

WELCOME TO TECHNICAL TALK WITH RF

May 20, 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 against a sunset sky. 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 a roof being worked on.

TECH TALK REMINDERS

Please keep your information up-to-date

- CORES, Generation Verification Forms, Entity Profile Questionnaires (quarterly)

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](#):

- [2023 ERO Periodic Data Submittal schedule](#)
- Timing of Standard effectiveness

BES Cyber System Categorization (CIP-002-5.1 a)

- 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](#)



WELCOME TO TECHNICAL TALK WITH RF

May 20, 2024



TECH TALK ANNOUNCEMENT

[Register Now](#)



FALL RELIABILITY & SECURITY SUMMIT



SEPT. 16-18, 2024



INDIANAPOLIS



Featuring an energy policy legislator panel with:

Brian Feldman
Maryland State Senator



Stephanie Hansen
Delaware State Senator



Eric Koch
Indiana State Senator



Dick Stein
Ohio State Representative



TECH TALK ANNOUNCEMENT



Multi-Regional IBR Webinar: State & Provincial Integration of Reliable Renewable Energy

Click here for [Registration](#)

May 29

Join us for a webinar where experts from the ERO Enterprise will shed light on proposed amendments to NERC's Rules of Procedures governing the registration criteria for inverter-based resources (IBRs) that would result in materially impactful IBRs becoming subject to NERC's Reliability Standards.



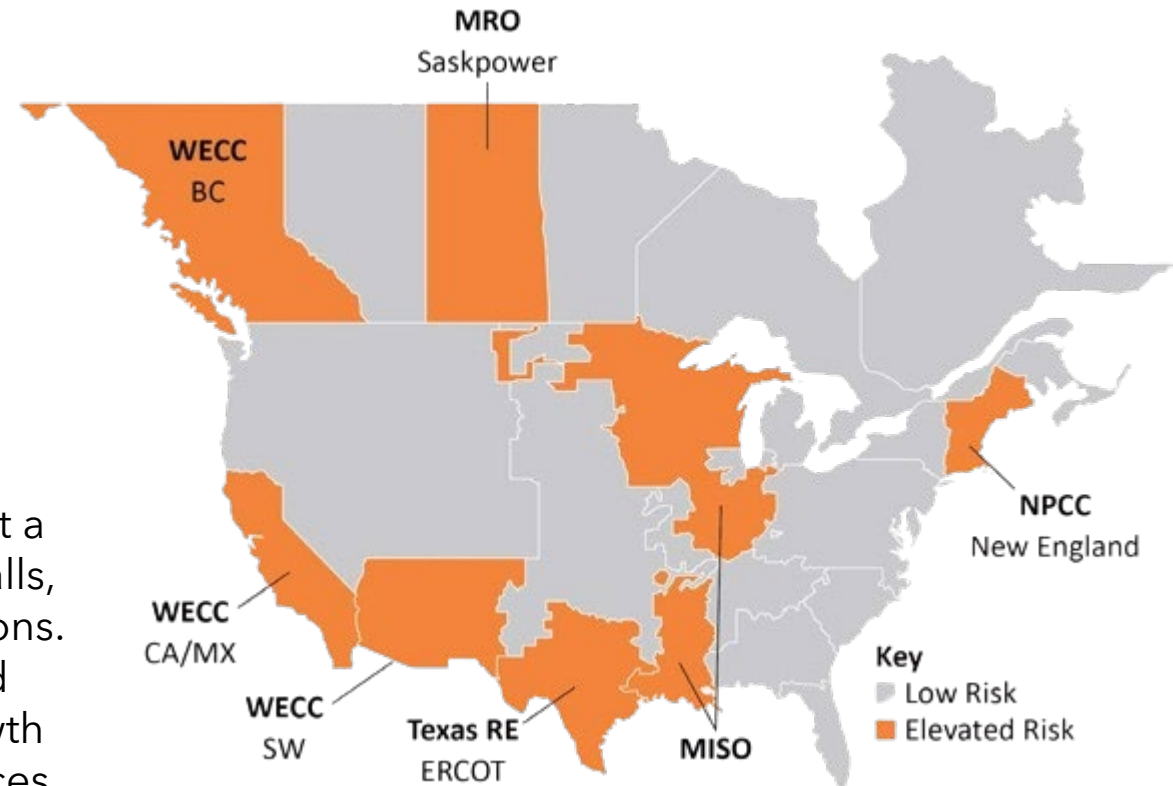
TECH TALK ANNOUNCEMENT



NERC Releases 2024 Summer Reliability Assessment

[Read Full Report](#)

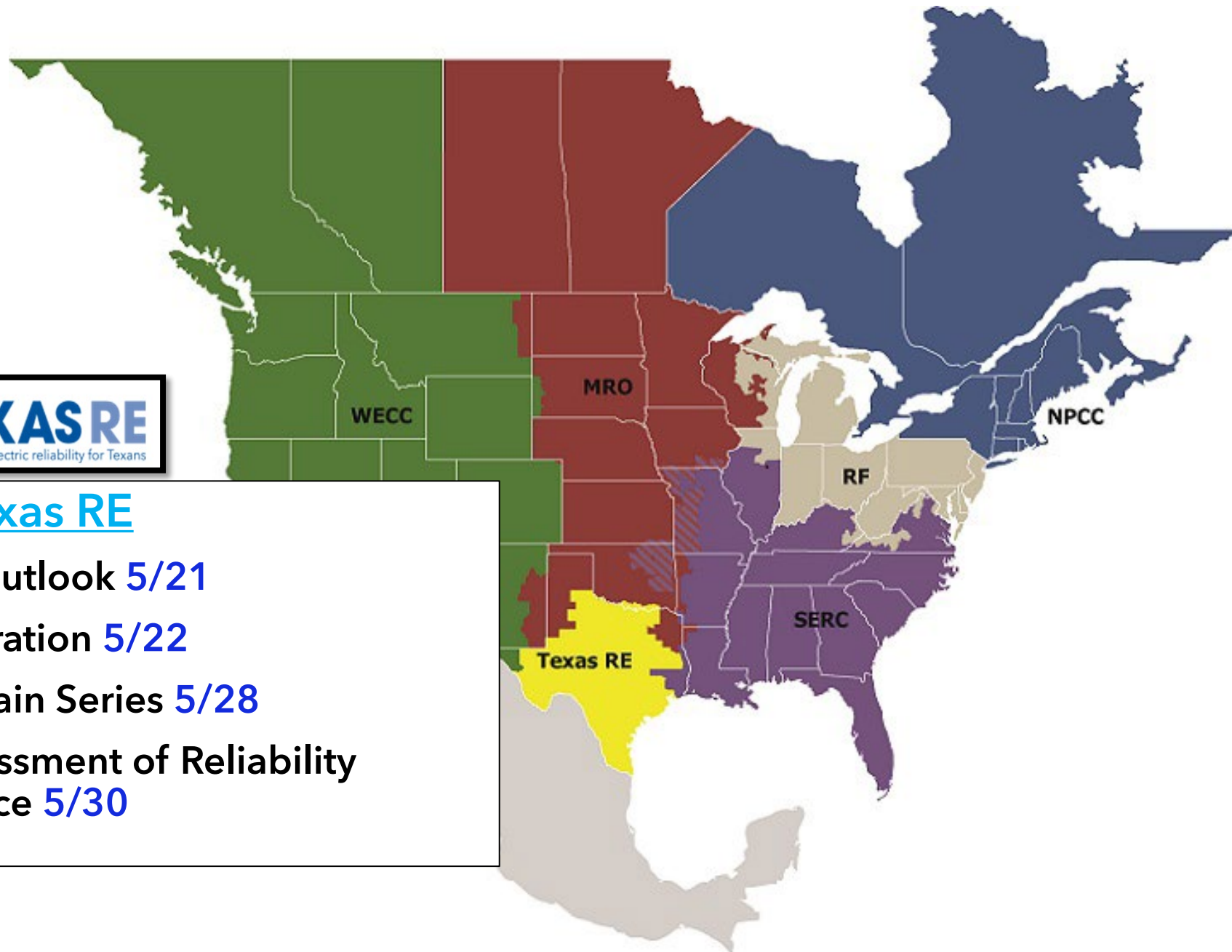
NERC's [2024 Summer Reliability Assessment \(SRA\)](#) finds that a large part of North America remains at risk of supply shortfalls, while other areas show reduced risk due to resource additions. Expected wide-area heat events that affect generation, wind output, or transmission systems coupled with demand growth in some areas are contributing to adequacy risks for resources and transmission. All areas are assessed to have adequate supply for normal peak load due, in large part, to a record 25 GW of additional solar capacity added since last year. However, energy risks are growing in several areas when solar, wind, and hydro output are low.





[Talk with Texas RE](#)

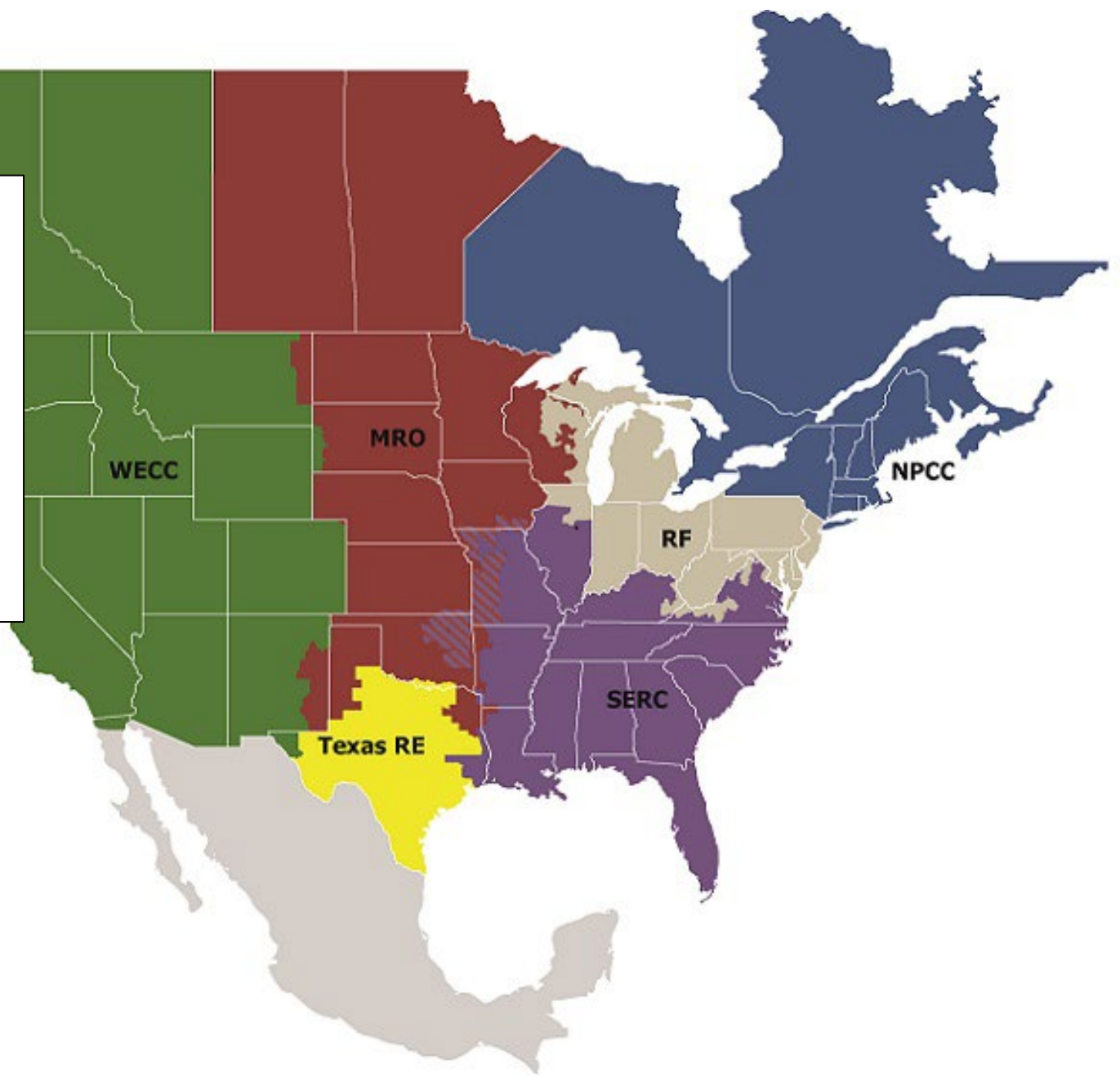
- Summer Outlook [5/21](#)
- IBR Registration [5/22](#)
- Supply Chain Series [5/28](#)
- 2023 Assessment of Reliability Performance [5/30](#)





Monthly Reliability and Security Monthly Webinar

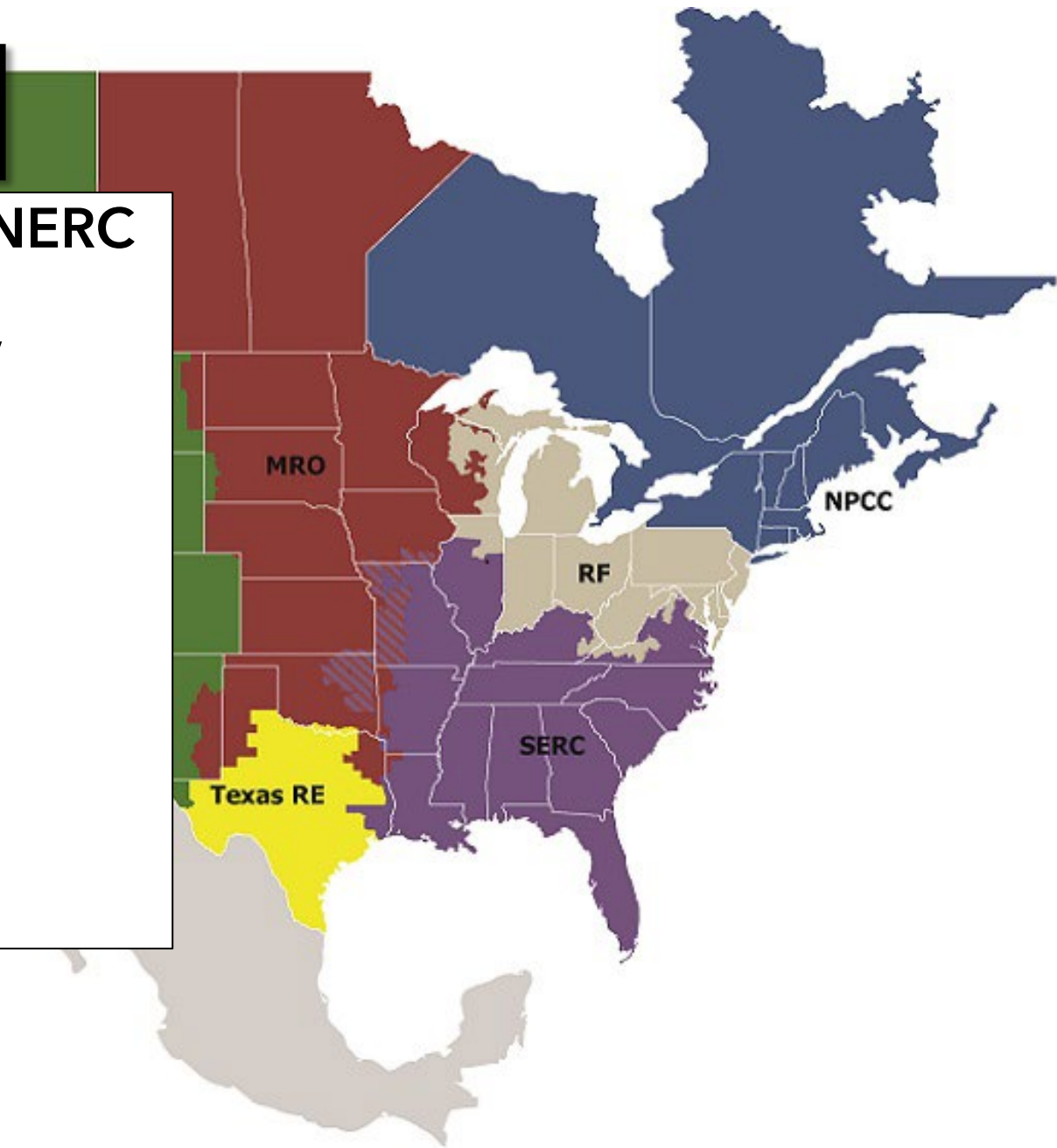
- [June 20](#)

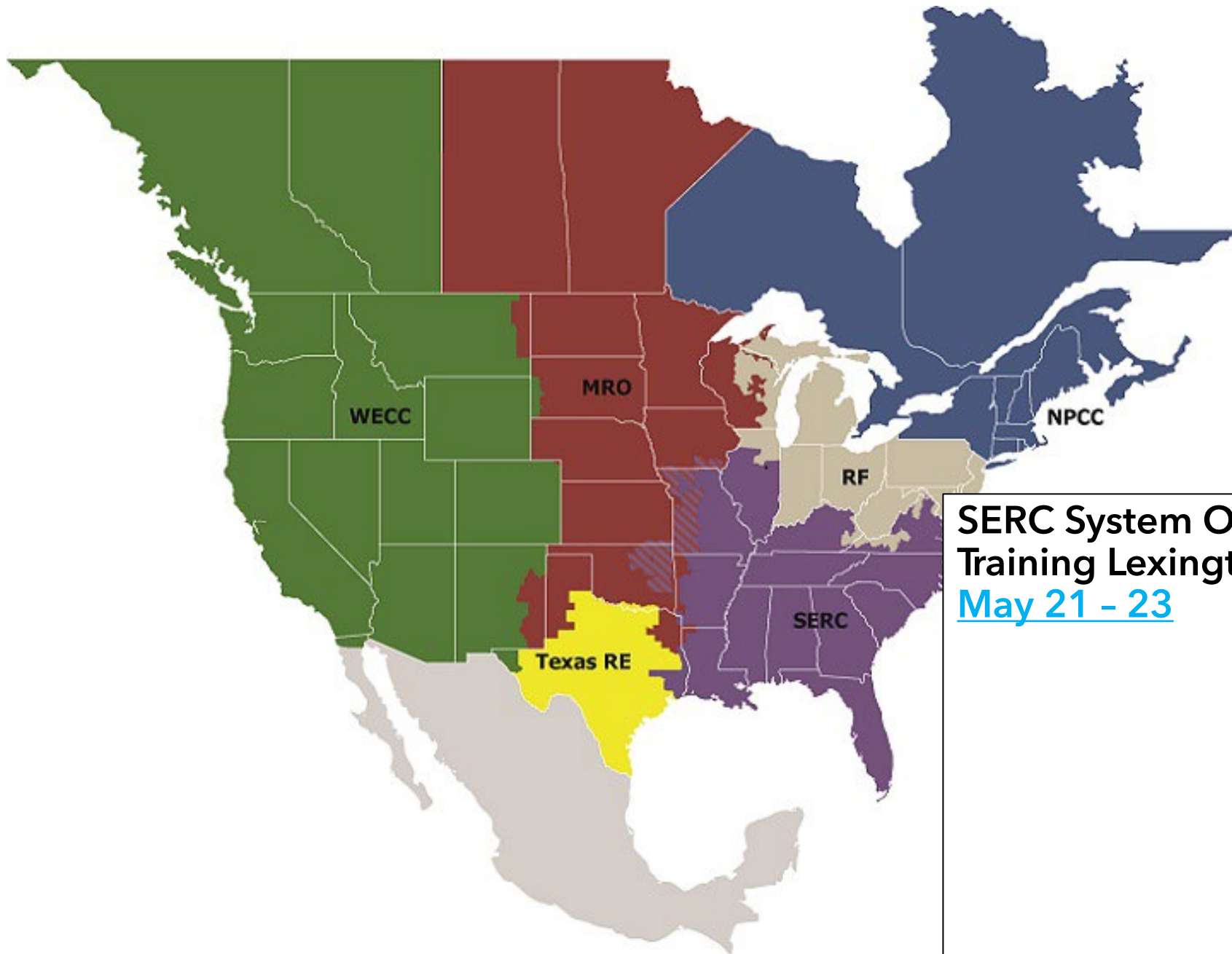




Introduction to the NERC Certification and Certification Review Process Webinar

- [June 4](#)



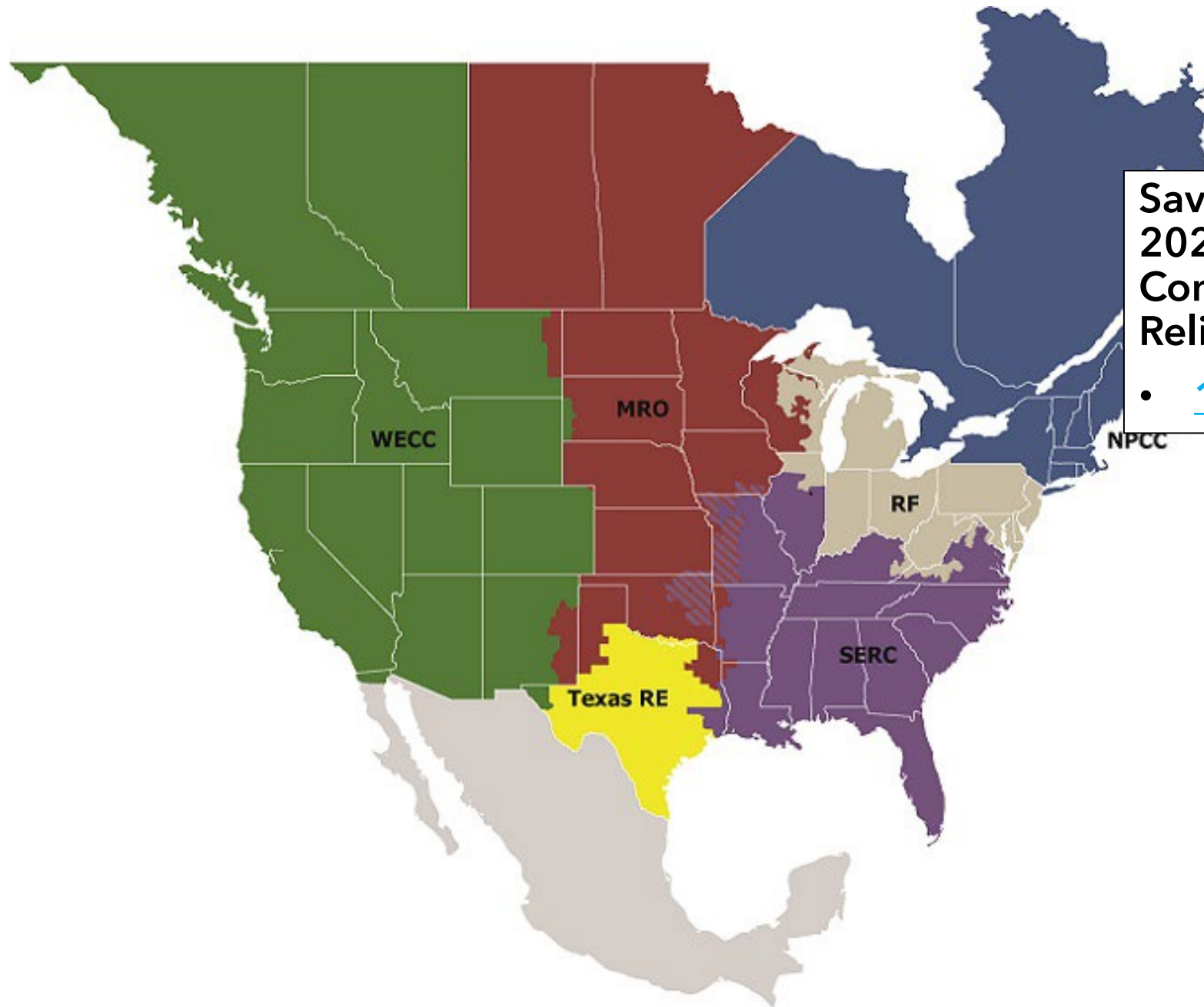


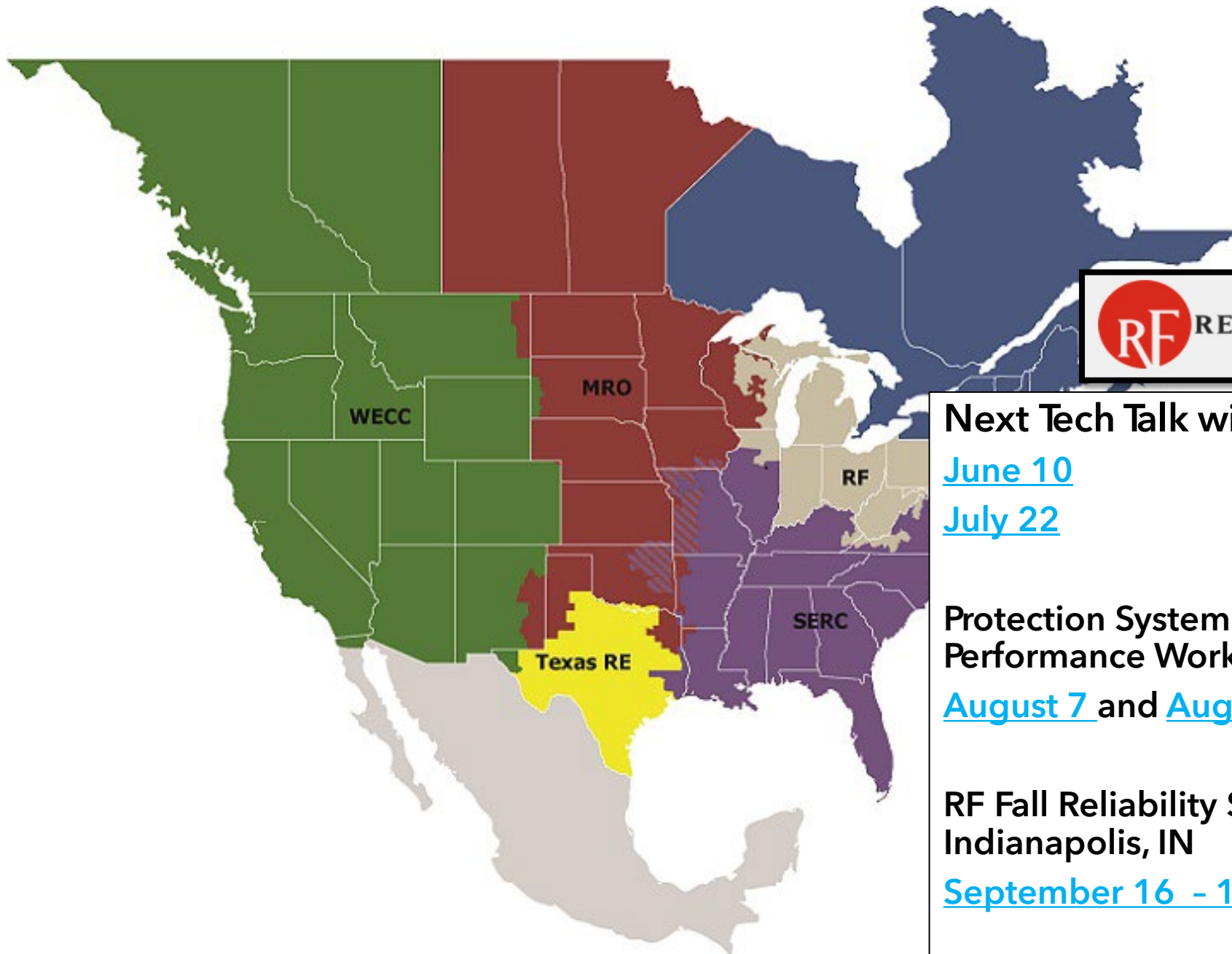
**SERC System Operator
Training Lexington, KY
[May 21 - 23](#)**



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

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





Next Tech Talk with RF

[June 10](#)

[July 22](#)

Protection System and Human Performance Workshop Webinar

[August 7](#) and [August 8](#)

**RF Fall Reliability Summit,
Indianapolis, IN**

[September 16 - 18](#)

TECH TALK REMINDER

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

CLICK HERE 


MON
20

May 20 @ 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

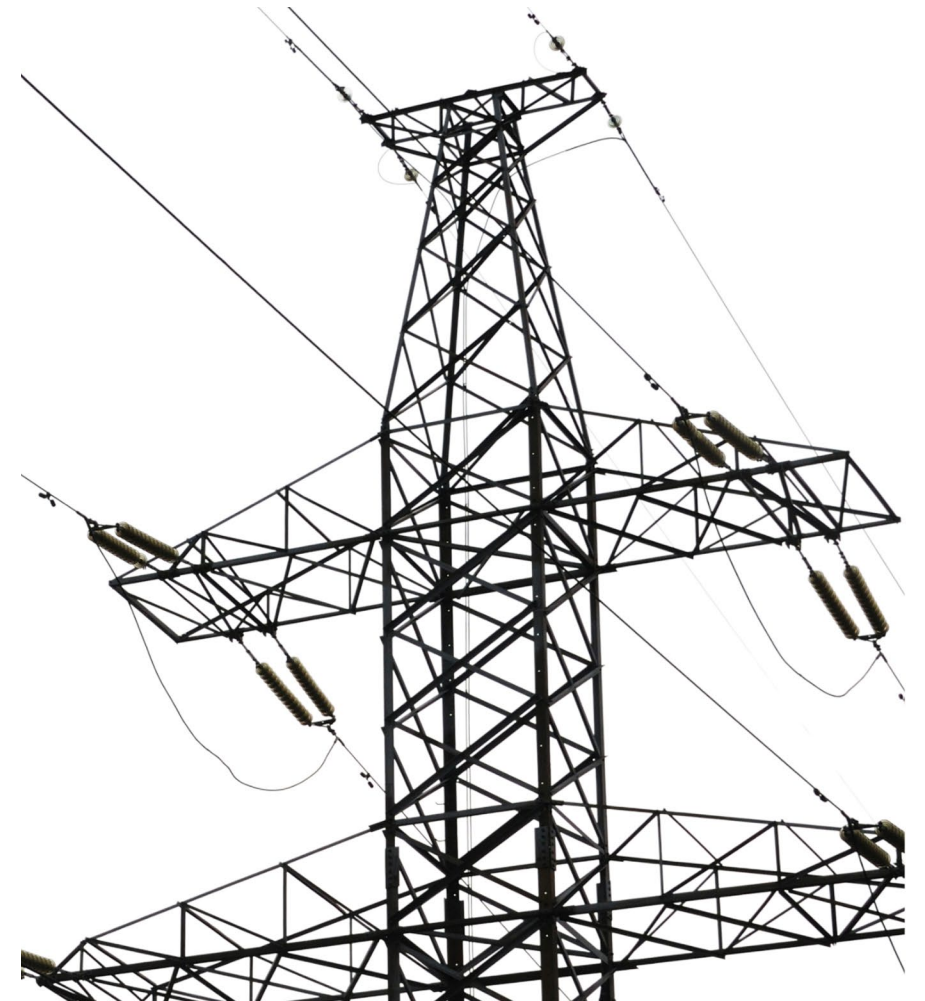
[SLIDO.com](https://www.slido.com)

#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

GO/GOP O&P AND CIP STANDARDS

- ASH CHAPPELL - RELIABILITYFIRST O&P TECHNICAL AUDITOR
- SHON AUSTIN - RELIABILITYFIRST CIP PRINCIPAL TECHNICAL AUDITOR

INTERNAL CONTROLS LESSONS LEARNED AND BEST PRACTICES

- JASON SMITH - DTE ENERGY DIRECTOR OF COMPLIANCE
- CHRIS PLENSDORF - DTE ENERGY MANAGER NERC COMPLIANCE
- JEFF WALLACE - DTE ENERGY SPECIALIST NERC COMPLIANCE

GO AND GOP O&P STANDARDS

Ash Chappell

Tech Talk with RF, May 20, 2024



RELIABILITY FIRST

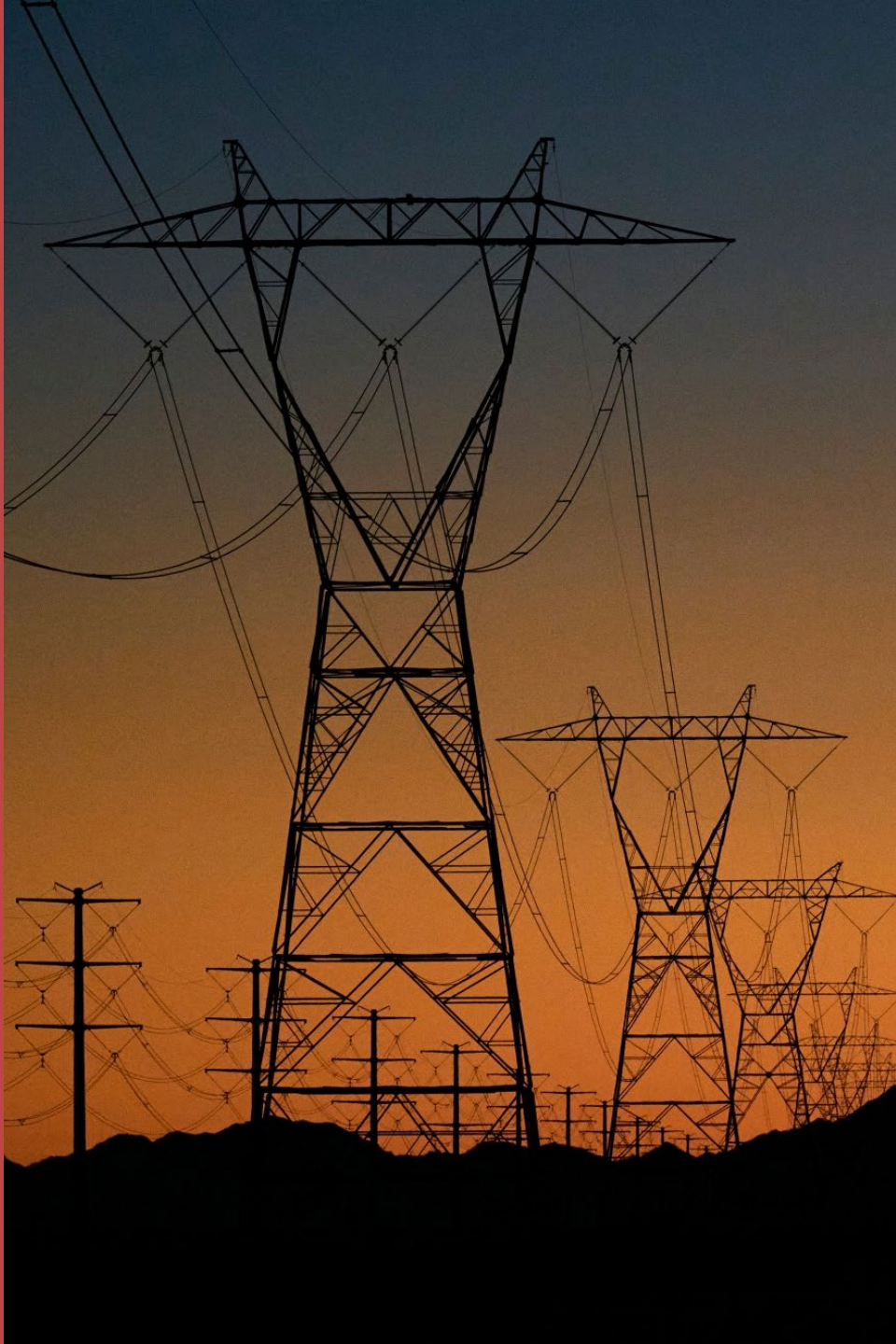
GO/GOP OUTLINE

- GO/GOP Standards
- The GO/GOP standards that are most violated (PNC)
- The GO/GOP standards with self-reports
- EOP-011-2 (R7 and R8)
transitioning over to EOP-012-2



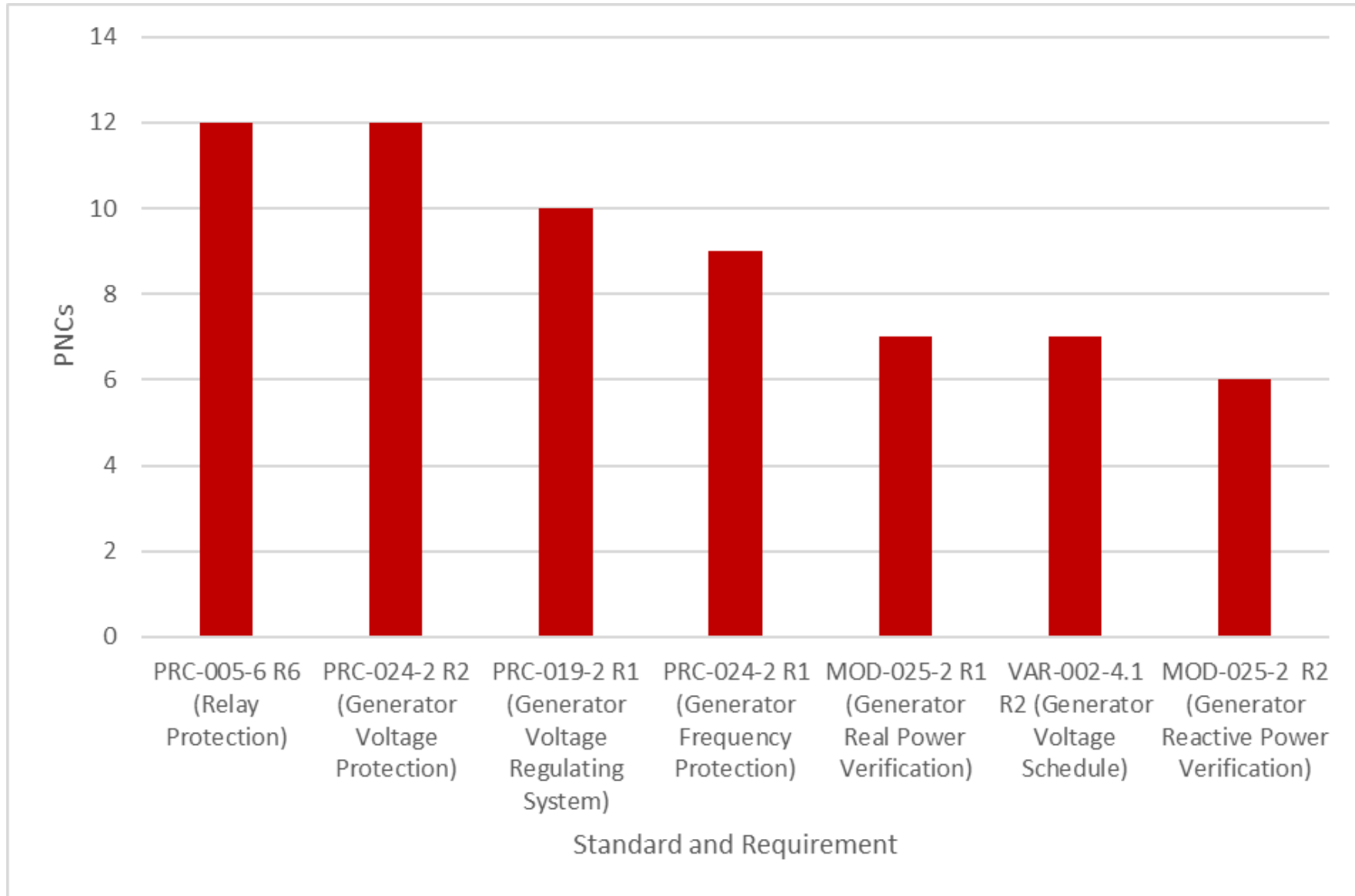
GO/GOP STANDARDS

THERE ARE 42 STANDARDS THAT COULD
APPLY TO A GO/GOP
(FROM THE O&P PERSPECTIVE)

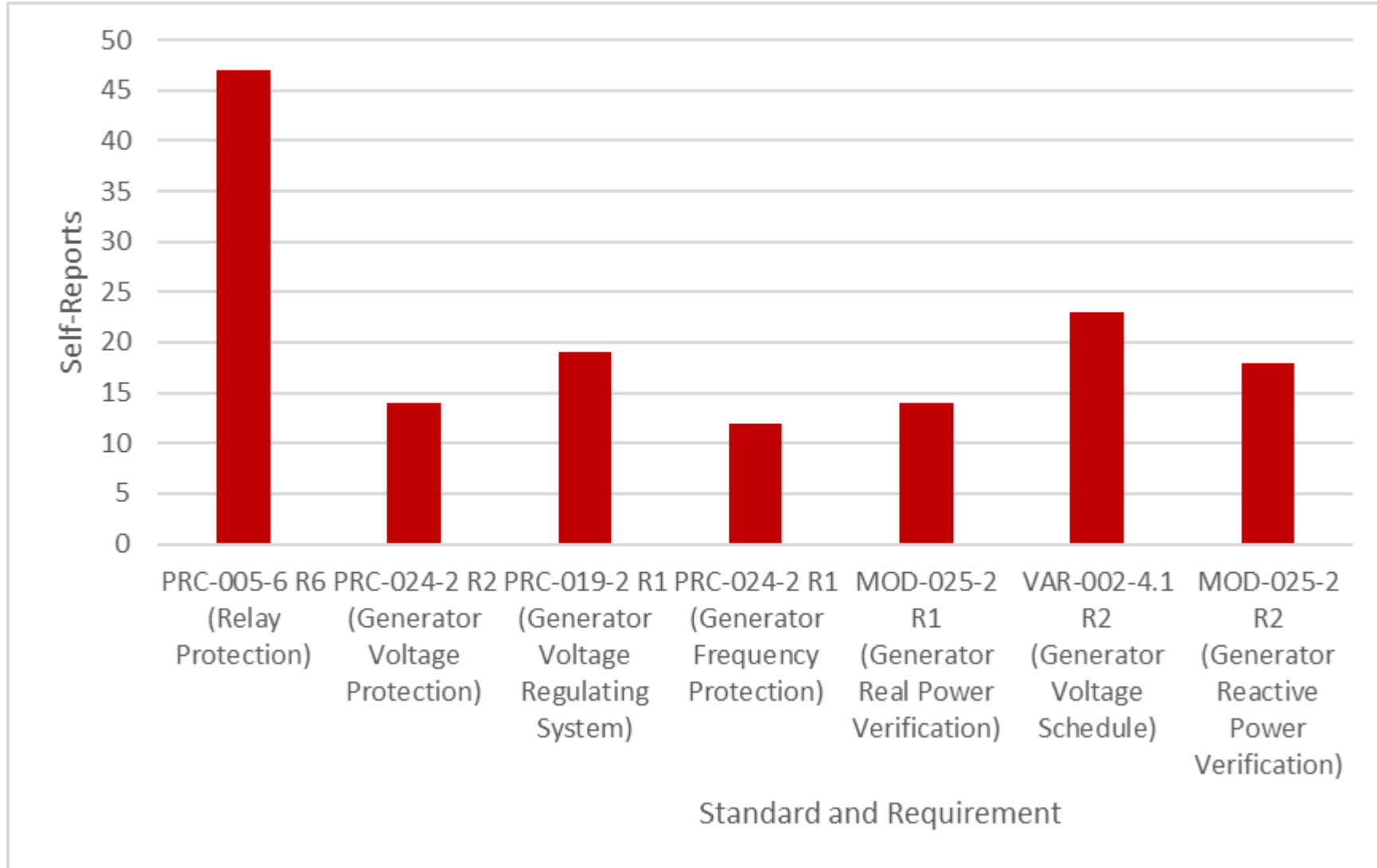


WHY IS RF COMMUNICATING THE MOST VIOLATED STANDARDS?

GO/GOP O&P STANDARDS WITH MOST PNCS FROM AUDIT FROM 2018-2023



GO/GOP O&P SELF-REPORTS FROM 2018-2023



GO/GOP STANDARDS

For Every Standard That We Reviewed There Were More Self-Report Than Finding From Monitoring Engagements.

- Complete necessary requirements in the time period interval.
- Reliance on contractor SME without adequate oversight.
- Status (automatic or manual) of the AVR or PSS, to maintain your voltage schedule.



GO/GOP STANDARDS

- In every standard reviewed there are more self-reports than compliance PNCs for the time period reviewed
 - For those that have robust internal controls programs, you are doing a great job of detecting reliability compliance gaps (this is a great thing).
 - As a reminder, our audit team should not be your internal control.
 - Compliance fitness starts with you, as we continue to partner together for the common goal of reliability.



MY COMPANY PURCHASED AN EXISTING GENERATOR - WHO IS RESPONSIBLE FOR COMPLIANCE SINCE LAST ENGAGEMENT?

- The new owner will be responsible for compliance from the last audit.
 - For example, generator Johnny Megawatt Inc. had a compliance audit in 2019 and was then sold in 2021.
 - In 2024, RF sent an Audit Notification Letter that Johnny Megawatt Inc. will have a compliance monitoring engagement.
 - The new owner would be responsible for compliance from 2019 (since the last compliance audit), not 2021 when they purchased it.



EOP-012-2 TIMEFRAME

February 2024 ● EOP-012-2 passed ballot

To be determined ● EOP-012-2 awaiting FERC Approval

May 2024 ● NERC Small Group Advisory Session (SGAS) for EOP-012-2

Oct. 1, 2024 ● EOP-012-1/2 effective (Depending On FERC Approval)

Q4 2024 ● RF performing on-site monitoring engagement for EOP-012-1/2



"Believe you can and you're halfway there!"

-Theodore Roosevelt



CIP STANDARDS FOR LOW IMPACT GO/GOP ENTITIES - 101

Shon Austin, Principal Technical Auditor

RF Tech Talk, May 20, 2024



OBJECTIVE

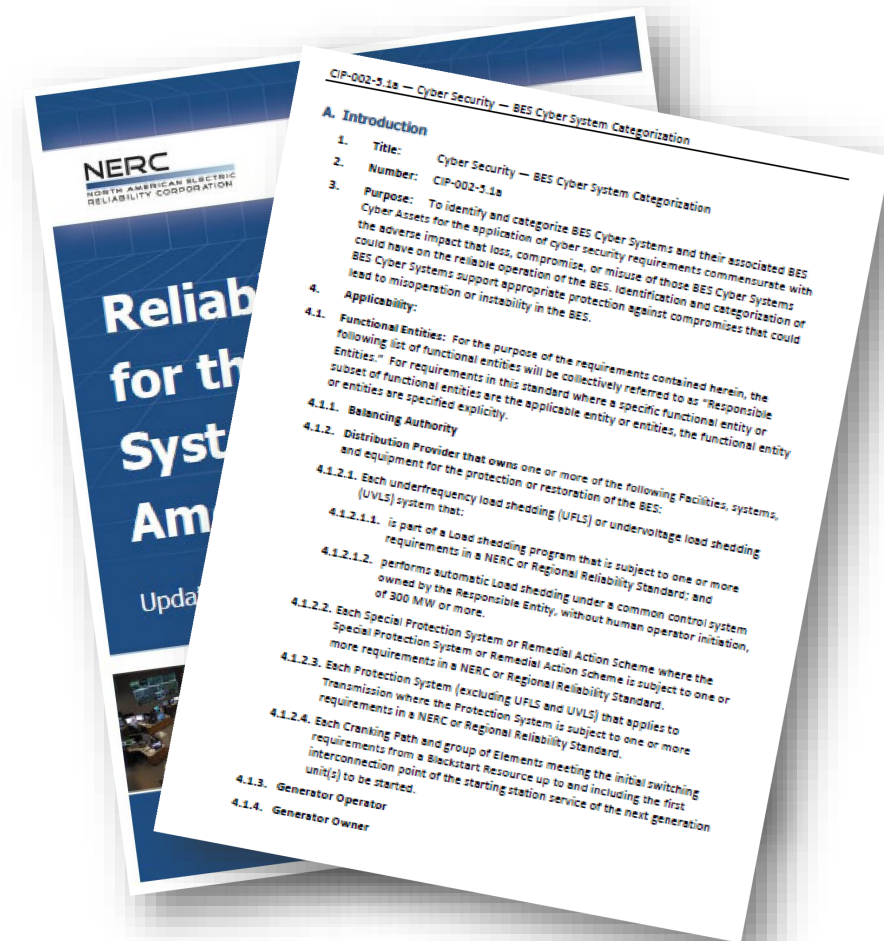
This presentation serves as a comprehensive desktop reference guide, offering valuable insights and resources pertaining to CIP-002-5.1a and CIP-003-8 processes

AGENDA

- LOW IMPACT DETERMINATION
- CIP-002-5.1A:
 - Background and information pertaining to Standard
- CIP-003-8:
 - Background and information pertaining to Standard
- INTERNAL CONTROLS: TYPES OF INTERNAL CONTROLS

LOW IMPACT DETERMINATION

- Categorization Criteria (CIP-002)
 - Requirement R1 only requires the discrete identification of BES Cyber Systems for those in the High Impact and Medium Impact categories.
 - All BES Cyber Systems for assets **not** included in **Attachment 1 – Impact Rating Criteria, Section 1 or Section 2, and listed in Section 3, default to Low Impact.**



CIP-002-5.1

- An implemented Process that considers each of the following assets for parts 1.1 through 1.3:
 - Control Centers and Backup Control Centers, Transmission Stations and Substations, Generation Resources, Systems and Facilities Critical to System Restoration (Blackstart Resources and Cranking Paths), Remedial Action Schemes that support the reliable operation of the BES and For Distribution Providers, Protection Systems specified in Applicability Section 4.2.1.
- P1.3 - Identify each asset that contains a low impact BES Cyber System according to Attachment 1, Section 3, if any (a discrete list of low impact BES Cyber Systems is not required).
- Evidence that the identifications in R1 and its parts (and update them if there are changes identified) have been reviewed at least once every 15 calendar months, even if there are no identified items in R1.
- Evidence that the CIP Senior Manager or delegate has approved the identifications required by R1 at least once every 15 calendar months, even if there are no identified items in R1.

Evidence Request Tool Reference	
Request ID	Standard & Requirement
CIP-002-R1-L1-01	CIP-002 R1
CIP-002-R1-L1-02	CIP-002 R1
CIP-002-R1-L1-03	CIP-002 R1
CIP-002-R1-L1-04	CIP-002 R1
CIP-002-R1-L1-05	CIP-002 R1
CIP-002-R1-L1-06	CIP-002 R1
CIP-002-R1-L1-07	CIP-002 R1
CIP-002-R1-L1-08	CIP-002 R1
CIP-002-R1-L1-09	CIP-002 R1
CIP-002-R2-L1-01	CIP-002 R2 Part 2.1 R2 Part 2.2

CIP-003-8 R1 & R2

- R1: Cyber Security Policies for the following:

- Cyber Security Awareness
- Physical Security Controls
- Electronic Access Controls
- Cyber Security Incident Response
- Transient Cyber Assets and Removable Media Malicious Code
- Declaring and Responding to CIP Exceptional Circumstances

- R2: Cyber Security Plans (and supporting evidence) for Low Impact BES Cyber Systems (BCS) that Include the Sections 1-5 in Attachment 1

- Each of the Sections in Attachment 1 provide additional detail for what each Low Impact Entity needs to have in place to meet the requirement
- R2 is the heavy lift for Low Impact Entities due to the number of additional “Requirements” listed in Attachment 1, Sections 1-5

Evidence Request Tool Reference	
Request ID	Standard & Requirement
CIP-003-R1-L1-01	CIP-003 R1
CIP-003-R2-L1-01	CIP-003 R2

CIP-003 R2 ATTACHMENT 1

- Section 1 – Cyber Security Awareness
 - Reinforce cybersecurity practices every 15 calendar months
- Section 2 – Physical Security Controls
 - Each Responsible Entity shall control physical access, based on need
- Section 3 – Electronic Access Controls
 - Permit only necessary inbound and outbound electronic access
 - Authenticate all Dial-up Connectivity, if any
- Section 4 – Cyber Security Incident Response
 - Identification, Classification and Response, Reportable, Roles and Responsibilities, Incident Handling, Testing at least every 36 calendar months, Updating process within 180 days after test or actual Incident
- Section 5 - Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation
 - Managed by the Responsible Entity – Method to mitigate the introduction of malicious code
 - Managed by a party other than the Responsible Entity – Method used to reduce the risk of malicious code introduction
 - Removable Media - Method(s) to detect malicious code on Removable Media & Mitigation strategy

Evidence Request Tool Reference	
Request ID	Standard & Requirement
CIP-003-R2-L1-02	CIP-003 R2 Sect 1
CIP-003-R2-L1-03	CIP-003 R2 Sect 4.4
CIP-003-R2-L1-04	CIP-003 R2 Sect 4.5
CIP-003-R2-L1-05	CIP-003 R2 Sect 4.6
CIP-003-R2-L2-01	CIP-003 R2 Sect 2
CIP-003-R2-L2-02	CIP-003 R2 Sect 3.1
CIP-003-R2-L2-03	CIP-003 R2 Sect 3.2
CIP-003-R2-L2-04	CIP-003 R2 Sect 4.2
CIP-003-R2-L2-05	CIP-003 R2 Sect 5.1
CIP-003-R2-L2-06	CIP-003 R2 Sect 5.2
CIP-003-R2-L2-07	CIP-003 R2 Sect 5.3

CIP-003 R2 ATTACHMENT 1

- Emphasis by the Compliance Team will be the detailed review of:

- Remote Access

Note: With the majority of Entities using contracted vendors to support their systems, it is vital that the interaction between the vendor and the Entity be highly secure.

- Be able to provide the following to the Compliance Team:

- Network Diagram(s) showing how the vendor accesses the Entity systems through their network architecture
- Firewall / Router Ruleset(s) and Configuration(s)
- Any other security controls in place

CIP-003 R3 & R4

- R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change.
- R4. The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates.

Evidence Request Tool Reference

Request ID	Standard & Requirement
CIP-003-R3-L1-01	CIP-003 R3
CIP-003-R4-L1-01	CIP-003 R4

INTERNAL CONTROLS

- Preventative Controls
 - Preventative controls aim to reduce the risk of a negative event occurring. Preventative controls can be physical or administrative controls depending on the requirement and capabilities at the entity's disposal.
 - Badge readers on a Control Center door are a physical preventative control, since they prevent unauthorized physical access into the Control Center. Common administrative preventative controls are procedures, checklists and training.
- Detective Controls
 - Detective controls seek to identify an issue that is occurring or has occurred.
 - Entity could establish alarms to alert system administrators if the physical access control system detects a door has been opened without a corresponding approved access card. In other words, the alarm detects and alerts personnel to a change from normal operations.
- Corrective Controls
 - Corrective controls correct issues once they have occurred.
 - Corrective controls return a situation to its normal state. Corrective controls can also be more compliance oriented. If a detective control identifies a potential noncompliance (PNC), the entity can remediate the issue and file a Self-Report.
- Testing Internal Controls
 - Once an entity has implemented internal controls, they can test the controls to verify that they are performing as expected. In a sense, testing controls is a control for the controls.



QUESTIONS & ANSWERS

Ash Chappell, Senior Technical Auditor,
O&P Compliance Monitoring

ash.chappell@rfirst.org

Shon Austin, Principal Technical Auditor,
CIP Compliance Monitoring

Shon.Austin@rfirst.org

THANK YOU

***Join us for our next Tech Talk -
June 10***

CIP Themes Report
RF's Managing Enforcement
Council - Tom Scanlon

Summer Reliability Assessment
RF's Principal Engineer - Tim
Fryfogle

[Webinar Link](#)

