881: Ambient Adjusted Ratings](#)
- [MISO is collaborating with transmission owners to implement FERC Order 881](#)
- [12 Months: Countdown to FERC 881 Deadline](#)
- [FERC Final Rule, Docket No. RM20-16, Order No. 881](#)

OUTREACH RESOURCE

Assist Visit Program

In addition to Certifications, our Entity Engagement group performs other outreach, with one specific example being our Assist Visit Program.

It is a “cousin” of certifications (Entity Engagement provides this service with our friendly customer service).

We have an SME for OPs and an SME for CIP that coordinate the program, which allows our entities to ask questions around standards requirements interpretations, internal control evaluations, and more.

We encourage all of you to take advantage of this program.

Please fill out the form on our website at:

<https://www.rfirst.org/tools-and-services/assist-visit/>

Assist Visit Request

Please do not submit any confidential or sensitive information (including CEII, BCSI) using this form or via email. Please be sure to inform us if you are currently engaged in audit activities or if you have an upcoming audit scheduled.

Name *(Required)*

FIRST

LAST

Email *(Required)*

Phone

NERC ID# or Pending NCR# (NCRXXXXX) *(Required)*

Entity Within Audit Period

Check if you have an active or scheduled audit

Prior or Additional Help

Check if you have already asked your questions of us or another region

Attachment

No file chosen

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

- Henry Ford



QUESTIONS & ANSWERS

Sam Ciccone

sam.ciccone@rfirst.org



THANK YOU

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

[Webinar Link](#)

