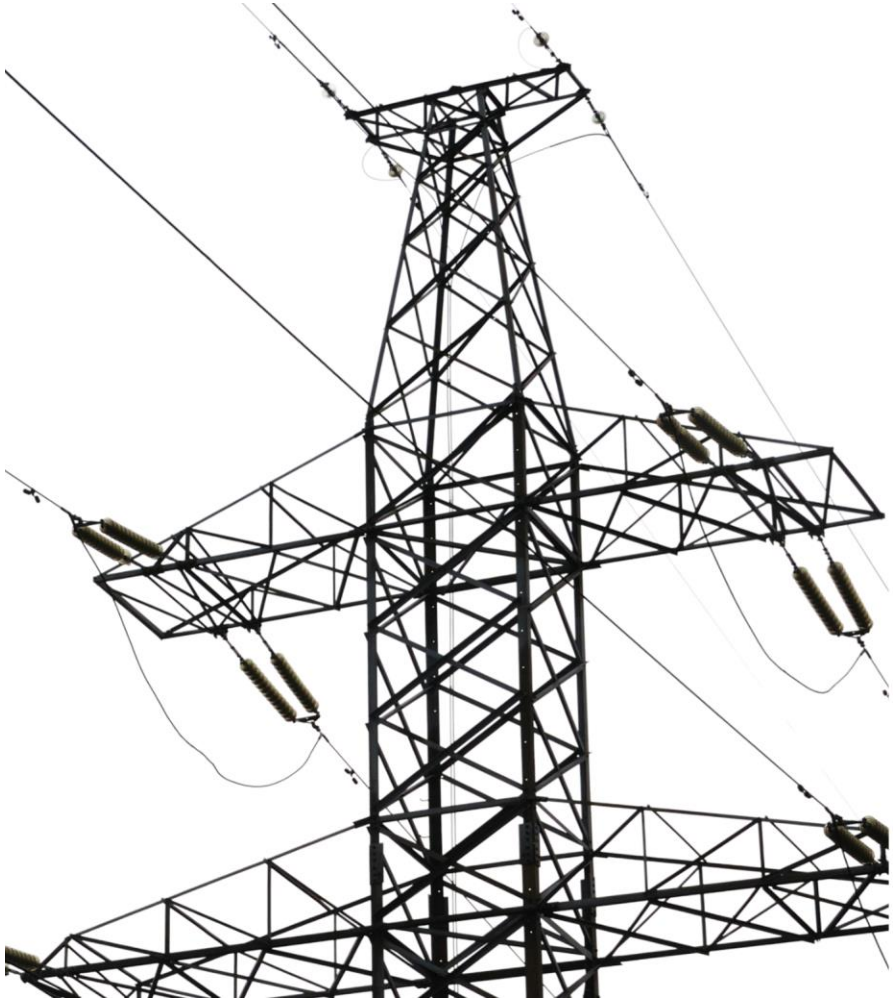
Anti-Trust Statement

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

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



FORWARD TOGETHER RELIABILITYFIRST

2025 FALL RELIABILITY SUMMIT

September 9, 2025

RELIABILITY FIRST

FORWARD TOGETHER RELIABILITYFIRST

2025 FALL RELIABILITY SUMMIT

10:00 a.m. – 4:15 p.m.

Morning Agenda

10:00 – 10:15a.m.	Welcome *Michelle Cross, Manager of Regulatory & Legislative Affairs, ReliabilityFirst*
10:15 a.m. – 12:00 p.m.	Powering the Future: CEO Perspectives on Reliability, Growth, and Security *Tim Gallagher, President & CEO, ReliabilityFirst (moderator)* *Joe McClelland, Director, Office of Energy Infrastructure Security, FERC* *Bill Fehrman, President & CEO, American Electric Power* *Paul Segal, CEO, LS Power* *Christine Martin, President, PPL Electric Utilities* *Todd Snitchler, President & CEO, Electric Power Supply Association*
12:00 – 1:00 p.m.	Lunch / Fireside Chat with FERC Chairman *Jim Robb, President & CEO, NERC (moderator)* *David Rosner, Chairman, FERC*

FORWARD TOGETHER RELIABILITYFIRST

Brian Thiry, Director Strategic Engagement, ReliabilityFirst

Christine Martin, President, PPL Electric Utilities

Bill Fehrman President & CEO, AEP

Todd Snitchler, President & CEO, Electric Power Supply Association

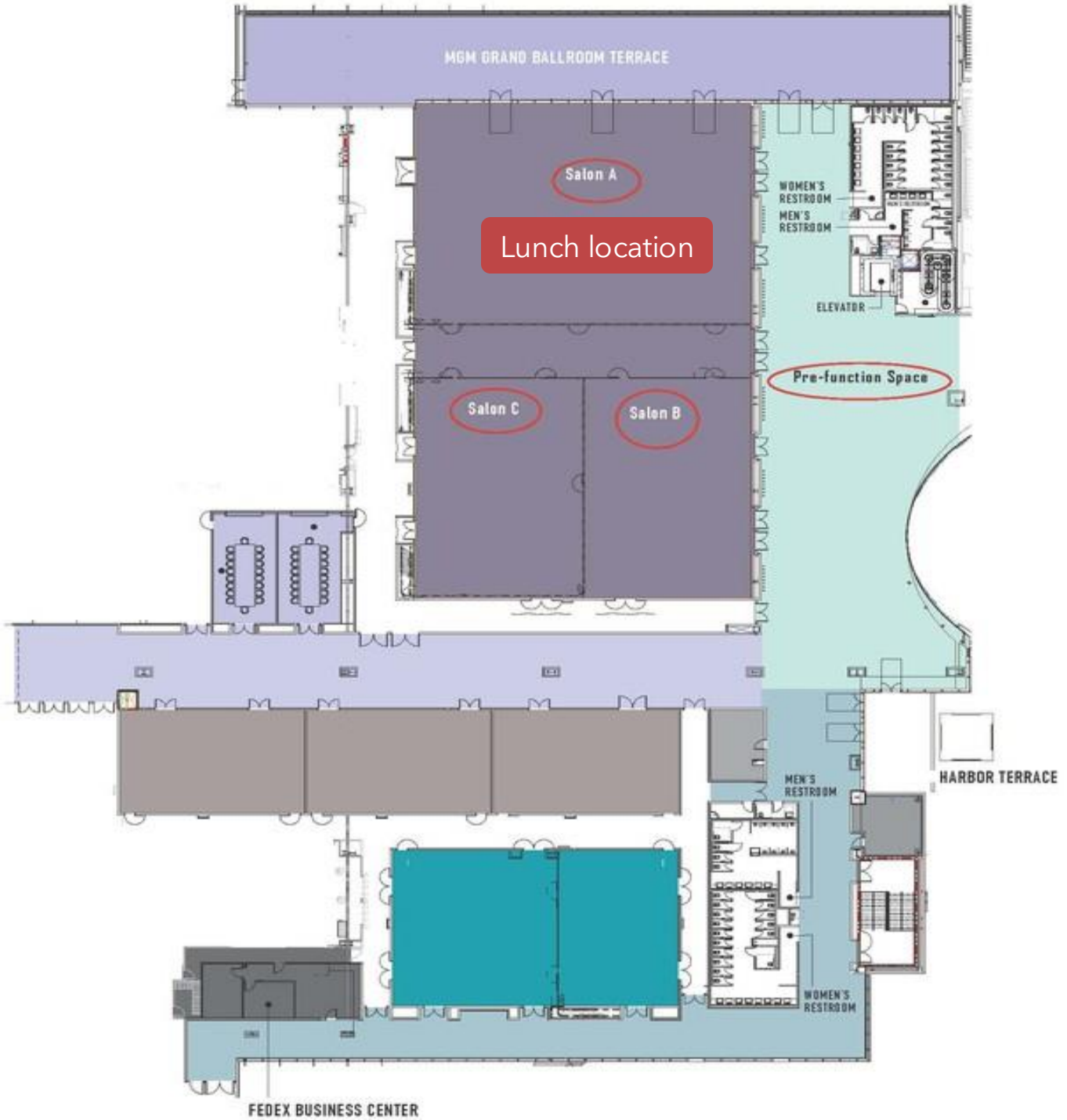
Paul Segal, CEO, LS Power

Joe McClelland, Director, Office of Energy Infrastructure Security, FERC

FORWARD TOGETHER RELIABILITYFIRST

LUNCH & KEYNOTE SPEAKER TIME

12:00 - 1:00 P.M.




Jim Robb
NERC President & CEO
David Rosner
FERC Chairman

FORWARD TOGETHER RELIABILITYFIRST

BREAK TIME

1:00 – 1:30 p.m.

Afternoon Agenda

1:30 – 2:15 p.m.	Standards Solutions – FERC Order 2222 and IBR Initiatives *Deepak Ramlatchan, Deputy Director, Office of Electric Reliability, FERC*
2:15 – 3:00 p.m.	How NextEra's NERC Information Command Center (NICC) Streamlines Reliability, Security, and Compliance *Sergey Peschanyy, Senior Manager of NERC Reliability Standards and Compliance, NextEra Energy*
3:00 – 3:15 p.m.	Break
3:15 – 3:45 p.m.	RF Enforcement and Compliance Updates *Elizabeth Arora, Senior Counsel, Legal and Enforcement, ReliabilityFirst* *Mallory Carlone, Manager, Operations and Planning, ReliabilityFirst*
3:45 – 4:00 p.m.	Wrap-Up

FORWARD TOGETHER RELIABILITYFIRST

ASK QUESTIONS TO PRESENTERS USING SLIDO

Join the conversation at SLIDO.com

#RFSummit25

FORWARD TOGETHER RELIABILITYFIRST

FERC TRANSMISSION REFORM

Deepak Ramlatchan

Deputy Director, Office of
Electric Reliability, FERC

Current and Emerging Solutions for Reliability Challenges

(FERC staff perspective)

Deepak Ramlatchan,
Deputy Director, Office of Electric Reliability
Federal Energy Regulatory Commission

September 2025

Overview

- Intro and OER Key Focus Areas
- Challenges and Solution Opportunities
  - Changing Resource Mix
  - Extreme Weather
  - Cyber Security
  - Load Growth: Large Loads

Office of Electric Reliability

Responsible for protecting and improving the reliability of the Bulk Power System

Oversight of NERC Reliability Standards development and enforcement

Engineering support for other FERC filings and rules

Leadership Team

Kal Ayoub

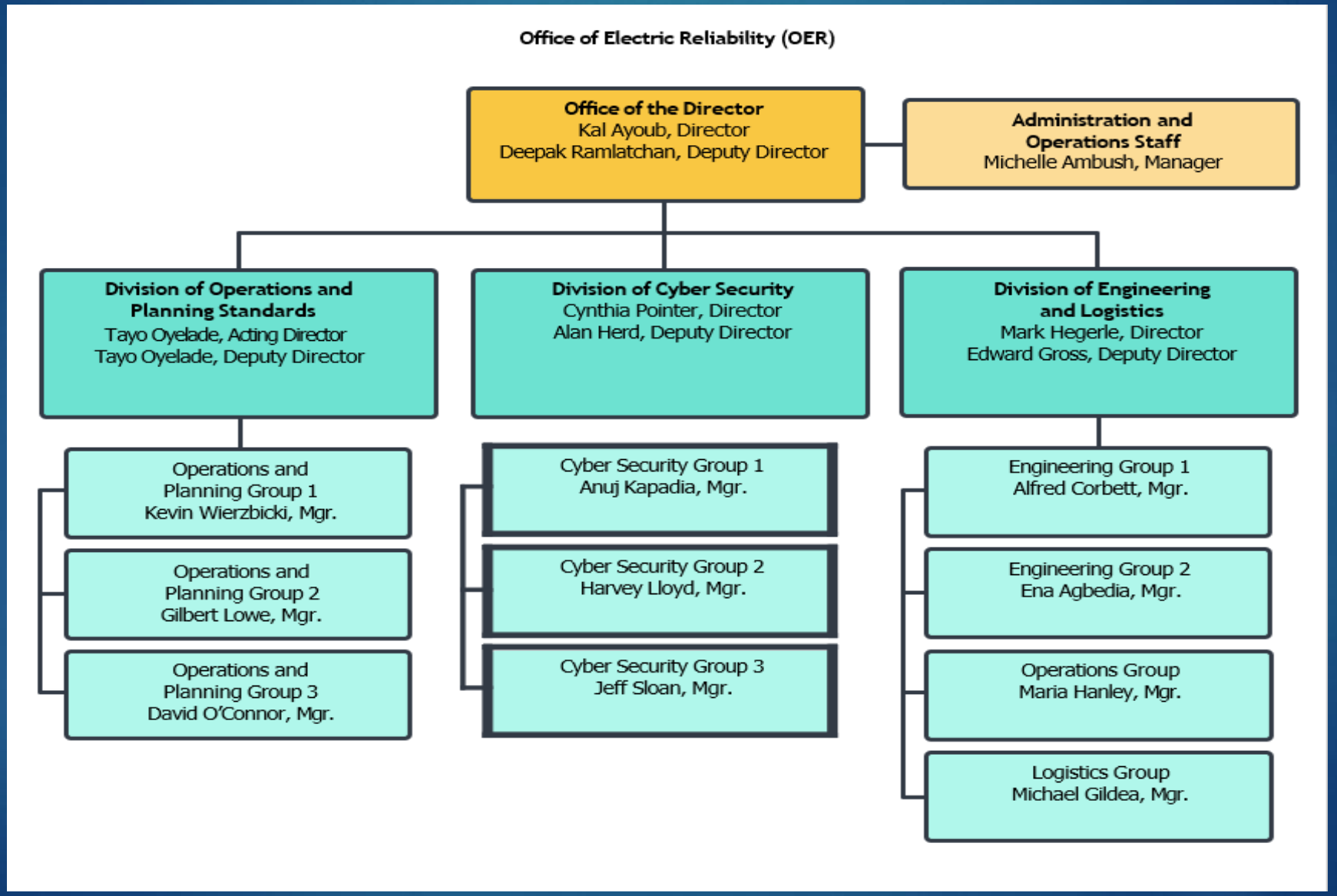
Director

Deepak Ramlatchan

Dep. Director

All opinions are my own and do not reflect the views of the Commission or any individual Commissioner

Office of Electric Reliability



OER Priorities

Cyber and Physical Security

Supply Chain Compromise
Protections for Low Impact Assets
Physical Security

Resource Transition

Inverter Based Resources (IBR)
Resource/Energy Adequacy
Priority System Attributes (e.g., quick start, ramping)

Extreme Weather

Asset Hardening (e.g., generator freeze protection)
System Planning and Design

5

Office of Electric Reliability

OER is the Commission's lead reliability office under section 215 of the FPA. OER performs the oversight role for electric reliability, approving and enforcing reliability standards developed by NERC

- Advise on whether to approve, remand or require changes to reliability standards proposed by NERC
  - Monitor or process 10-30 new or revised reliability standards per year
- Oversee compliance with approved standards by users, owners, and operators of the Bulk-Power System (BPS)

OER Functions and Responsibilities

- Review NERC-proposed penalties
- Provide technical support on tariff filings and rulemakings, focusing on system engineering and reliability impacts
  - Review over 500 FPA section 205/206 filings per year
- Analyze and issue reports on blackouts and major grid events with recommendations to mitigate recurrence
- Monitor the bulk-power system 24/7 to ensure the Commission is informed of major and evolving system events
- Perform seasonal energy market and electric reliability assessment

Actions to Address Reliability Challenges

- Resource Transition
  - Order No. 901 – directives for new or revised reliability standards covering IBR data sharing, model validation, planning and operational studies, and performance requirements
  - IBR Registration Orders (RD22-4, RR24-2) – Issued June 2024, requires NERC to determine which IBRs are required to comply with relevant reliability standards by May 2026

Actions to Address Reliability Challenges

- Order 901
  - Three batches of standards due November 2024, 2025, and 2026
  - First batch filed: November 2024 (Commission approved)
    - Performance requirements for frequency and voltage Ride-through, post-disturbance ramp rates, phase lock loop synchronization, other known causes of IBR tripping or momentary cessation, disturbance monitoring data sharing, and post-event performance validation for registered IBRs.
      - PRC-028-1 - Disturbance Monitoring and Reporting for IBRs – approved in RD25-2-000, February 2025.
      - PRC-029-1 - Frequency and Voltage Ride-through Requirements for IBRs – approved with directives in RM25-3-000 (Order No. 909), July 2025 ***[Note: pending request for clarification]***
      - PRC-030-1 - Unexpected IBR Event Mitigation – approved in RD25-3-000, February 2025

Actions to Address Reliability Challenges

- Order 901
  - Second batch November 4, 2025: Data sharing, data and model validation for registered IBRs, unregistered IBRs, and IBR-DERs in the aggregate.
  - Third batch November 2026: Planning and operational studies for registered IBRs, unregistered IBRs, and IBR-DERs in the aggregate.
  - Effective Date of New or Revised Standards: all new or modified IBR-related Reliability Standards must be effective and enforceable "well in advance of 2030."

Actions to Address Reliability Challenges

- Cybersecurity

- **Internal Network Security Monitoring**: issued Order No. 907 (June 2025) and Order No. 907-A (August 2025) approving Reliability Standard CIP-015-1 that requires internal network security monitoring inside an entity's electronic security perimeter and directing modifications to extend protections to access control systems outside of the electronic security perimeter (RM24-7).
- FERC-led CIP Compliance Audits: Commission staff continue to conduct non-public cybersecurity audits for compliance with the CIP Reliability Standards, and publish an annual anonymized report on lessons learned from those audits for the benefit of industry and stakeholders.

Actions to Address Reliability Challenges

- Cybersecurity – potential future action

- Low Impact Security: NERC filed modifications to Reliability Standard CIP-003 (December 2024) with improved protections for low impact assets; currently pending Commission action.
- Virtualization: NERC filed modifications to 11 of 13 CIP Reliability Standards (July 2024), as supplemented in a petition (May 2025), primarily to address the use of virtualization and other emerging technologies; currently pending Commission action.
- Supply Chain Security: issued Notice of Proposed Rule Making (September 2024) to direct NERC to develop new/modified Reliability Standards to address gaps in the Reliability Standards related to Supply Chain Risk Management (RM24-4). Held a public workshop (March 2025).

Actions to Address Reliability Challenges

- Extreme Weather
- TPL-008-1 (Transmission System Planning Performance Requirements for Extreme Temperature Events), filed in response to Order No. 896, approved February 2025
- EOP-012-3 (Extreme Cold Weather Preparedness and Operations), the revised generator winterization reliability standard, filed April 2025 in RD25-7-000
  - Commission previously accepted and directed further revisions to address concerns pertaining to generator cold weather constraints and corrective action implementation

Emerging Opportunities

Order No. 2222 and 2222-A

- Eliminate barriers to DER aggregation participation in the RTO/ISO markets.
  - Barriers present when the rules governing participation in those markets are designed for traditional resources and limit the services that emerging technologies can provide.
    - E.g., most DERs tend to be too small to meet minimum size requirements to participate in the markets on a stand-alone basis and may be unable to meet certain qualification and performance requirements.
  - Previous participation models for aggregated resources, including DERs, often require those resources to participate in the RTO/ISO markets as demand response, which limits their operations and the services that they are eligible to provide.
  - By removing barriers to the participation, Order No. 2222 enhances competition and, in turn, allows a larger portfolio of resources to provide essential services.

Emerging Opportunities

- Order No. 2222
- Defines a DER as "any resource located on the distribution system, any subsystem thereof or behind a customer meter."
  - Resources may be in front of and behind the customer meter, electric storage resources, intermittent generation, distributed generation, demand response, energy efficiency, thermal storage, EVs (and others).
  - Definition is technology-neutral, thereby ensuring that any resource that is technically capable of providing wholesale services through aggregation is eligible to do so
- Defines a DER aggregator as "the entity that aggregates one or more DERs for purposes of participation in the capacity, energy and/or ancillary service markets of the RTOs and/or ISOs."
  - The DER aggregator is the RTO/ISO market participant, not the DER, and is the single point of RTO/ISO contact: responsible for managing, dispatching, metering and settling the individual resources.

Emerging Opportunities

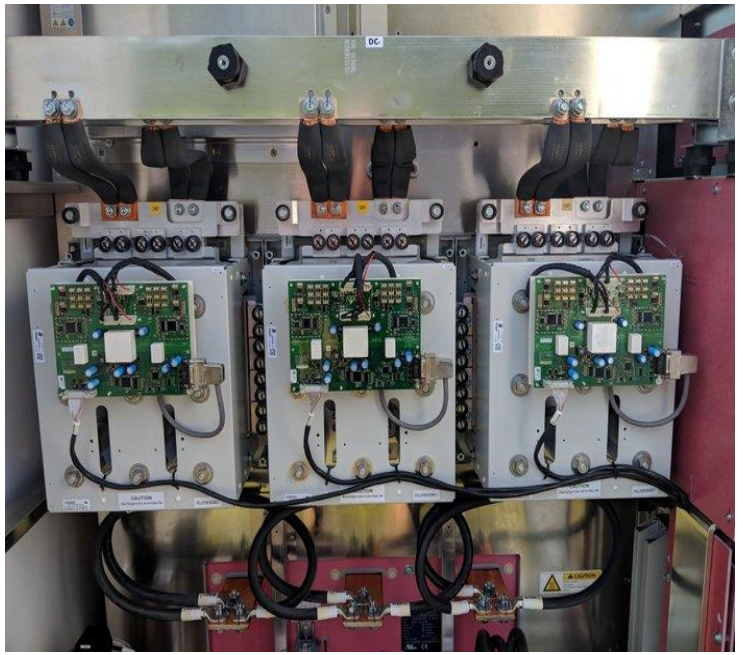
- Order No. 2222
  - For each RTO/ISO, the tariff provisions addressing distributed energy resource aggregations must:
    - Allow DER aggregations to participate directly in RTO/ISO markets and establish DER aggregators as a type of market participant;
    - Establish a **minimum size requirement** for DER aggregations that does not exceed 100 kW and allow heterogenous aggregations;
    - Address **locational requirements** for DER aggregations;

Emerging Opportunities

- Order No. 2222
  - PJM Roll-Out:
    - Energy & Ancillary Services: February 2028
    - Capacity Market: 2028/2029 delivery year
  - Potential Implications
    - Driver of Virtual Power Plants
    - Another participation model for microgrids
    - Virtualization/cyber implications

Emerging Opportunities

- Additional Emerging Solutions
  - Interconnection:
    - Order 2023
    - Queue specific acceleration initiatives
    - Artificial Intelligence
  - Grid Forming Inverters
    - Can establish voltage and frequency



Load Growth: Large Loads

- NERC Large Load Task Force
  - Power System Stability
  - Resource Adequacy
  - BPS Balancing and Reserves
- FERC's 206 Proceeding on co-located loads
- Region Specific Initiatives
  - PJM Critical Issue Fast Path

Megapack

"Today's problem is dealing with extreme power jitter…

We are having some power fluctuation issues, when you do synchronized training it's like having an orchestra and it can go loud to quiet very quickly, at the sub-second level. The electrical system freak out about that – with 10-20 MW shifts several times per second."

- Elon Musk
  August 2024 in conversation with Lex Fridman about xAI Memphis data center

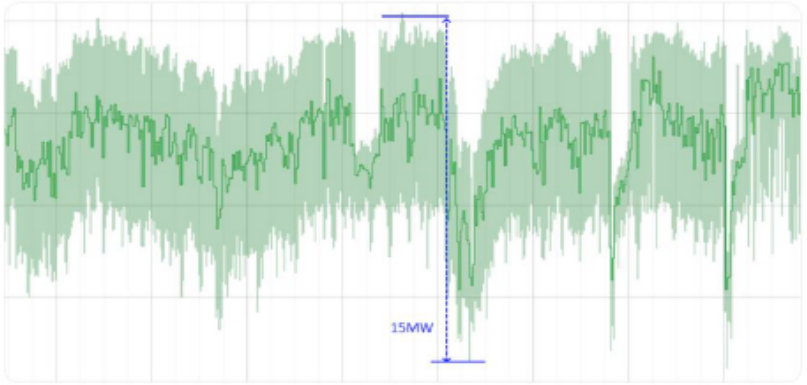


Fig. 1. Large power fluctuations observed on cluster level with large-scale synchronized ML workloads

"In our latest batch-synchronous ML workloads running on dedicated ML clusters, we observed power fluctuations in the tens of megawatts"

- Google Technical Lead Manager and VP, Engineering
  February 2025, Blog Post

Large Load Issues

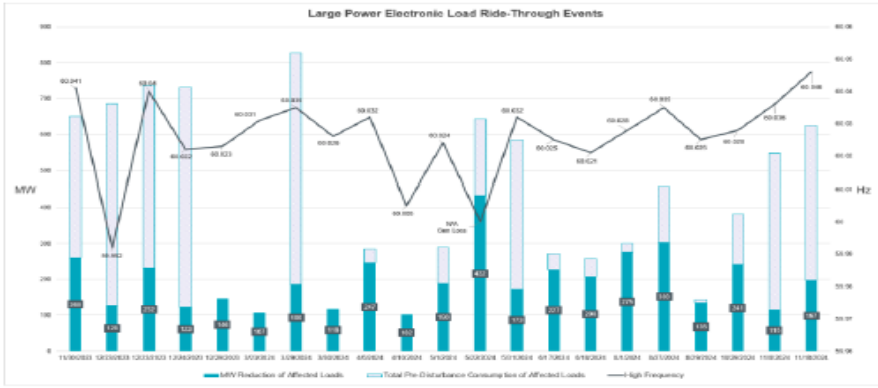
Megapack

Challenge: Low Voltage Ride Through (LVRT) of data centers

Dominion: 1.5 GWs across 60 data centers

July 2024 – due to reclosing attempts on faulted 230 kV system

ERCOT: Many events of 100s of MWs



Grid Operator Perspective

- Challenging to manage load drops at this scale
- Over frequency and voltage concerns

Data Center Perspective

- UPS systems working as intended
- Protecting our expensive and reliability critical equipment from utility system faults

Large Load Issues

Upcoming

- September Commission Meeting
- Annual Reliability Technical Conference
  - This year scheduled for October 21
- Modernization of Standards Processes and Procedures Task Force
  - Recommendations to the Board February 2026

Questions

- Challenges and Solution Opportunities
  - Changing Resource Mix
  - Extreme Weather
  - Cyber Security
  - Load Growth: Large Loads

FORWARD TOGETHER RELIABILITYFIRST

HOW NEXTERA'S NERC INFORMATION COMMAND CENTER (NICC) STREAMLINES RELIABILITY, SECURITY, AND COMPLIANCE

Sergey Peschanyy

Senior Manager of NERC Reliability Standards and Compliance, NextEra Energy

Managing Risk to the Bulk Electric System

NextEra Energy - NERC Information Command Center (NICC)

Presenters:

Sergey Peschanyy, Senior Manager – NERC Center of Excellence

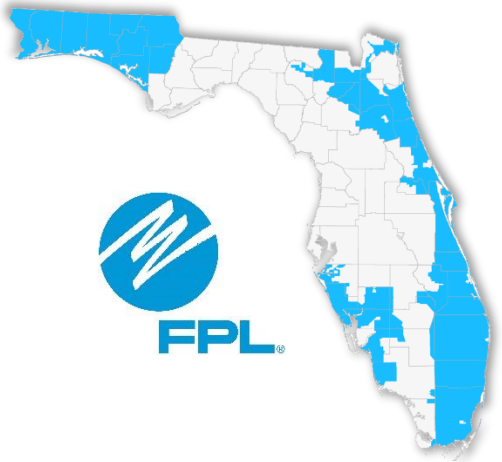
Date:

September 9, 2025

NextEra Energy is powered by industry leading companies focused on customer value and operational excellence.

NEXTera ENERGY

- World's largest generator of renewable energy from the wind and sun, committed to producing clean, emissions-free electricity across North America.

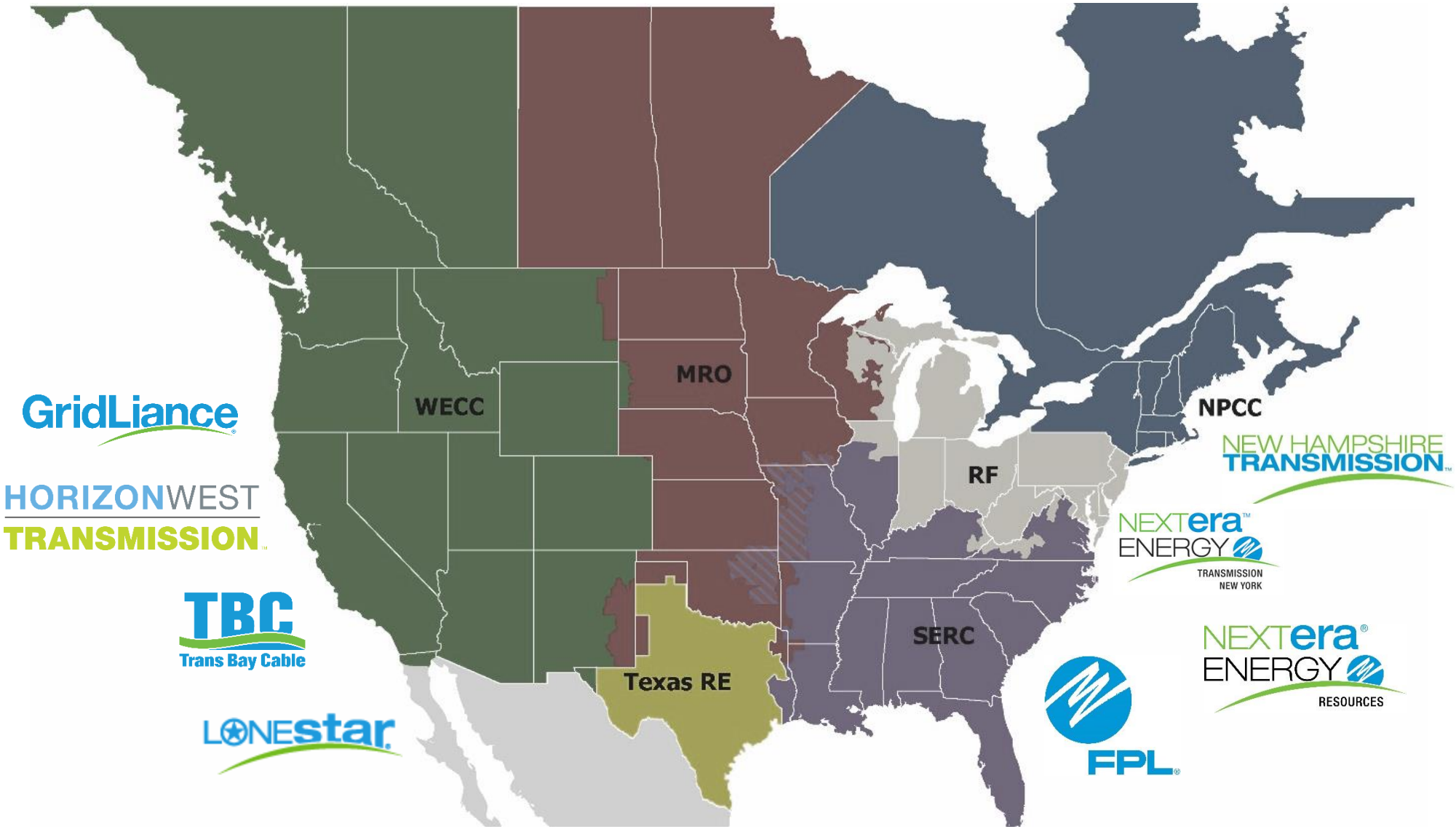


- America’s largest energy utility (vertically integrated) serving over 12 million people across Florida with reliable and affordable electric power.

NEXTera™ ENERGY TRANSMISSION

- Leading competitive transmission company that owns, develops, finances, constructs, operates and maintains transmission assets across North America.
- Operates through its regional subsidiaries to integrate renewable energy and strengthen the electric grid..

NextEra Energy's NERC compliance obligations span across several subsidiaries and operate in every region.



NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Organization Registration and Certification Program and Compliance Monitoring and Enforcement Program Annual Report

February 12, 2025

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Top 10 O&P Noncompliance Reported in 2024

In 2024, the most frequently reported noncompliance involving the O&P Standards included PRC-005, FAC-008, MOD-025 and VAR-002. FAC-008 has been an ERO Enterprise focus area for several years. PRC-005 and VAR-002 both involve high frequency conduct. MOD-025 involves verification and reporting of generator and synchronous condenser real and reactive power capability to the transmission planners. MOD-025 has the highest reported noncompliance of the MOD family.

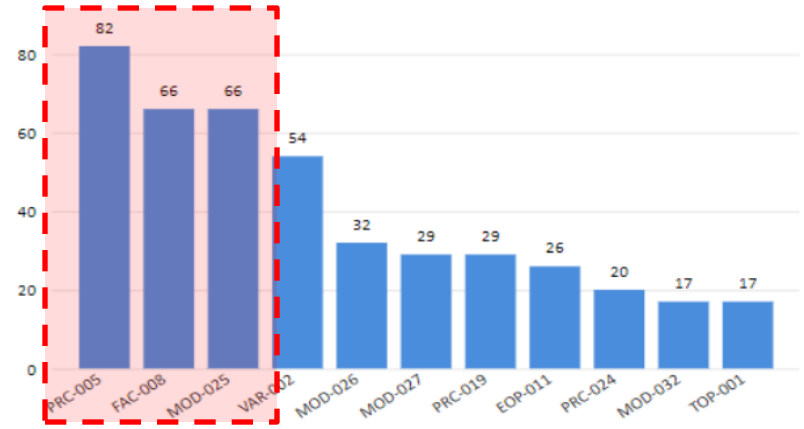


Figure 7: Top 10 O&P Noncompliance Reported in 2024

Top 10 CIP Noncompliance Reported in 2024

In 2024, the most frequently reported noncompliance involving the CIP Standards included CIP-010, CIP-007, and CIP-004, which all involve high volume and high frequency conduct.

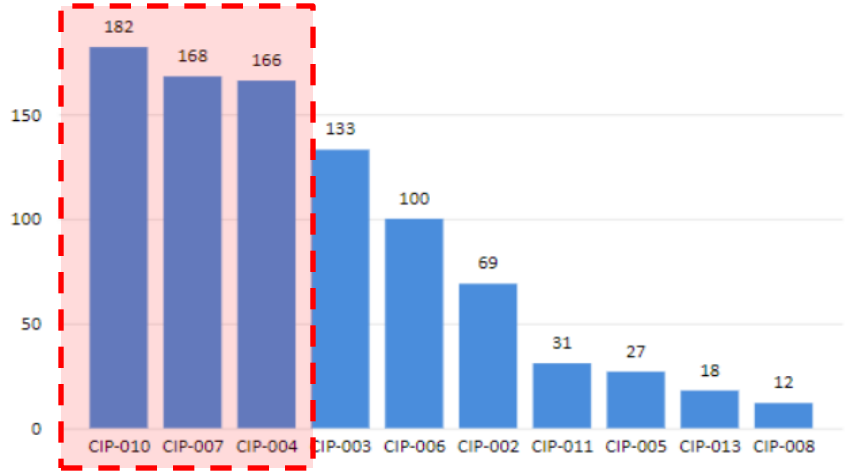


Figure 6: Top 10 CIP Noncompliance Reported in 2024

There are 83 NERC Reliability Standards with over 1,400 individual requirements requiring strict compliance.

Critical Infrastructure Protection (CIP)

Standard Number	Standard Title	Standard Number	Standard Title	Standard Number	Standard Title
CIP-002-5.1a	Cyber Security — BES Cyber System Categorization	CIP-007-6	Cyber Security — System Security Management	CIP-012-1	Cyber Security – Communications between Control Centers
CIP-003-8	Cyber Security — Security Management Controls	CIP-008-6	Cyber Security — Incident Reporting and Response Planning	CIP-013-2	Cyber Security - Supply Chain Risk Management
CIP-004-6	Cyber Security — Personnel & Training	CIP-009-6	Cyber Security — Recovery Plans for BES Cyber Systems	CIP-014-3	Physical Security
CIP-005-7	Cyber Security — Electronic Security Perimeter(s)	CIP-010-4	Cyber Security — Configuration Change Management and Vulnerability Assessments	CIP-015	System Access Control Internal Network Monitoring (New)
CIP-006-6	Cyber Security — Physical Security of BES Cyber Systems	CIP-011-2	Cyber Security — Information Protection		

Initial Scope Of The NICC

Operations and Planning (O&P)

Standard Number	Standard Title	Standard Number	Standard Title	Standard Number	Standard Title	Standard Number	Standard Title
BAL-001-2	Real Power Balancing Control Performance	FAC-003-5	Transmission Vegetation Management	PRC-004-6	Protection System Misoperation Identification and Correction	TOP-001-6	Transmission Operations
BAL-002-3	Disturbance Control Standard – Contingency Reserve for Recovery from a Balancing Contingency Event	FAC-008-5	Facility Ratings	PRC-005-6	Protection System, Automatic Reclosing, and Sudden Pressure Relaying Maintenance	TOP-002-5	Operations Planning
BAL-005-1	Balancing Authority Control	FAC-011-4	System Operating Limits Methodology for the Operations Horizon	PRC-006-5	Automatic Underfrequency Load Shedding	TOP-003-7	Transmission Operator and Balancing Authority Data and Information Specification and Collection
BAL-007-1	Near-term Energy Reliability Assessments	FAC-014-3	Establish and Communicate System Operating Limits	PRC-008-0	Implementation and Documentation of Underfrequency Load Shedding Equipment Maintenance Program	TOP-010-1(i)	Real-time Reliability Monitoring and Analysis Capabilities
COM-001-3	Communications	MOD-025-2	Verification and Data Reporting of Generator Real and Reactive Power Capability and Synchronous Condenser Reactive Power Capability	PRC-010-2	Undervoltage Load Shedding	TPL-001-5.1	Transmission System Planning Performance Requirements
COM-002-4	Operating Personnel Communications Protocols	MOD-026-1	Verification of Models and Data for Generator Excitation Control System or Plant Volt/Var Control Functions	PRC-011-0	Undervoltage Load Shedding System Maintenance and Testing	TPL-007-4	Transmission System Planned Performance for Geomagnetic Disturbance Events
EOP-004-4	Event Reporting	MOD-027-1	Verification of Models and Data for Turbine/Governor and Load Control or Active Power/Frequency Control Functions	PRC-012-2	Remedial Action Schemes	TPL-008-1	Transmission System Planning Performance Requirements for Extreme Temperature Events
EOP-005-3	System Restoration from Blackstart Resources	MOD-031-3	Demand and Energy Data	PRC-017-1	Remedial Action Scheme Maintenance and Testing	VAR-001-5	Voltage and Reactive Control
EOP-006-3	System Restoration Coordination	MOD-032-1	Data for Power System Modeling and Analysis	PRC-019-2	Coordination of Generating Unit or Plant Capabilities, Voltage Regulating Controls, and Protection	VAR-002-4.1	Generator Operation for Maintaining Network Voltage Schedules
EOP-008-2	Loss of Control Center Functionality	MOD-033-2	Steady-State and Dynamic System Model Validation	PRC-023-6	Transmission Relay Loadability	TOP-003-7	Transmission Operator and Balancing Authority Data and Information Specification and Collection
EOP-010-1	Geomagnetic Disturbance Operations	NUC-001-4	Nuclear Plant Interface Coordination	PRC-024-3	Frequency and Voltage Protection Settings for Generating Resources	TOP-010-1(i)	Real-time Reliability Monitoring and Analysis Capabilities
EOP-011-4	Emergency Operations	PER-003-2	Operating Personnel Credentials	PRC-025-2	Generator Relay Loadability	TPL-001-5.1	Transmission System Planning Performance Requirements
EOP-012-2	Extreme Cold Weather Preparedness and Operations	PER-005-2	Operations Personnel Training	PRC-026-2	Relay Performance During Stable Power Swings	TPL-007-4	Transmission System Planned Performance for Geomagnetic Disturbance Events
FAC-001-4	Facility Interconnection Requirements	PER-006-1	Specific Training for Personnel	PRC-027-1	Coordination of Protection Systems for Performance During Faults	TPL-008-1	Transmission System Planning Performance Requirements for Extreme Temperature Events
FAC-002-4	Facility Interconnection Studies	PRC-002-5	Disturbance Monitoring and Reporting Requirements	PRC-028-1	Disturbance Monitoring and Reporting Requirements for Inverter-Based Resources		

= NICC Operational (Monitored & Audit Supported) By EOY 2025

= All Others Integrated 2026 Thru 2028

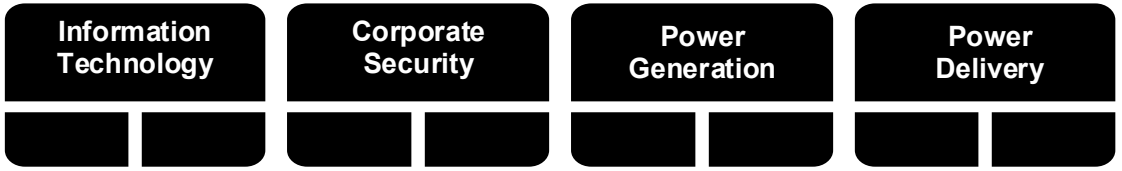
This equates to more than 1 million compliance tasks that need to be completed and documented successfully EACH YEAR to be fully compliant! Even achieving a Six Sigma quality level would result in 3 or 4 non-compliances (subject to financial penalties) every year!

In 2020, we saw an opportunity and a need to reimagine our approach specific to our NERC compliance program.

Audit Support

Before

Spin up the audit machine / Reactive

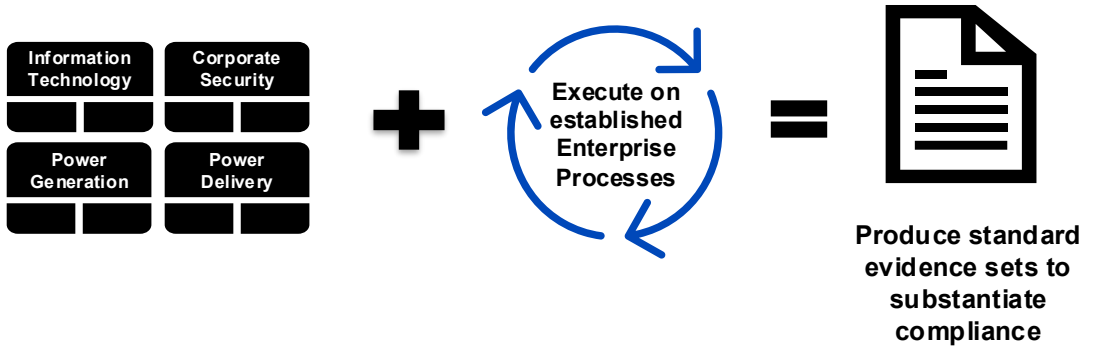


- Manual evidence production / minimal information validation
- Different processes and interpretations of what was needed to substantiate compliance
- Presentation by business unit resulted in fragmented view / representation of the registered entity
- O&M costs associated with audit support and execution continued to increase
- Focus was on compliance not on managing security risk

After

Always Audit Ready / Proactive

FPL · NEXTera ENERGY RESOURCES · LONEstar · NEXTera ENERGY TRANSMISSION NEW YORK · NEW HAMPSHIRE TRANSMISSION · GridLiance · HORIZONWEST TRANSMISSION · TBC Trans Bay Cable



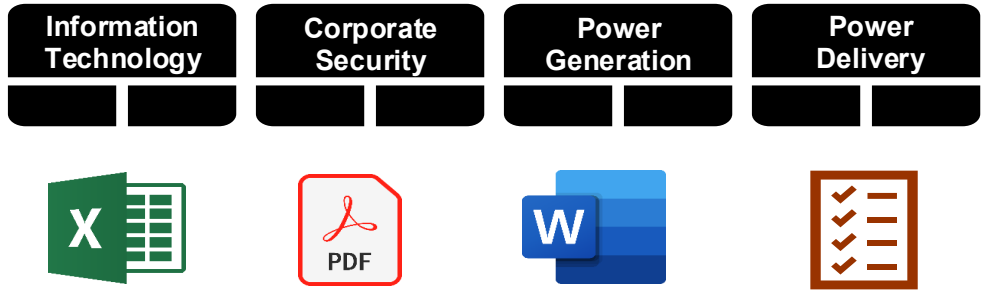
Produce standard evidence sets to substantiate compliance

In 2020, we saw an opportunity and a need to reimagine our approach specific to our NERC compliance program.

Audit Support

Before

"Spin up the audit machine" / Reactive



- Manual evidence production / minimal information validation
- Different processes and interpretations of what was needed to substantiate compliance
- Presentation by business unit (vs. Registered Entity) resulted in fragmented view / representation of the registered entity
- O&M costs associated with audit support and execution continued to increase
- Focus was on compliance not on managing security risk

Only Time Compliance Evidence is 100% Assembled, Tested & Assured

Preparation

- Months of manual planning & preparation
- 100+ people
- Unsure of scope
- Boil the ocean

Audit Notification

- Company
- Date Range
- Standards & Requirements

Evidence Generation

- Process Narratives (RSAW)
- Audit Workbook (ERT)
- Initial Evidence Requests (L1/L2 & Follow-On Data Requests)

Submission to Auditors

- Audit scope drives level of effort & cycle time

Hours devoted to manual prep work not relevant to audit scope could have been used elsewhere

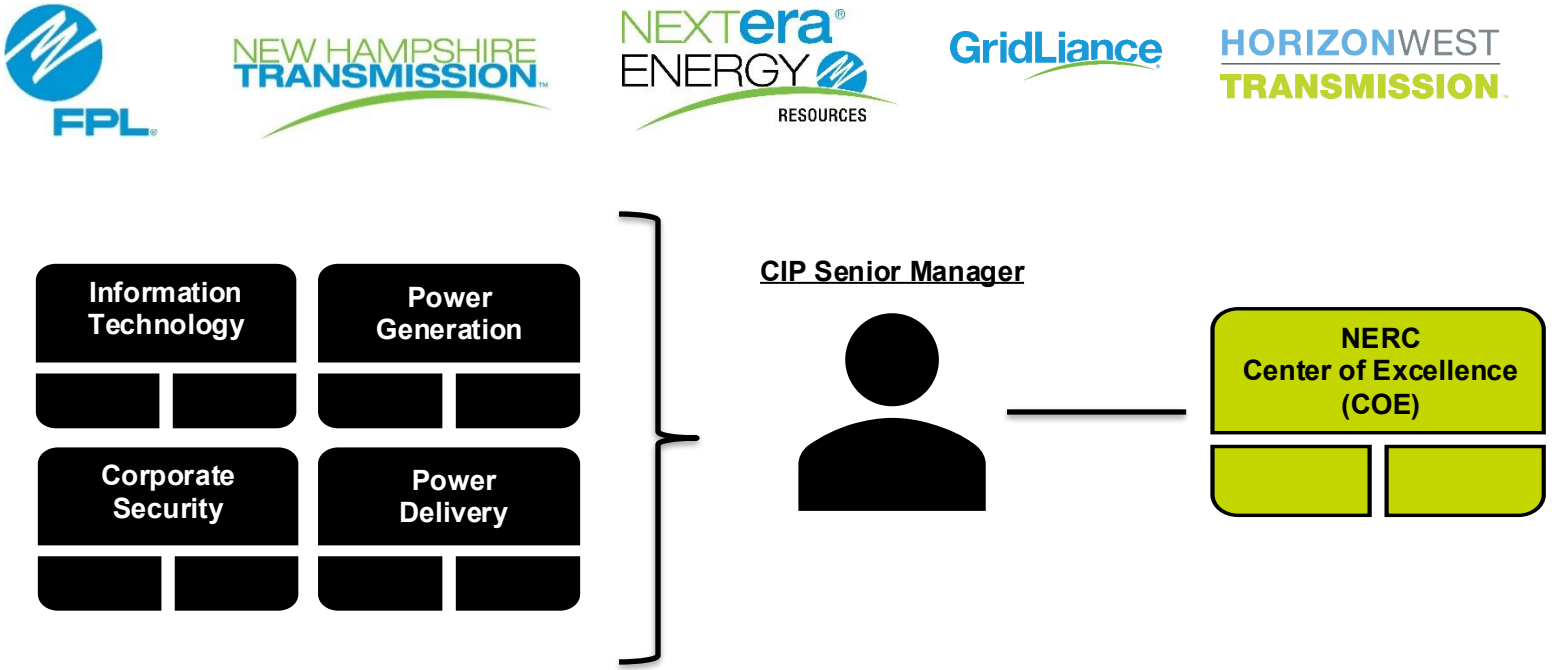
"Open Book Test"

Subsequent "ad-hoc" requests for evidence

On site interviews

Automation of evidence generation, quality assurance, and delivery is how we go from Good to Great

To induce change, we needed an organization that could serve as an aggregator with purview across all lines of business and all registered entities.



1. **Ensuring Compliance and Security**: The NERC CIP Center of Excellence (CIP COE) at NextEra Energy ensures compliance with NERC CIP standards through robust processes that safeguard the physical and cyber security of critical infrastructure.
2. **Proactive Risk Mitigation**: CIP COE plays a key role in mitigating security and compliance risks by proactively addressing potential cyber vulnerabilities and ensuring essential protections are in place to secure operations.
3. **Expert Support and Validation**: As subject matter experts, the CIP COE provides strategic support during audit engagements, ensuring regulatory compliance and validating the accuracy and reliability of compliance-related information.
4. **Enhancing Resilience and Operational Excellence**: By integrating best practices and rigorous oversight, the NERC CIP COE enhances NextEra Energy's security posture, resilience, and commitment to operational excellence.

One Team, One CIP Program

Information Management

Program Management

Risk Management

With our reimagination efforts underway, the NERC Center of Excellence established a vision for the future that would capitalize on an environment that was data rich.

NEE Registered Entities performing NERC Registered Functions

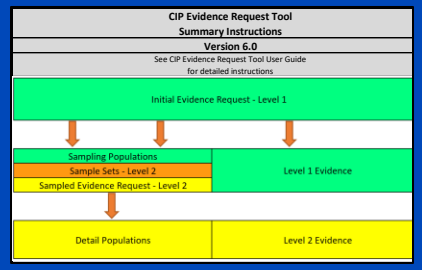
FPL
TBC Trans Bay Cable
LONEstar
NEW HAMPSHIRE TRANSMISSION
NEXTera ENERGY RESOURCES
NEXTera ENERGY TRANSMISSION
HORIZONWEST TRANSMISSION
GridLiance

NEE Service Organizations supporting grid reliability / security

- Information Technology
- Corporate Security
- Power Generation
- Power Delivery
- Integrated Supply Chain
- Human Resources

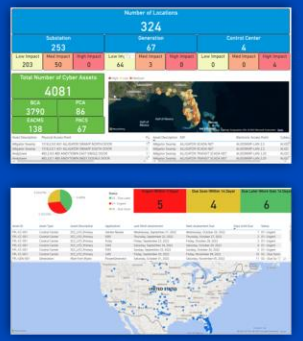
Execute on established Enterprise Processes

Leverage common toolset



NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION
Reliability Standard Audit Worksheet[1]
CIP-003-8 – Cyber Security — Security Management Controls

Continuous Audit Readiness



Real-Time Operational Monitoring

Establish common meta data and aggregate into a unified CIP Data Warehouse

Produce standard evidence sets to substantiate compliance

Program Approach we moved toward

NEXTera ENERGY

What is Continuous Monitoring?

Foundational Elements of a Continuous Monitoring System

1

Automated and Verified Systems

Monitor threats, vulnerabilities, and compliance status continuously, ensuring data accuracy and completeness.

(NIST SP 800-137, Section 3.1.2)

2

Timely Awareness and Real-Time Information Validation

Provide timely notifications about potential issues and validate compliance in real-time, maintaining continuous audit readiness.

(NIST SP 800-137, Sections 2.3.2 and 3.1.3)

3

Complete and Frequent Data Acquisition

Comprehensive data sets are gathered and validated frequently to inform monitoring efforts and detect emerging issues early.

(NIST SP 800-137, Sections 3.1.4 and 3.1.5)

4

Proactive Auditing

Real-time data is used to perform continuous and proactive auditing, enhancing control testing and validation frequency.

(NIST SP 800-137, Section 3.2.4)

5

Informed Decision Making and Risk Management

Automated and human decision-making is supported via an established operational model, maintaining acceptable risk levels through adherence to SLAs and critical process validation checks.

(NIST SP 800-137, Sections 2.2 and 3.3)

Operationalize internal controls and real time continuous monitoring to assist with mitigating risk

F *Failure*

M *Mode*

E *Effect*

A *Analysis*

Identify what can go wrong with the process, consider the potential for occurrence, the negative effects that can be realized, and determine ways to mitigate the likelihood.

Control Type

- Prevent
- Detect

Control Frequency

- Automated
- Manual

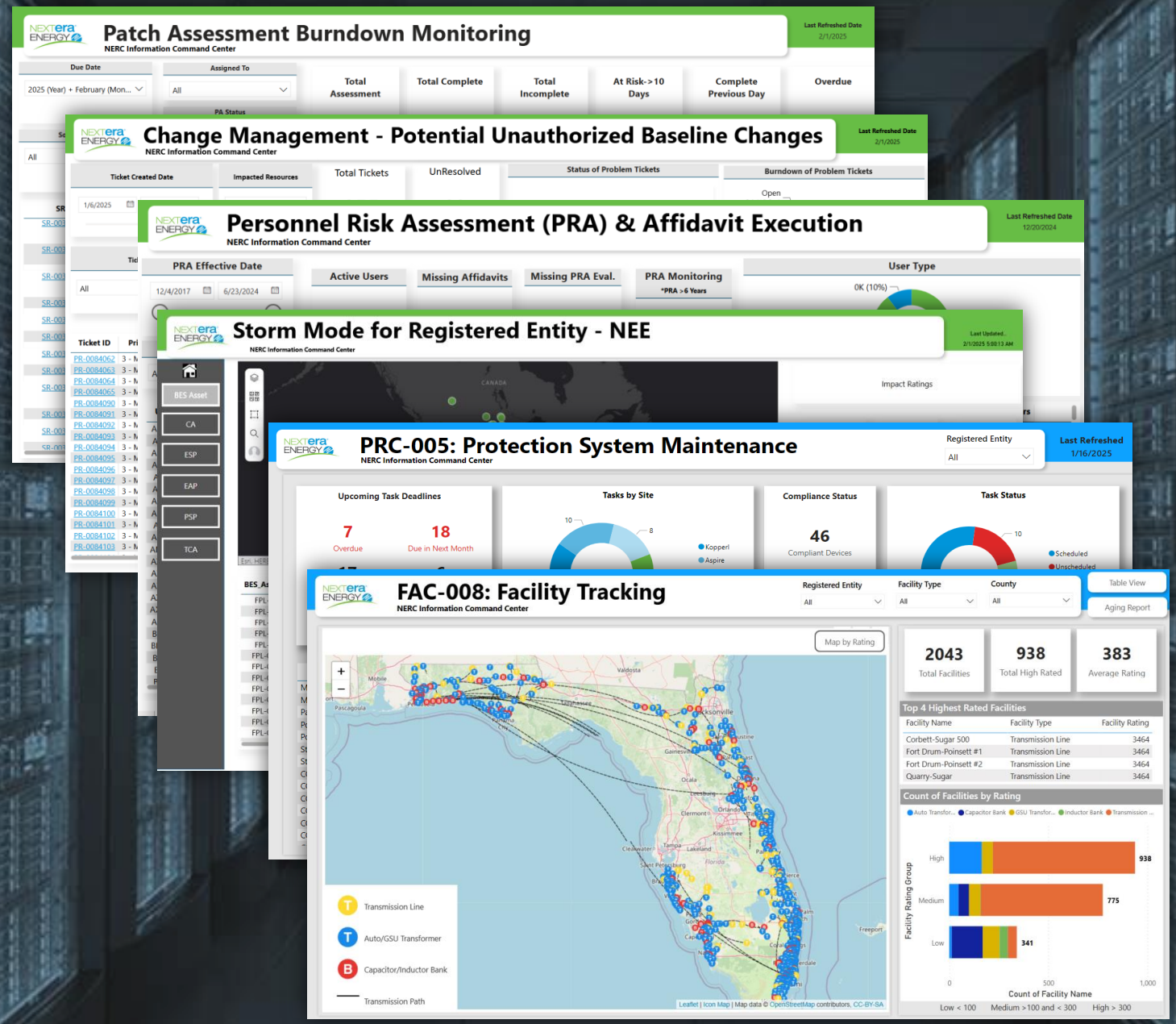
Operational Model

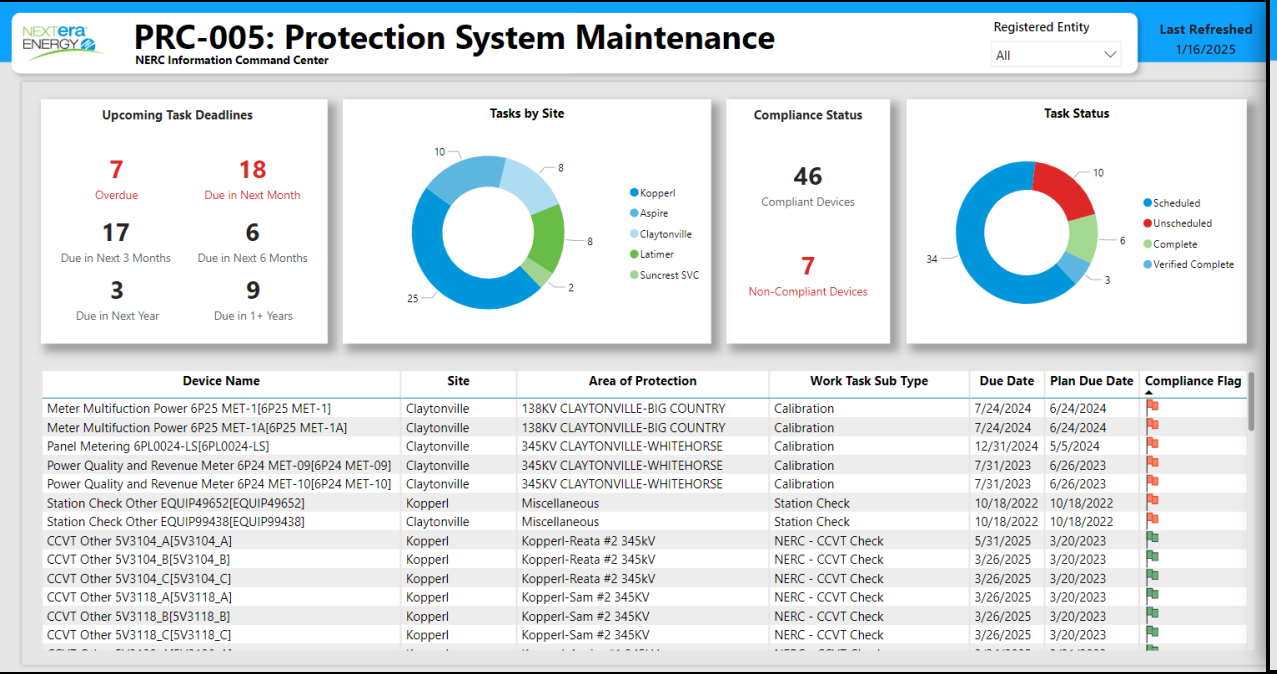
Establish playbooks to respond to off normal conditions identified and determine appropriate SLAs to ensure the process remains in control (as designed).

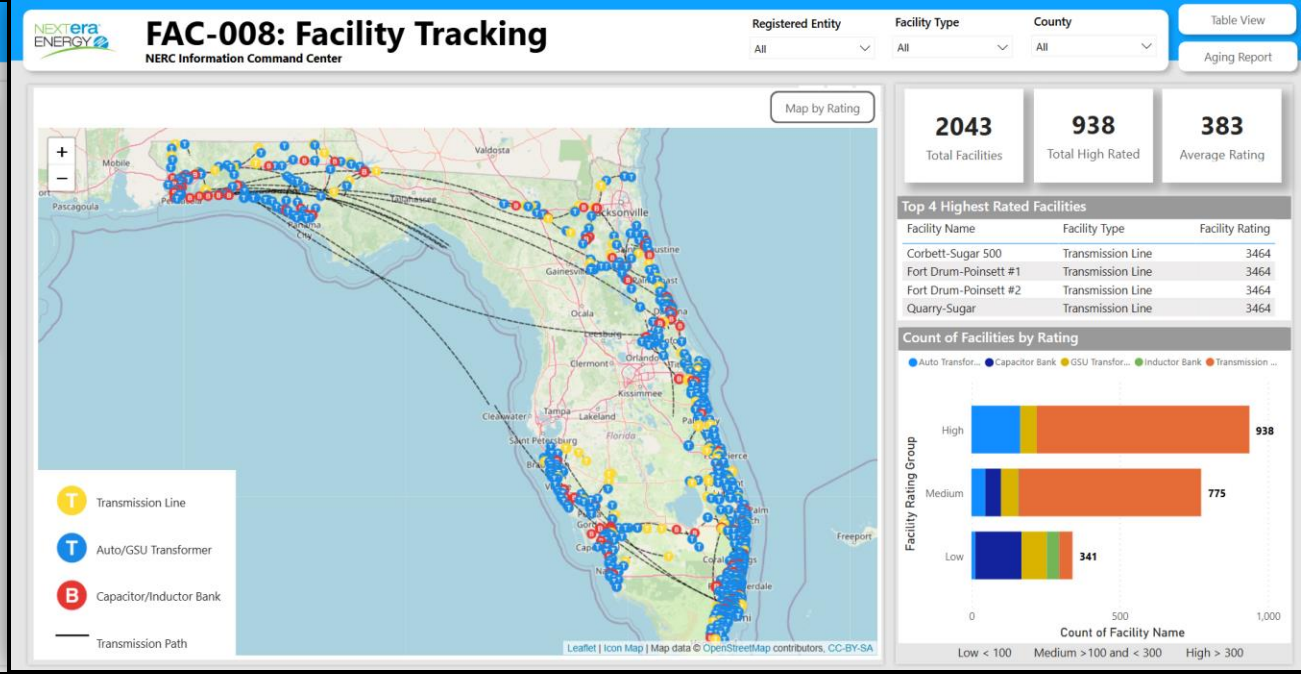
NERC Information Command Center (NICC) is now live as we look to refine continuous monitoring in the Critical Infrastructure Protection (CIP) space

- Real time continuous monitoring and automated information validation
- Enhanced situational awareness and audit support capabilities
- Unified visibility between the activities associated with NERC CIP and NERC O&P compliance obligations
- Reduced risk to the business

We implemented proactive measures to reduce risk tied to our NERC compliance obligations all centered around a safe, secure, reliable grid.







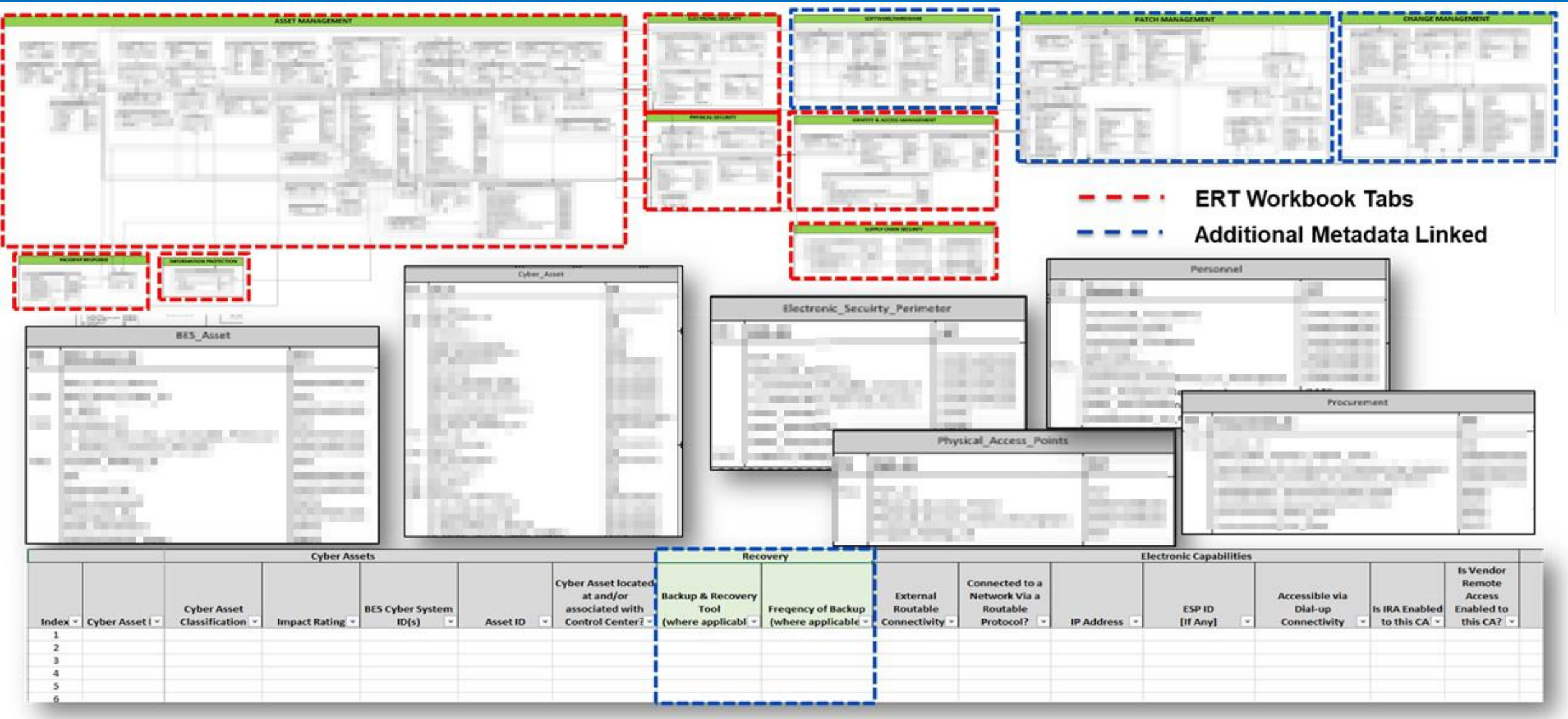
Each visualization will have an associated Operational Model

- Response plan tied to process control limits
- Early indicators of off normal conditions
- Processes to perform information validation

Instructions on pull the data from source systems

- Identification of source systems
- Establish standard on metadata needed
- Steps to extract and load the data

In data rich environment and with standard definition for continuous monitoring, we set out on a journey to build an Information Management system.



NERC Information Command Center (NICC) – Data Warehouse

Source Systems

- Security & Compliance Systems
- Data Management & Storage Systems
- Business Operations Platforms
- Location & Geospatial Systems
- Specialized/Other Systems

ETLs

Extract, Transform, Load

Data Warehouse

Centralized aggregated data hub used for analytics to perform continuous monitoring and audit support services

Extract Transform and Load (ETL) Health

NERC Information Command Center (NICC)

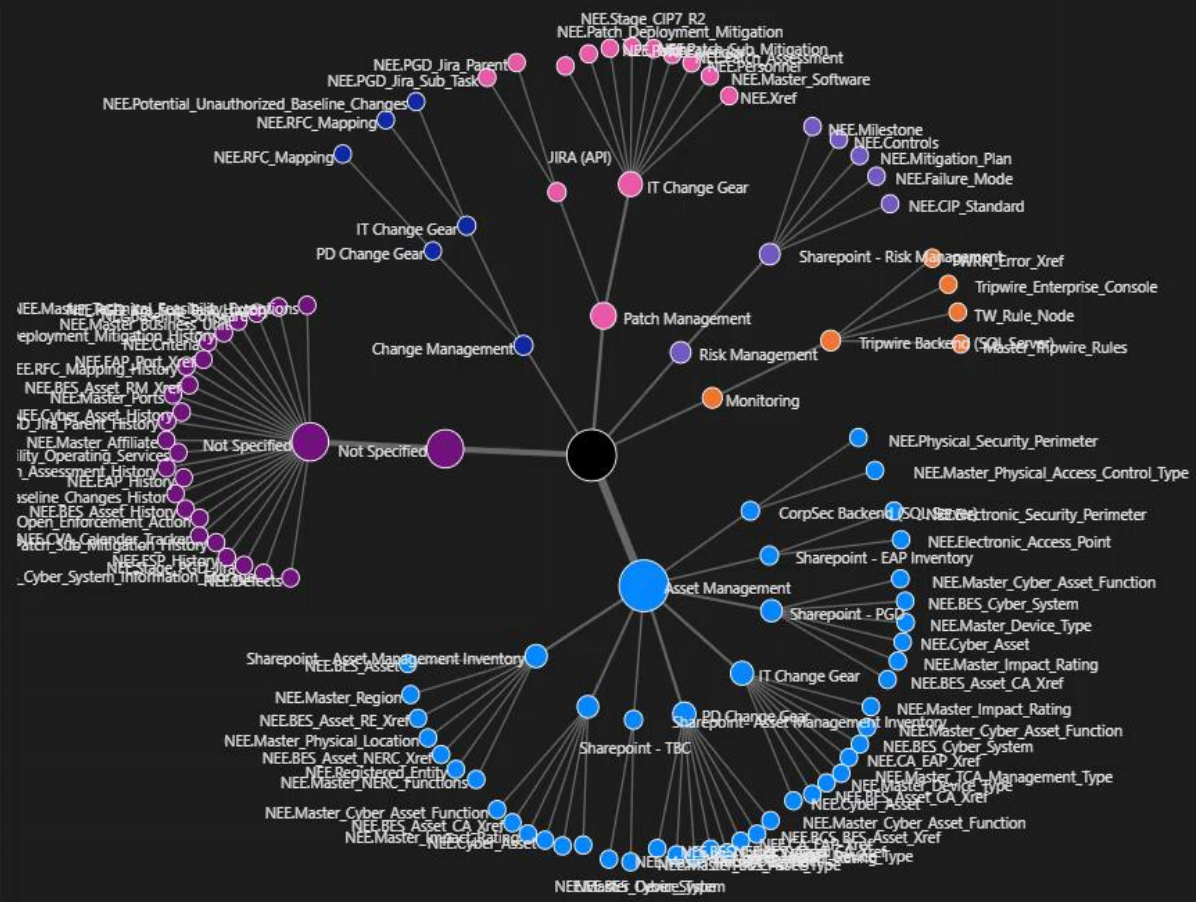
Successful Jobs	Failed Jobs
68	0

March 11, 2025

9:00 AM

Job Status: All | **Domain**: All | **Tool**: All | **Table**: All

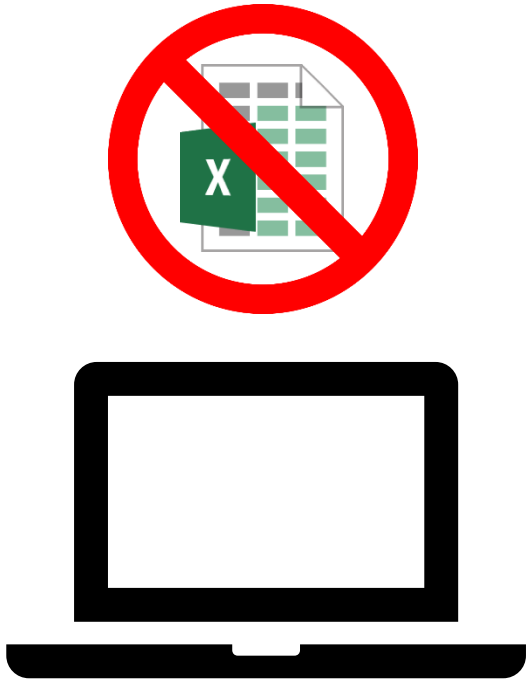
Domain	Tool	Table	Job Status
Asset Management	CorpSec Backend (SQL Server)	NEE.Master_Physical_Access_Control_Type	Success
		NEE.Physical_Security_Perimeter	Success
	IT Change Gear		Success
	PD Change Gear	NEE.BCS_BES_Asset_Xref	Success
		NEE.BES_Asset_CA_Xref	Success
		NEE.BES_Cyber_System	Success
		NEE.CA_EAP_Xref	Success
		NEE.Cyber_Asset	Success
		NEE.Master_Cyber_Asset_Function	Success
		NEE.Master_Device_Type	Success
		NEE.Master_Impact_Rating	Success
	Sharepoint - Asset Management Inventory	NEE.BES_Asset	Success
		NEE.BES_Asset_NERC_Xref	Success
		NEE.BES_Asset_RE_Xref	Success
		NEE.Master_NERC_Functions	Success
		NEE.Master_Physical_Location	Success
		NEE.Master_Region	Success
		NEE.Registered_Entity	Success
	Sharepoint - EAP Inventory	NEE.Electronic_Access_Point	Success
		NEE.Electronic_Security_Perimeter	Success
	Sharepoint - PGD	NEE.BES_Asset_CA_Xref	Success
		NEE.BES_Cyber_System	Success
		NEE.Cyber_Asset	Success
		NEE.Master_Cyber_Asset_Function	Success
		NEE.Master_Device_Type	Success
		NEE.Master_Impact_Rating	Success
	Sharepoint - TBC	NEE.BES_Asset_CA_Xref	Success
		NEE.BES_Cyber_System	Success
		NEE.Cyber_Asset	Success
		NEE.Master_Cyber_Asset_Function	Success



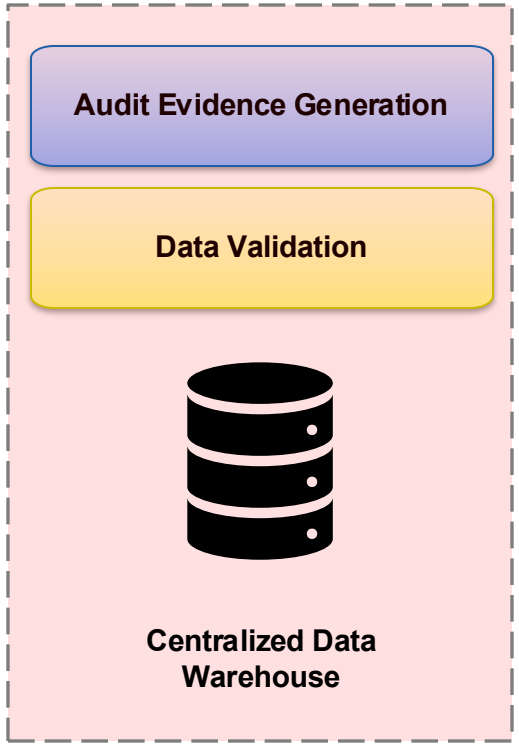
Asset Management

NERC Information Command Center (NICC)

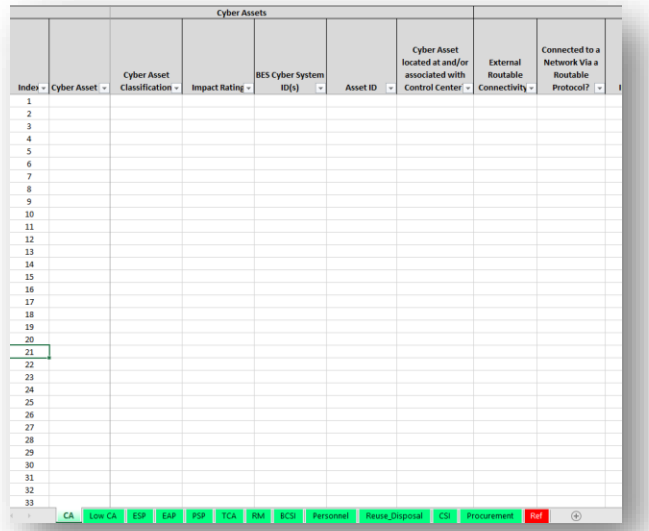
Asset Management – Continuous Monitoring & Audit Support



Asset Management System

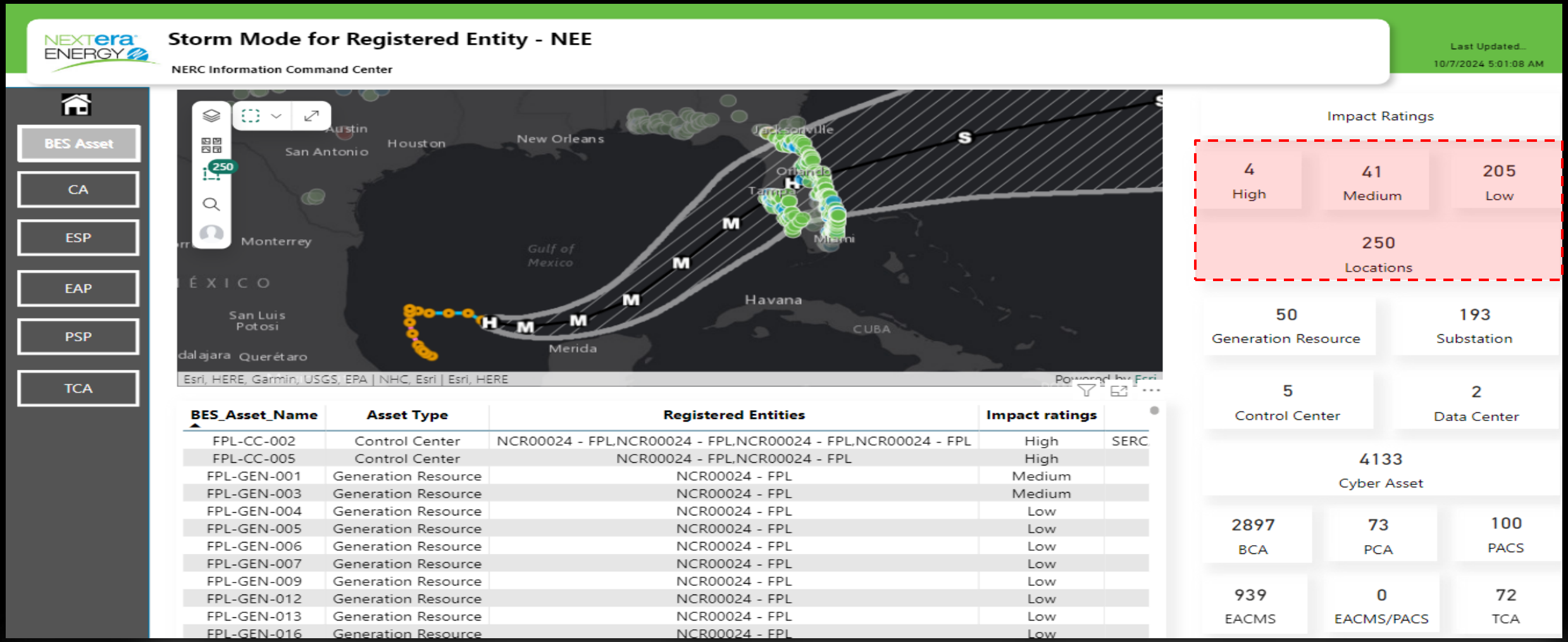


ERT Workbook by RE



NERC Information Command Center (NICC)

Asset Management – Storm Response



BES_Asset_Name	Asset Type	Registered Entities	Impact ratings	
FPL-CC-002	Control Center	NCR00024 - FPL,NCR00024 - FPL,NCR00024 - FPL,NCR00024 - FPL	High	SERC
FPL-CC-005	Control Center	NCR00024 - FPL,NCR00024 - FPL	High	
FPL-GEN-001	Generation Resource	NCR00024 - FPL	Medium	
FPL-GEN-003	Generation Resource	NCR00024 - FPL	Medium	
FPL-GEN-004	Generation Resource	NCR00024 - FPL	Low	
FPL-GEN-005	Generation Resource	NCR00024 - FPL	Low	
FPL-GEN-006	Generation Resource	NCR00024 - FPL	Low	
FPL-GEN-007	Generation Resource	NCR00024 - FPL	Low	
FPL-GEN-009	Generation Resource	NCR00024 - FPL	Low	
FPL-GEN-012	Generation Resource	NCR00024 - FPL	Low	
FPL-GEN-013	Generation Resource	NCR00024 - FPL	Low	
FPL-GEN-016	Generation Resource	NCR00024 - FPL	Low	

- Direct feed from NOAA
- Overlay with CIP002 – Asset Management Data
- Assists with storm response

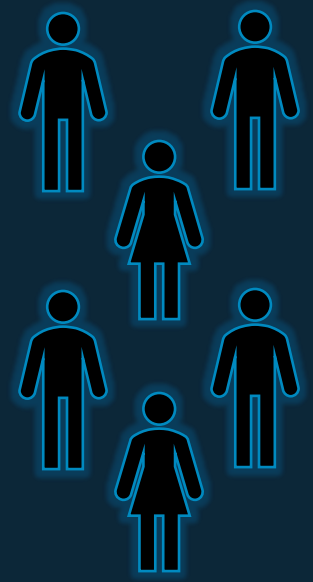
Patch Management

From January 2021 to August 2022, a total of 21 out of 65 samples selected specific to CIP007 R2 – Security Patch Assessments exceeded the 35-day max allowed cycle time by an average of 1-7 days – a 32% Defect Rate!

DMAIC – Define / Measure

Inputs

SMEs



Patch Sources

Applicability Logic Applied

Available

Applicable

Outputs

IT Patch Assessments
Stored in SharePoint

PGD Patch Assessments
Stored in PGD Documentum

Corp Sec Patch Assessments
Stored in CS Documentum

PD Patch Assessments
Stored in PD Documentum

In 2023, we started an 18-month journey that called for the reimagination of our work tied to Security Patch Assessments and Orchestration.

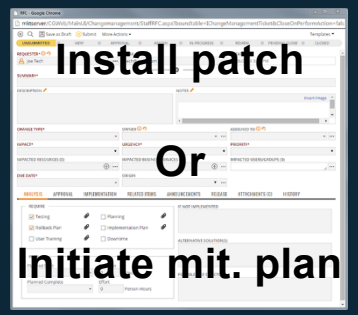
DMAIC – Analyze / Improve

Asset Discovery
Automated (Preferred)
Manual

Centralized Application Database

Software / Applications
Patch Sources
Responsible SMEs

Patch Mgmt. Task Generation / Tracking
Source – Application database
Execution via Change Gear



NERC Information Command Center (NICC)

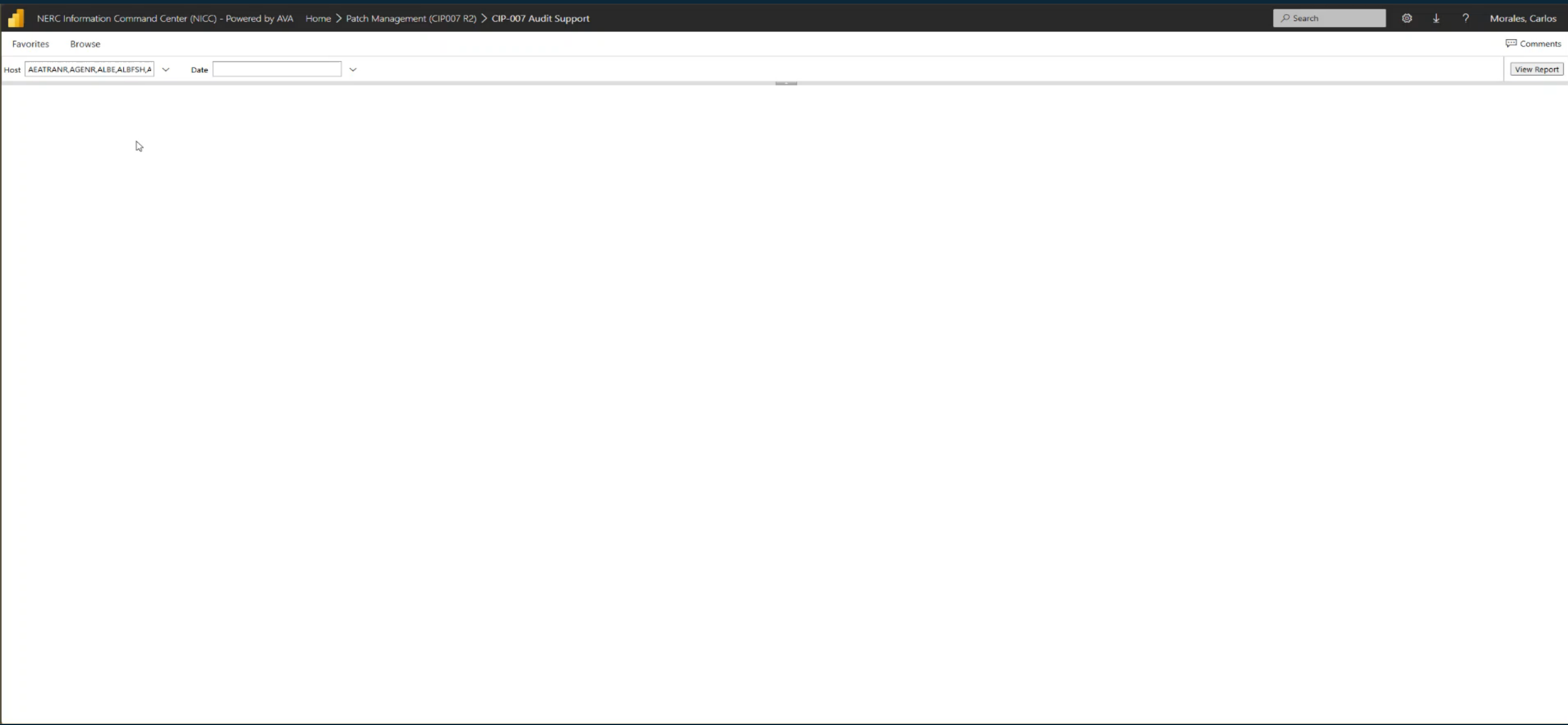
- ✓ Real Time Monitoring
- ✓ Condition Response
- ✓ Trend Analysis
- ✓ Process Execution Evaluation

Our CIP Program is now realizing a 41% decrease in average time to complete patch assessments.

	June 2024 Total Patch Assessments Required to Perform (Opportunities)	June 2024 Total Patch Assessments Completed (Actuals)	June 2024 Average Completion Window	July 2024 Total Patch Assessments Required to Perform (Opportunities)	July 2024 Total Patch Assessments to Complete (Opportunities)	July 2024 Average Completion Window
Information Technology	271	271	**23** Days	255	255	**24** Days
Corporate Security	8	8	**25** Days	11	11	**17** Days
Power Delivery (TSO)	70	70	**23** Days	66	66	**24** Days
Power Delivery (GCS)	134	134	**22** Days	231	231	**21** Days
Power Delivery (PDC)	13	13	**24** Days	13	13	**25** Days
Power Generation	16	16	**25** Days	15	15	**23** Days
Totals	**512**	**512**	**24** **Days**	**591**	**591**	**22** **Days**

NERC requires Patch Assessments to be performed no later than 35 days from the last assessment performed. Historical audit performance also noted that when we realized defects in patch assessment execution, we missed the 35 requirement by an average of 1 and 7 days.

Time to complete NERC's data request tied to patch management went from 6 weeks to 5 days - Over an 80% improvement!



The future of the NERC Information Command Center (NICC) will be powered our AI enabled Advanced Virtual Auditor (AVA).

Real-time cross validation of data using AI generated validation rules generated by the AI-Enabled Virtual Auditor (AVA).

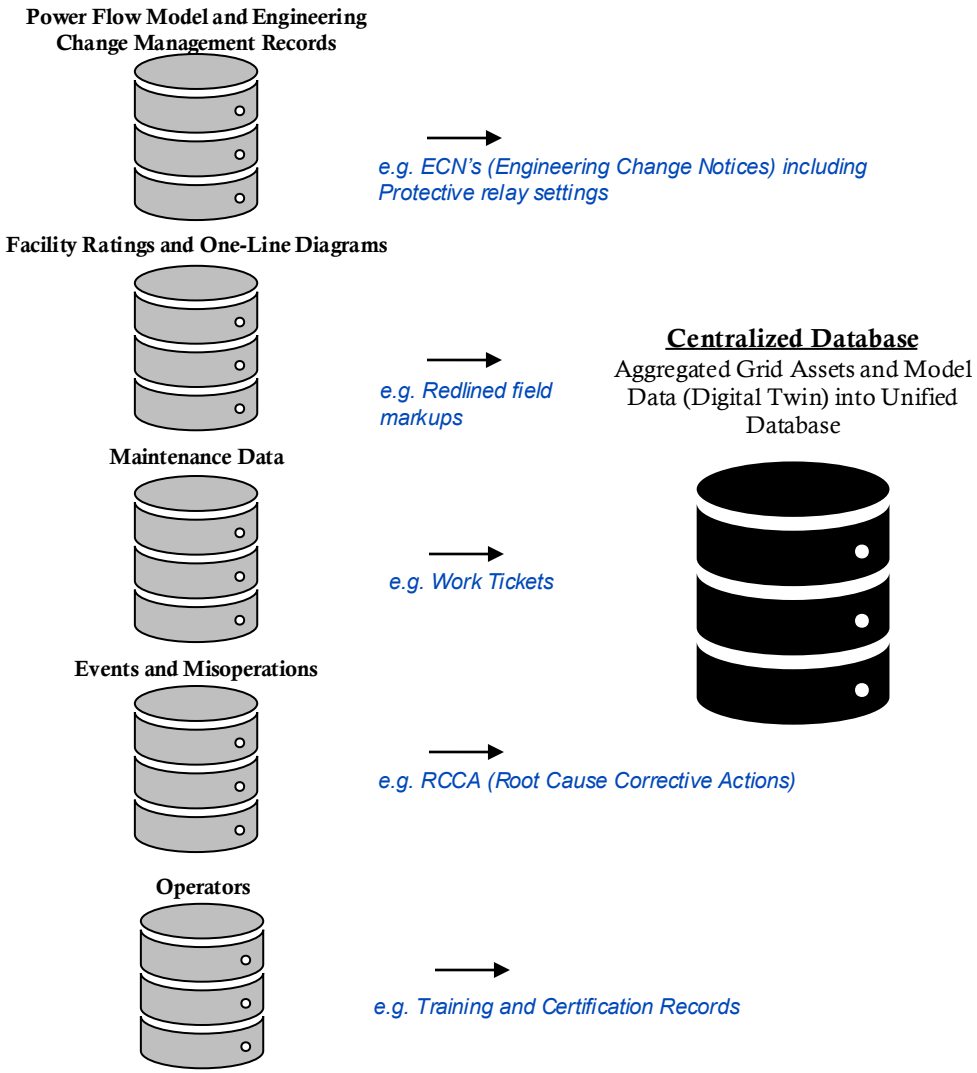
NERC Auditor's "Open Book Test"

NERC Evidence Request Tool (ERT) Workbook

Excel based workbook (blank template) in development at the NERC Regions (Work in Progress)

Examples of meta data requested

1. Power Flow Model Data and Engineering Change Management Records
2. Protective Relays
3. Facility Ratings and One-Line Diagrams
4. Maintenance Data
5. Events and Misoperations
6. Operator Training and Certification



AVA

"Ava please perform the following action…"

* Please validate the meta data associated with the **list of Protective Relays**

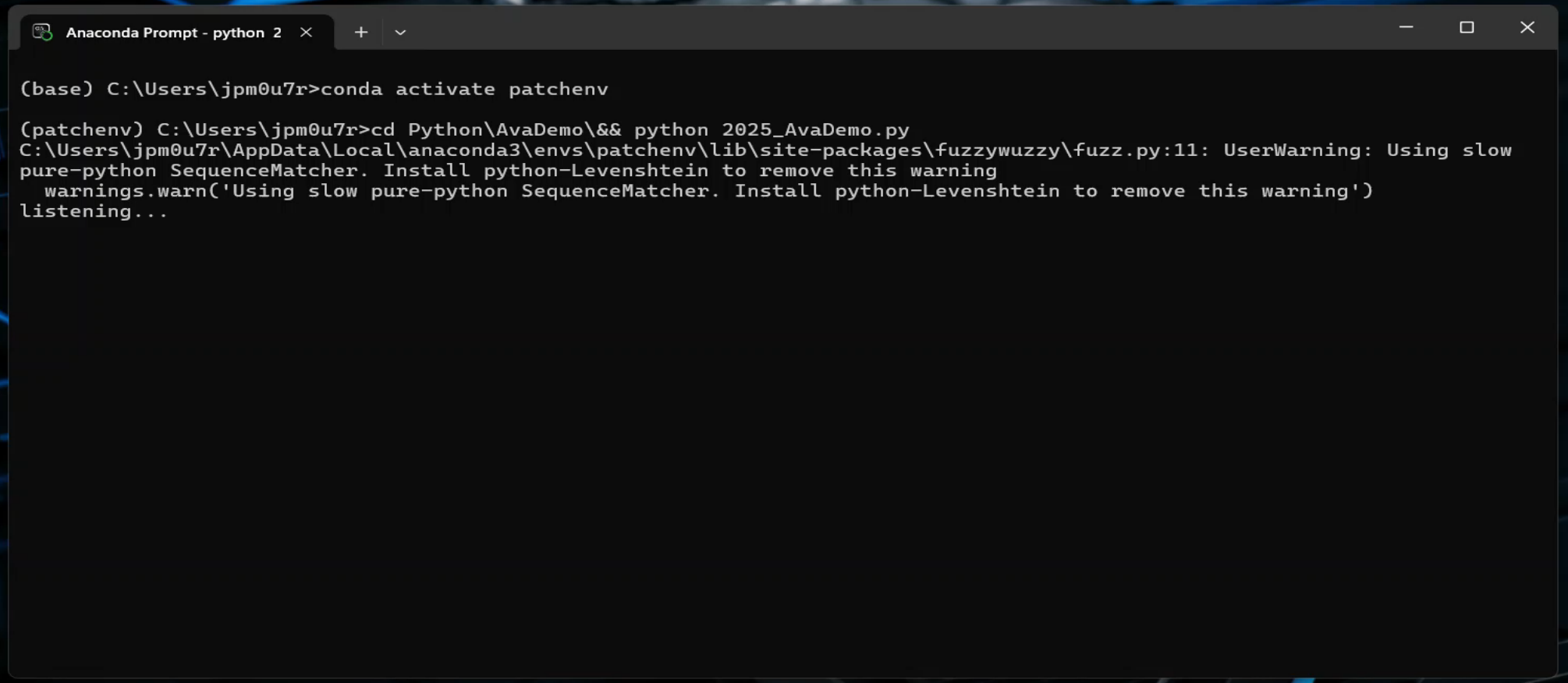
- ❑ Check for consistency between Model and Actual Data ***BAL MOD EOP***
- ❑ Check for correlations between Misops/Events and BES Element Changes ***PRC***
- ❑ Check Facility Ratings against Model Ratings for consistency ***FAC***
- ❑ Check for Relay Setting change timeliness ***PRC***

* Please validate the meta data associated with the **list of Systems that run / protect the BES**

- ❑ Check for missing or outdated Operator Training and Certification Records ***PER***
- ❑ Check for Corrective Actions and Work Ticket timely actions ***MOD FAC***
- ❑ Check for systems with common Root Causes to Misops/Events for possible spread ***PRC***
- ❑ Check for correlations between ECN processes delays and mistakes and model inaccuracies against Misoperations and Events ***MOD***
- ❑ Track the percentage of "Unknown" Root Causes versus population as guide for lurking compliance unknown-unknowns ***PRC***

Use Case (Change Management): We are required by NERC to maintain / produce a complete & accurate BES Element Inventory. Today, the inventory (and associated meta data) is collected by different lines of business and aggregated into a unified platform. From there, we (humans) perform data validations against specific criteria and identify off normal conditions in the data set that need to be investigated. We plan on teaching AVA to perform these validations more frequently and add to the list of validation criteria as needed.

AVA generates & validates the ERT Workbook required for all NERC CIP Audits along with detecting off normal conditions tied task execution!



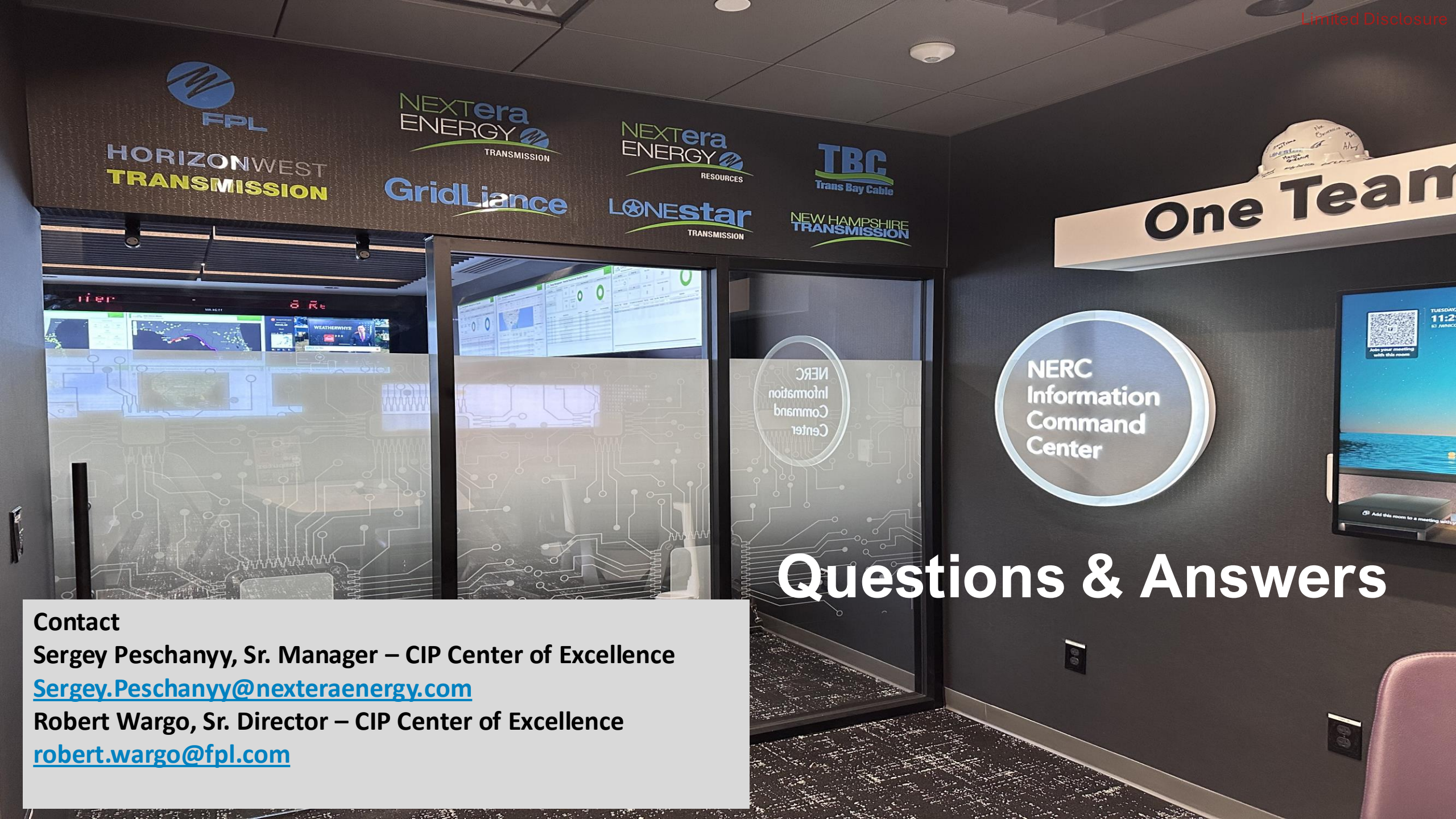
NICC 2.0 is coming! We are expanding the existing space to realize our vision of a unified NERC Information Command Center to include both CIP and O&P compliance obligations.

NERC Information Command Center (NICC) Continuous Monitoring Key

1	**Automated and Verified Systems:** CM involves automated systems that continuously monitor threats, vulnerabilities, and compliance status, ensuring that the collection of data is accurate, complete and up-to-date (NIST SP 800-137, Section 3.1.2).
2	**Timely Awareness:** The system provides timely notifications about potential issues, allowing prompt responses to threats and vulnerabilities and potential compliance issues (NIST SP 800-137, Section 2.3.2).
3	**Real-time Compliance Validation:** The CM system validates compliance in real-time, ensuring that the organization meets regulatory and internal standards consistently and is in continuous audit readiness with fully documented evidence sets generated at task completion (NIST SP 800-137, Section 3.1.3).
4	**Complete Data Acquisition:** A comprehensive data set is gathered, assembled, and contextualized to inform monitoring efforts. This ensures that all relevant information is available for analysis (NIST SP 800-137, Section 3.1.4).
5	**Frequent Data Validation:** Data is validated frequently to maintain continuous compliance and to provide early detection of emerging issues, thereby allowing for corrective action before any non-compliance or risk becomes significant (NIST SP 800-137, Section 3.1.5).
6	**Proactive Auditing:** CM enables both internal and external auditors to perform continuous and proactive auditing, using real-time data to test and validate controls more frequently, including the use of an AI Virtual Auditor (AVA) (NIST SP 800-137, Section 3.2.4).
7	**Informed Decision Making:** The system supports both automated decision-making (through business rules) and complex decision-making requiring human intervention. This leads to timely and informed responses to potential issues (NIST SP 800-137, Section 2.2).
8	**Risk Management:** CM helps maintain an acceptable risk appetite for the organization by ensuring that processes adhere to established Service Level Agreements (SLAs), and that validation checks are in place at critical process steps (NIST SP 800-137, Section 3.3).
9	**Regulatory Cost:** Compliance Program Cost Tracking/Long Term Cost Savings / Continuous Improvement

The NICC *Powered by AVA*

Product Module Offerings



Questions & Answers

Contact
Sergey Peschanyy, Sr. Manager – CIP Center of Excellence
Sergey.Peschanyy@nexteraenergy.com
Robert Wargo, Sr. Director – CIP Center of Excellence
robert.wargo@fpl.com


NEXTera®
ENERGY

FORWARD TOGETHER RELIABILITYFIRST

ASK QUESTIONS TO PRESENTERS USING SLIDO

Join the conversation at SLIDO.com

#RFSummit25

FORWARD TOGETHER RELIABILITYFIRST

BREAK TIME

15 minutes

FORWARD TOGETHER RELIABILITYFIRST

RF ENFORCEMENT AND COMPLIANCE UPDATES

Elizabeth Arora

Senior Counsel, Legal and Enforcement, ReliabilityFirst

Mallory Carlone

Manager, Operations and Planning, ReliabilityFirst

RELIABILITY FIRST

FORWARD TOGETHER RELIABILITYFIRST

2025 ENFORCEMENT UPDATE

Elizabeth Arora, Senior Enforcement Counsel

September 9, 2025

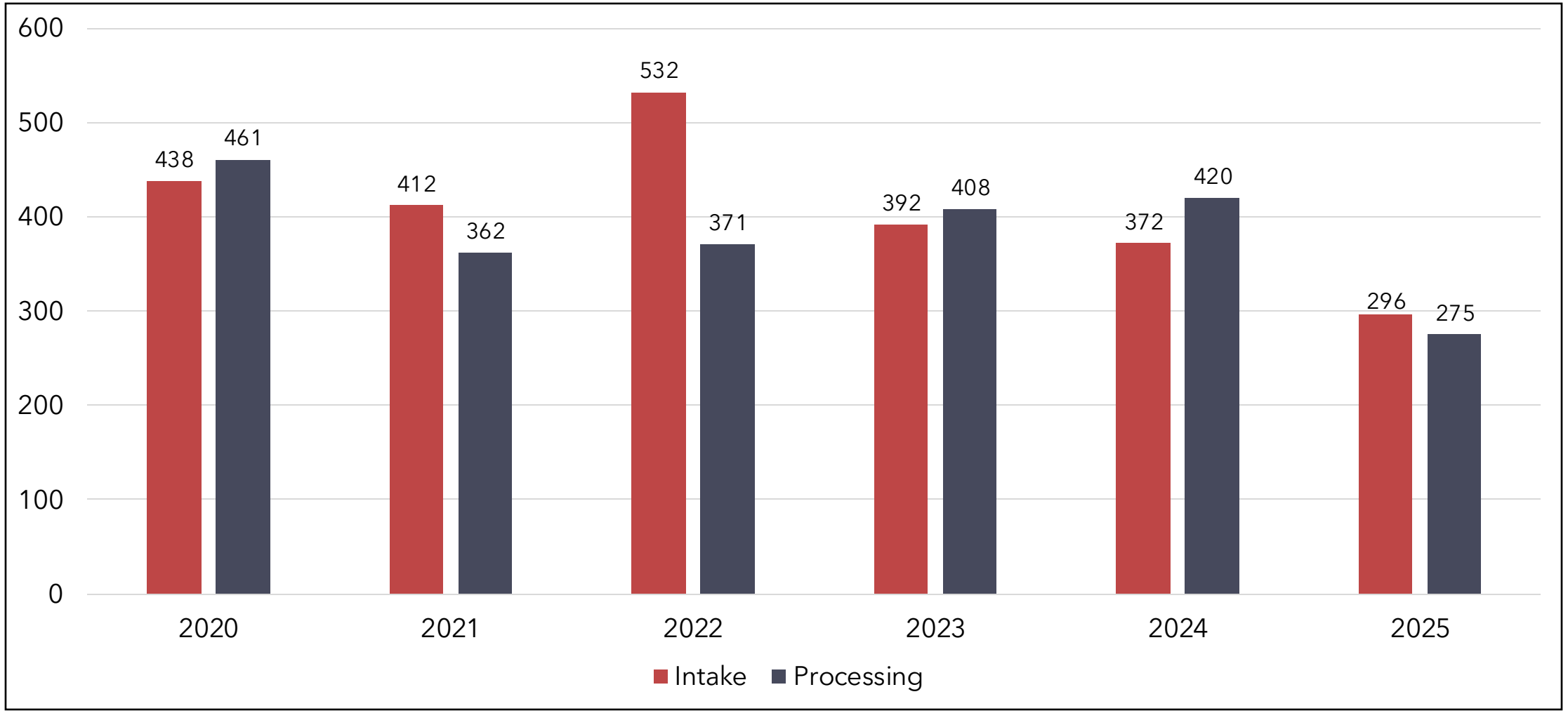
RELIABILITY FIRST

FORWARD TOGETHER RELIABILITYFIRST

ROADMAP

- ANNUAL VIOLATION INTAKE & PROCESSING
- INTAKE COMMENTARY
- OPEN INVENTORY
- DISPOSITION PROCESSING TIMELINES & PRIORITIES
- GENERAL DISCUSSION

RF ANNUAL INTAKE AND PROCESSING

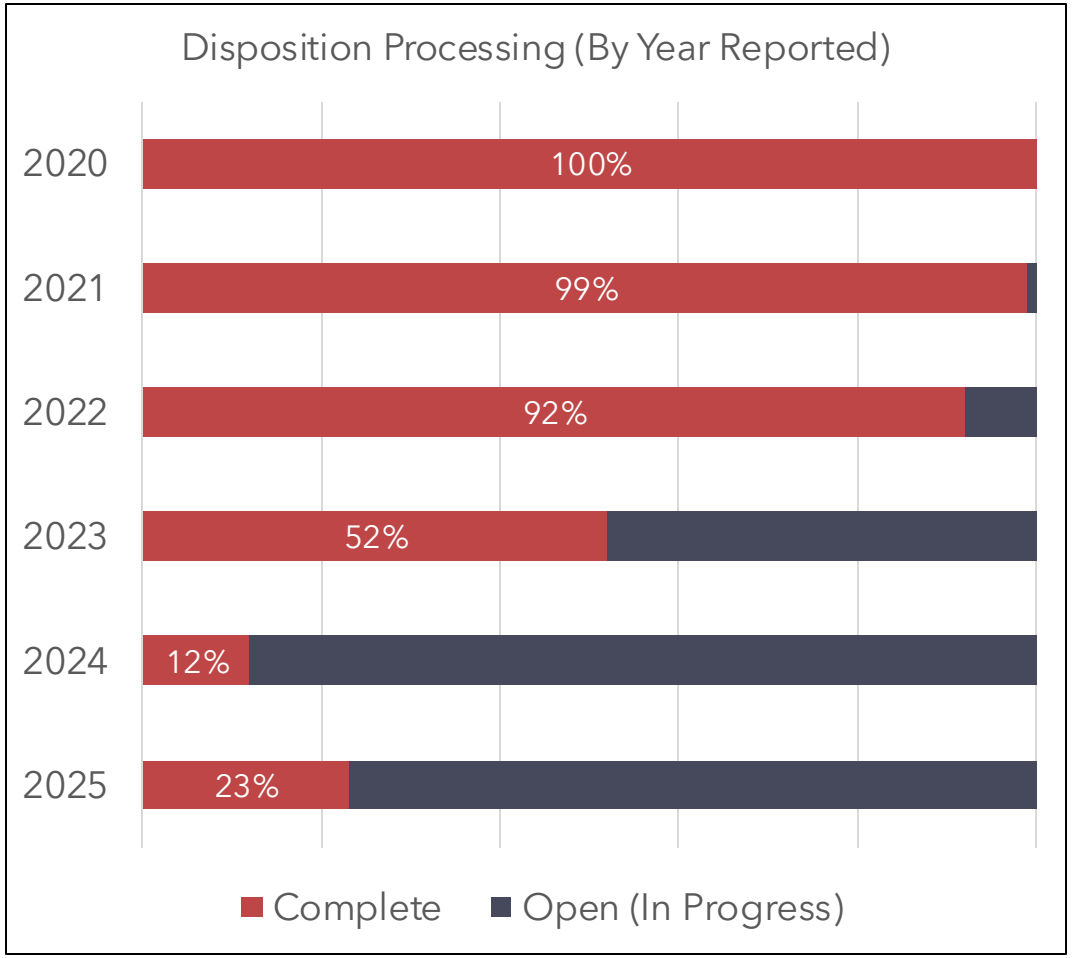


Intake Commentary

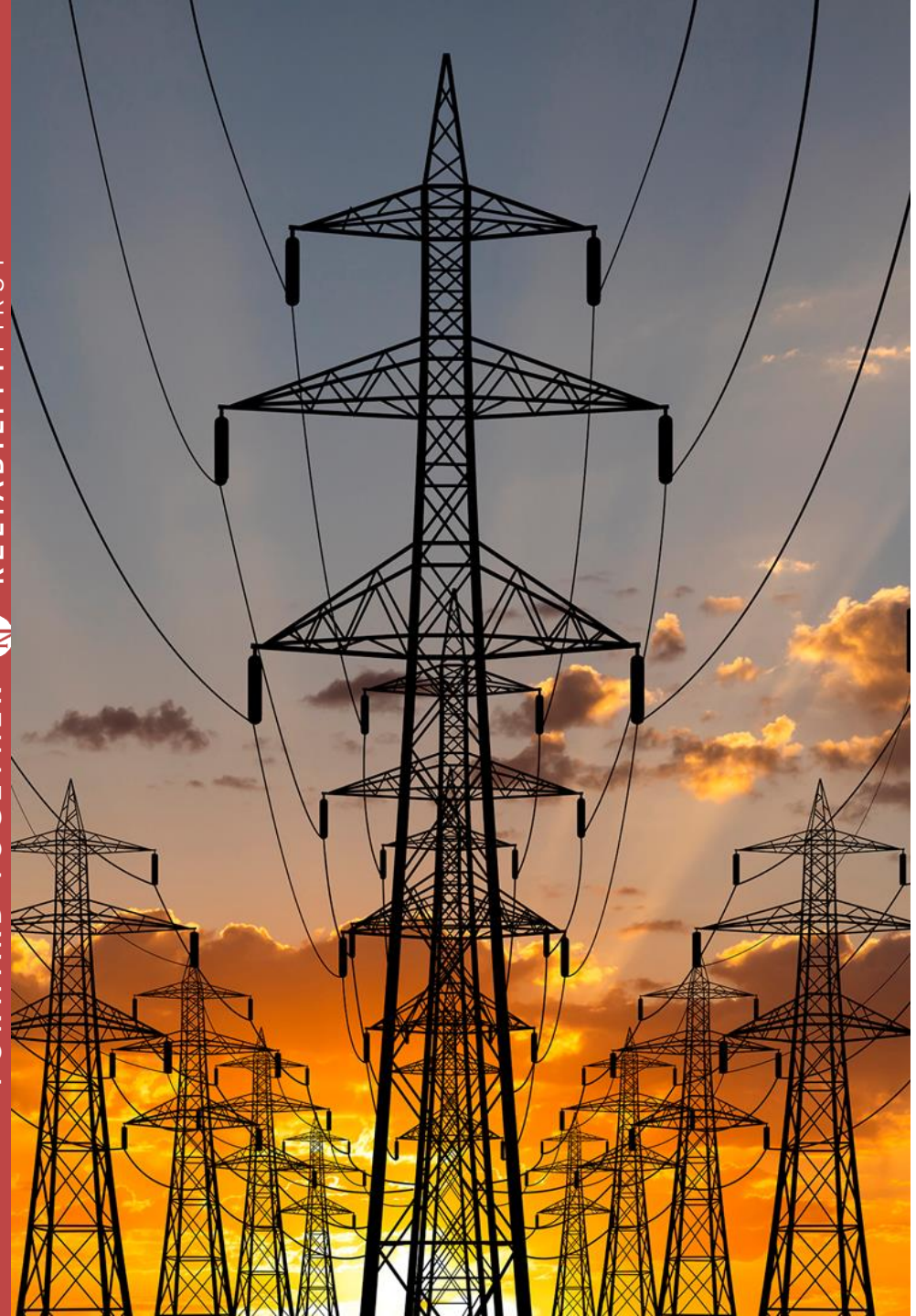
Standard and Requirement	Summary of Requirement	Intake Volume	Examples of Issues/Comments
CIP-004-7 R5	Access revocation	17	• Delinquent revocation of physical and electronic access for employees and contractors
CIP-003-8 R2	Security Management Controls (Low Impact Bulk Electric System Cyber Systems)	17	• Most instances focus on Cyber Security Incident Response Plans (CSIRP), including plan adequacy and plan testing
CIP-007-6 R2	Security patch management	16	• Instances reflect failures to identify patch sources, untimely patch evaluation, and untimely patch applications
FAC-008-5 R6	Establish Facility Ratings consistent with Facility Ratings methodology	6	• Facility Rating accuracy is critical to modeling, analysis, planning, operations, and relaying, and Facility Ratings continue to be an area of focus

RF VIOLATION INVENTORY

Inventory by Year		
2020 & Earlier	0	0%
2021	4	<1%
2022	40	5%
2023	189	24%
2024	327	42%
2025	227	29%
	787	100%



FORWARD TOGETHER RELIABILITYFIRST



DISPOSITION PROCESSING TIMELINES

OBJECTIVES:

- CLOSE LOW RISK/PRIORITY CASES WITHIN MONTHS OF RECEIPT
- ASSIST IN RISK-BASED ALLOCATION OF ENFORCEMENT RESOURCES
- ASSIST IN REDUCING INVENTORY
- PROVIDE REGISTERED ENTITIES WITH REGULATORY CLARITY AND CERTAINTY ON A DESIRABLE AND ACTIONABLE TIMELINE

WHAT RF NEEDS FROM REGISTERED ENTITIES:

- QUALITY SELF-REPORTS
- TIMELY SUBMISSION OF MITIGATION
  - NERC Registered Entity Self-Report and Mitigation Plan User Guide
  - Enforcement Explained: Self-reporting credit and disposition efficiency

DISPOSITION PROCESSING PRIORITIES

Significant or programmatic misses at smaller entities	• 2024 CIP Themes Report
Performance drift in physical security programs	
Facility Ratings	• ERO Enterprise Themes and Best Practices for Sustaining Accurate Facility Ratings
Protection and control	• PRC-005-6 Maintenance Tables • Enforcement Explained: Protecting the grid in normal and abnormal conditions using the Generation Protection Standards
Voltage control and reactive support	• Enforcement Explained: A Concerning Trend in VAR-002-4.1 R1 and R3
Vegetation management	• Enforcement Explained: Trends in vegetation management

FORWARD TOGETHER RELIABILITYFIRST

GENERAL DISCUSSION

elizabeth.arora@rfirst.org

FORWARD TOGETHER RELIABILITYFIRST

ASK QUESTIONS TO PRESENTERS USING SLIDO

Join the conversation at SLIDO.com

#RFSummit25

FORWARD TOGETHER RELIABILITYFIRST

COMPLIANCE MONITORING

Mallory Carlone, Manager, Operations and Planning

September 9, 2025

RELIABILITY FIRST

FORWARD TOGETHER RELIABILITYFIRST

DISCUSSION POINTS

SCHEDULING

SCOPING

DETERMINATIONS – POSITIVE OBSERVATIONS

FORWARD TOGETHER RELIABILITYFIRST

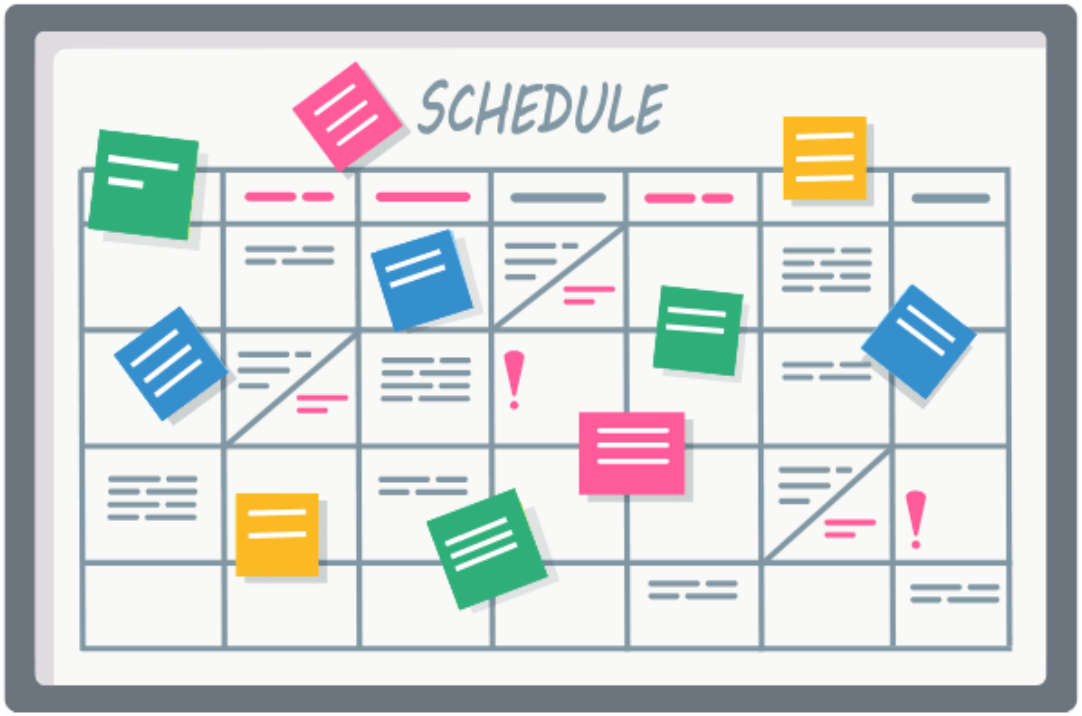
SCHEDULE CREATION

RELIABILITY FIRST

HIGH LEVEL RISK BASED OVERSIGHT

RISK BASED SCHEDULING

- Items for consideration
  - RoP Requirement
  - Compliance Oversight Plans
  - Prior Year Schedule Changes
  - Emerging Industry Risks
  - Previous Engagement Performance
  - CMEP Implementation Plan
  - Etc.



FORWARD TOGETHER RELIABILITYFIRST

SCOPE CREATION

RELIABILITY FIRST

IRA/COP PROCESS

ENTITY RISK PROFILE QUESTIONNAIRE

INHERENT RISK ASSESSMENT

COMPLIANCE OVERSIGHT PLAN

INHERENT RISK ASSESSMENT

Risk Factor
Balancing Authority (BA) Coordination
CIP – External Electronic Communication
CIP - Impact Rating Criteria
CIP – Monitor and Control Capability
Critical Transmission
Largest Generator Facility
Load
Planned Facilities
RAS/SPS
System Restoration
Total Generation Capacity
Transmission Portfolio
UFLS Development and Coordination
UFLS Equipment
UVLS
Variable Generation
Voltage Control
Workforce Capability

Compliance Oversight Plan

Performance Considerations
Compliance History
Events
Internal Controls
Misoperations
Generation
Transmission

Other Considerations
Risk Elements
Emerging Risk
JRO/CRF or other agreements
NERC Alerts

COMPLIANCE OVERSIGHT PLAN

Oversight Strategy			
Category	**Category Description**	**Target Monitoring Interval**	**Primary CMEP Tools**
1	Represents an entity that has higher inherent risk without demonstrated positive performance considerations.	Every 1-3 years	Compliance Audit (on/off-site) Spot Check Self-Certification
2	Represents an entity that has higher inherent risk with demonstrated positive performance considerations.	Every 2-4 years	Compliance Audit (on/off-site) Spot Check Self-Certification
3	Represents an entity that has moderate inherent risk without demonstrated positive performance considerations.	Every 3-5 years	Compliance Audit (on/off-site) Spot Check Self-Certification
4	Represents an entity that has moderate inherent risk with demonstrated positive performance considerations.	Every 4–6 years	Compliance Audit (off-site) Spot Check Self-Certification
5	Represents an entity that has lower inherent risk without demonstrated positive performance considerations.	Every 5-7 years	Compliance Audit (off-site) Spot Check Self-Certification
6	Represents an entity that has lower inherent risk with demonstrated positive performance considerations.	Every 6+ years	Compliance Audit (off-site) Spot Check Self-Certification

Risk Category
Asset/System Identification
Asset/System Management and Maintenance
Asset/System Physical Protection
Emergency Operations Planning
Entity Coordination
Identity Management and Access Control
Long-term Studies/Assessments
Modeling Data
Normal System Operations
Operating During Emergencies/Backup & Recovery
Operational Studies/Assessments
System Protection
Training

SCOPING CONSIDERATIONS

POSITIVE OBSERVATIONS

- Items which the auditors believe are areas where the Registered Entity's performance showed **initiative**, **innovation**, and **exceeded industry norms**, etc.
  - *"The flowchart of modeling carefully lays out transition points…considers checkpoints, questions, handoffs, and some internal controls."*
  - *"The team was very accommodating, transparent, and communicative. Several SME's took part in the discussions and leading the demonstrations."*
  - *"It was apparent that lessons learned (i.e. wind breaks, insulation) and efficiency/safety gains (i.e. drainage) were constantly being evaluated and implemented when possible."*
  - *"The Security Authorization Package (SAP) summary presents the Information Security Risk Management group's overall risk assessment results and recommendations. It offers several key benefits, including enhanced clarity and accessibility, improved decision-making, strengthened accountability, greater time efficiency, and more effective risk management and operational efficiency for the procurement process."*

ENHANCE THE PARTNERSHIP

- Tell your story
- Collaboration and Productive conversation
- Transparency
- Building Trust
- Promote your program's success
- Preparedness/proactive
- Sustainability

2026 INTERNAL CONTROLS WORKSHOP

SAVE THE DATE:
FEB. 23 - 25, 2026

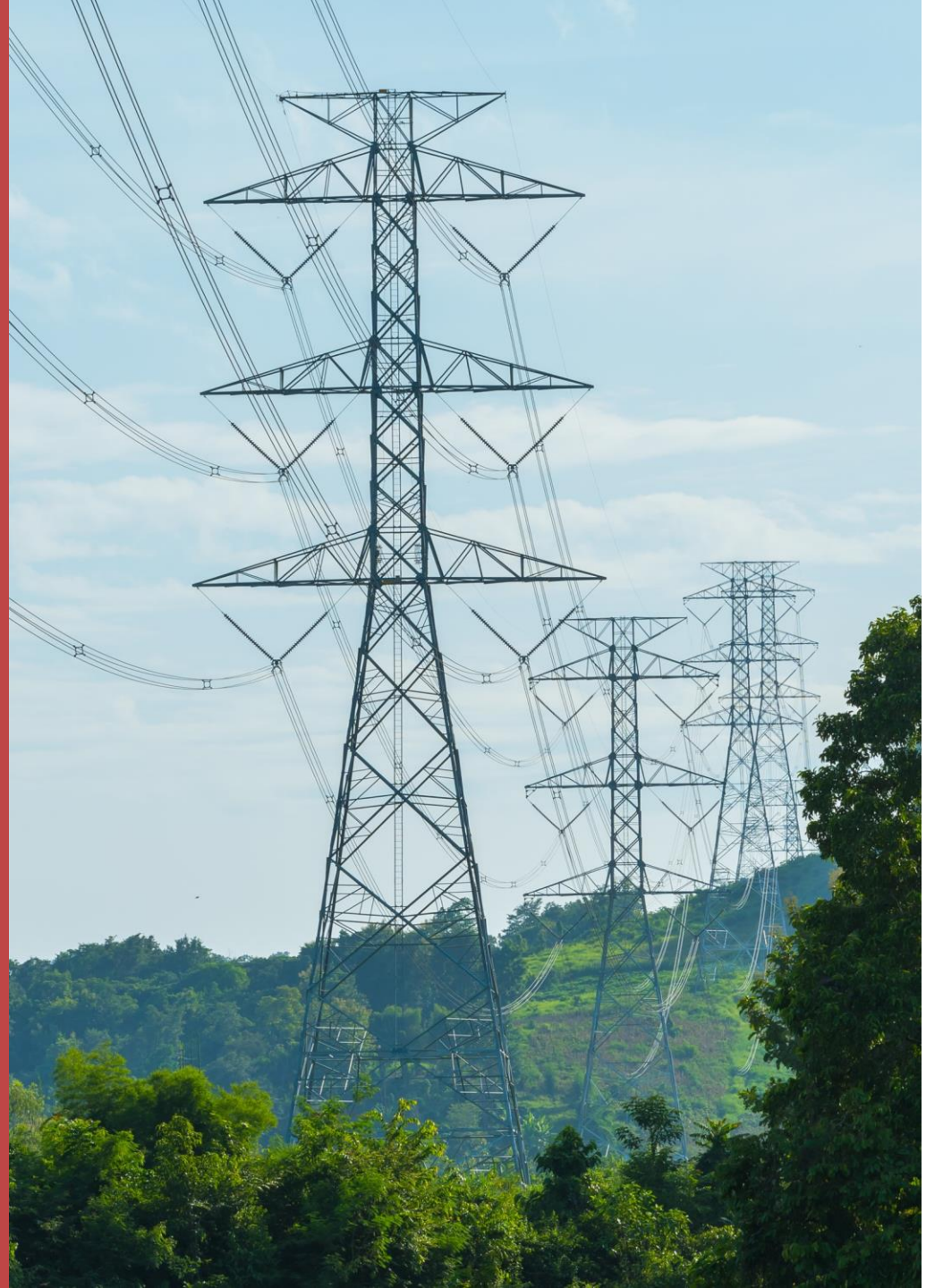
CLEVELAND

Help us, help you! What topics, standards, or questions would you like to cover?

We're inviting RF registered entities to collaborate in shaping the agenda. Share your ideas, challenges, and priorities using the QR code below. Let's build this together!

forms.office.com/r/Kc5ZbUYGVe

FORWARD TOGETHER RELIABILITYFIRST



FORWARD TOGETHER RELIABILITYFIRST

QUESTIONS & ANSWERS

Mallory.Carlone@RFirst.org

AUDIT SCOPE REFERENCE LINKS:

- Risk Factors and Risk Categories
  - https://www.nerc.com/pa/comp/CAOneStopShop/Risk%20Factors%20and%20Risk%20Categories.pdf
- Risk Elements – ERO CMEP Implementation Plan
  - https://www.nerc.com/pa/comp/CAOneStopShop/Risk%20Factors%20and%20Risk%20Categories.pdf
- Standards Under Development
  - https://www.nerc.com/pa/Stand/Pages/Standards-Under-Development.aspx
- Elevated Risks to the BES
  - https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC_Long%20Term%20Reliability%20Assessment_2024.pdf
- Emerging Risks
  - https://www.nerc.com/comm/RISC/Related%20Files%20DL/2025_RISC_ERO_Priorities_Report.pdf

FORWARD TOGETHER RELIABILITYFIRST

ASK QUESTIONS TO PRESENTERS USING SLIDO

Join the conversation at SLIDO.com

#RFSummit25

AGENDA FOR TOMORROW
WEDNESDAY, SEPT. 10

7:30 – 8:30 a.m. **Breakfast**

8:30 a.m. - 12:00 p.m.

Track 1 NERC 101 – Salon A

Topics include: Navigating the NERC and RF websites, RSAWs, what to expect before, during, after audit; RF Tools and Services; Periodic Data Submittals and other xADs data submittals; NERC Alerts, Events Analysis, working with your case manager, and more!

Track 2 Internal Controls Workshop – Salon B

Topics include: Communicating NERC and RF's expectations regarding internal controls reviews (design, testing, monitoring), and hands-on activities for the participants to practice identifying and designing controls for enhanced reliability, security, and resilience

Track 3 Energy Policy Leadership Roundtable Discussion – Salon C

Topics include: The Pace of Change (resource adequacy, essential reliability services, load growth, permitting and siting); Shaping Policy into Solutions (new technologies and innovations, meshing federal/state policies and across state lines); and Protecting the Grid of the Future (cyber and physical security, security partners and preparedness)

FORWARD TOGETHER RELIABILITYFIRST

RELIABILITY FIRST

Internal Controls Workshop
Evening reception: Monday, Feb. 23
Workshop: Tuesday, Feb. 24 - Wednesday, Feb. 25

Expect:
Small group discussions
Sharing industry experiences
Choose your own tracks
Move between topics or dive deep

Women's Leadership Conference
Evening reception: Wednesday, Feb. 25 Conference: Thursday, Feb. 26 Feb. 25

Expect:
Panels focused on professional development, mentorship, empowerment, and insights tailored to the energy sector
Networking opportunities
Professional development resources