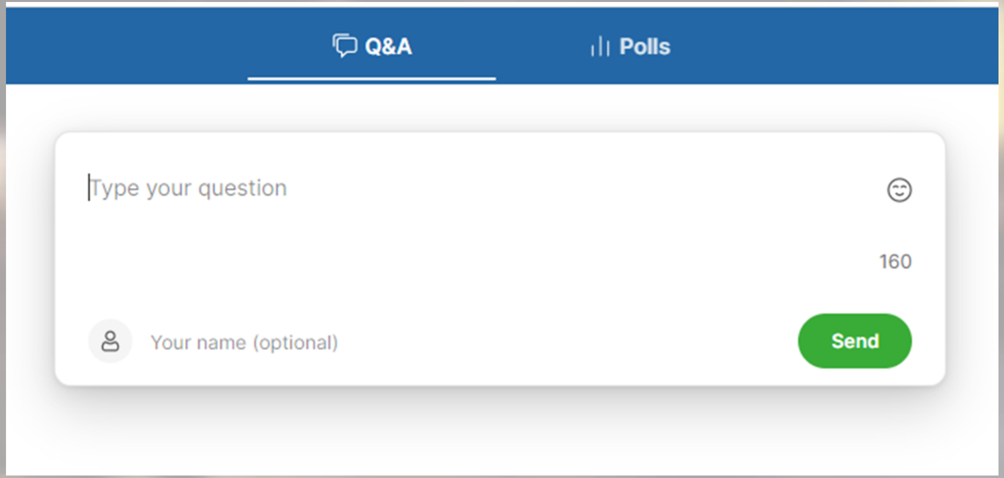
Fall Standards, Security, & Reliability Workshop

Begins at 9:00 a.m. Central

- New BCSI in the Cloud Standards
- FERC Vulnerability and Physical Security Assessment Program
- New Weatherization Requirements
- Emerging Cyber and Physical Risks
- Entity Ownership Change Considerations
- Cyber Informed Transmission Planning
- Change Management Controls
- Emerging Issues with Distributed Energy Resources
- Grid Forming Inverter Technology: Opportunities for a Changing Grid

To submit questions during the workshop, please visit **slido.com** and enter today's participant code: **TXRE**



STANDARDS, SECURITY, & RELIABILITY

FALL WORKSHOP

Welcome and Instructions

Matthew Barbour– Texas RE
Manager, Communications and Training

Antitrust Admonition

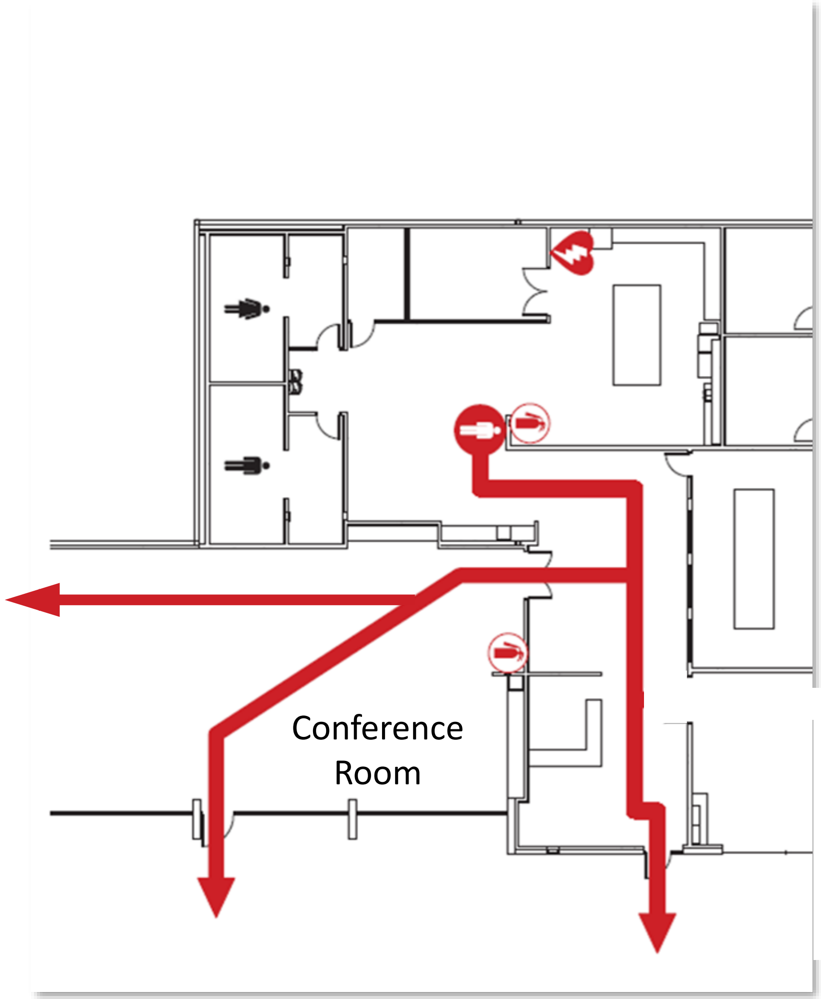
Texas Reliability Entity, Inc. (Texas RE) strictly prohibits persons participating in Texas RE activities from using their participation as a forum for engaging in practices or communications that violate antitrust laws. Texas RE has approved antitrust guidelines available on its website. If you believe that antitrust laws have been violated at a Texas RE meeting, or if you have any questions about the antitrust guidelines, please contact the Texas RE General Counsel.

Notice of this meeting was posted on the Texas RE website and this meeting is being held in public. Participants should keep in mind that the listening audience may include members of the press, representatives from various governmental authorities, and industry stakeholders.

Safety Moment

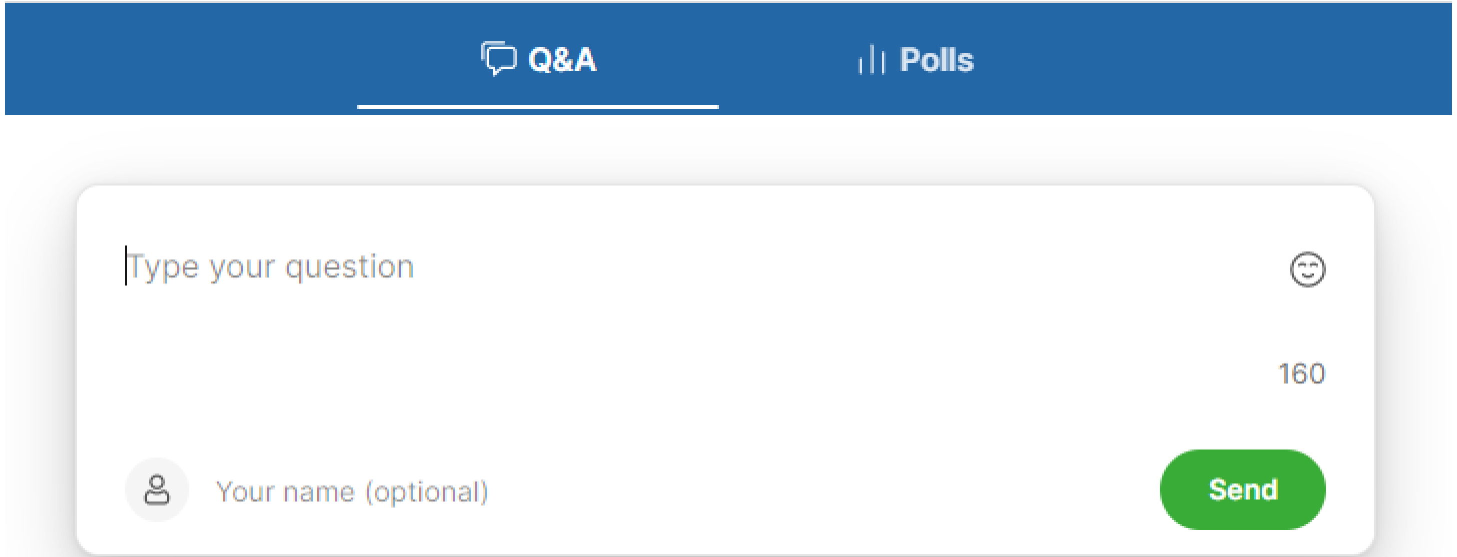
In case of emergency, evacuate through the nearest door

Rally point is in the front parking lot



Questions

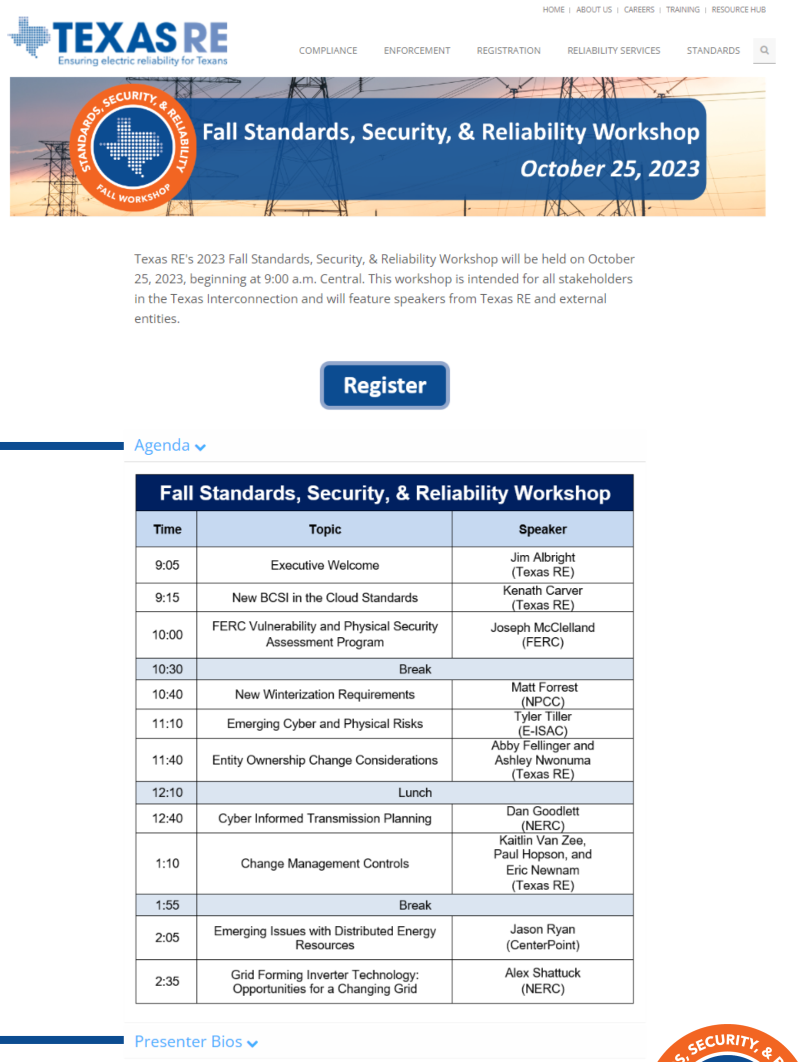
To submit questions during the workshop, please visit **slido.com** and enter today’s participant code: **TXRE**



Agenda & Presenter Bios

Agenda

Presenter Bios



HOME | ABOUT US | CAREERS | TRAINING | RESOURCE HUB
TEXAS RE
Ensuring electric reliability for Texans
COMPLIANCE
ENFORCEMENT
REGISTRATION
RELIABILITY SERVICES
STANDARDS
STANDARDS, SECURITY, & RELIABILITY
FALL WORKSHOP

Fall Standards, Security, & Reliability Workshop

October 25, 2023

Texas RE's 2023 Fall Standards, Security, & Reliability Workshop will be held on October 25, 2023, beginning at 9:00 a.m. Central. This workshop is intended for all stakeholders in the Texas Interconnection and will feature speakers from Texas RE and external entities.

Register

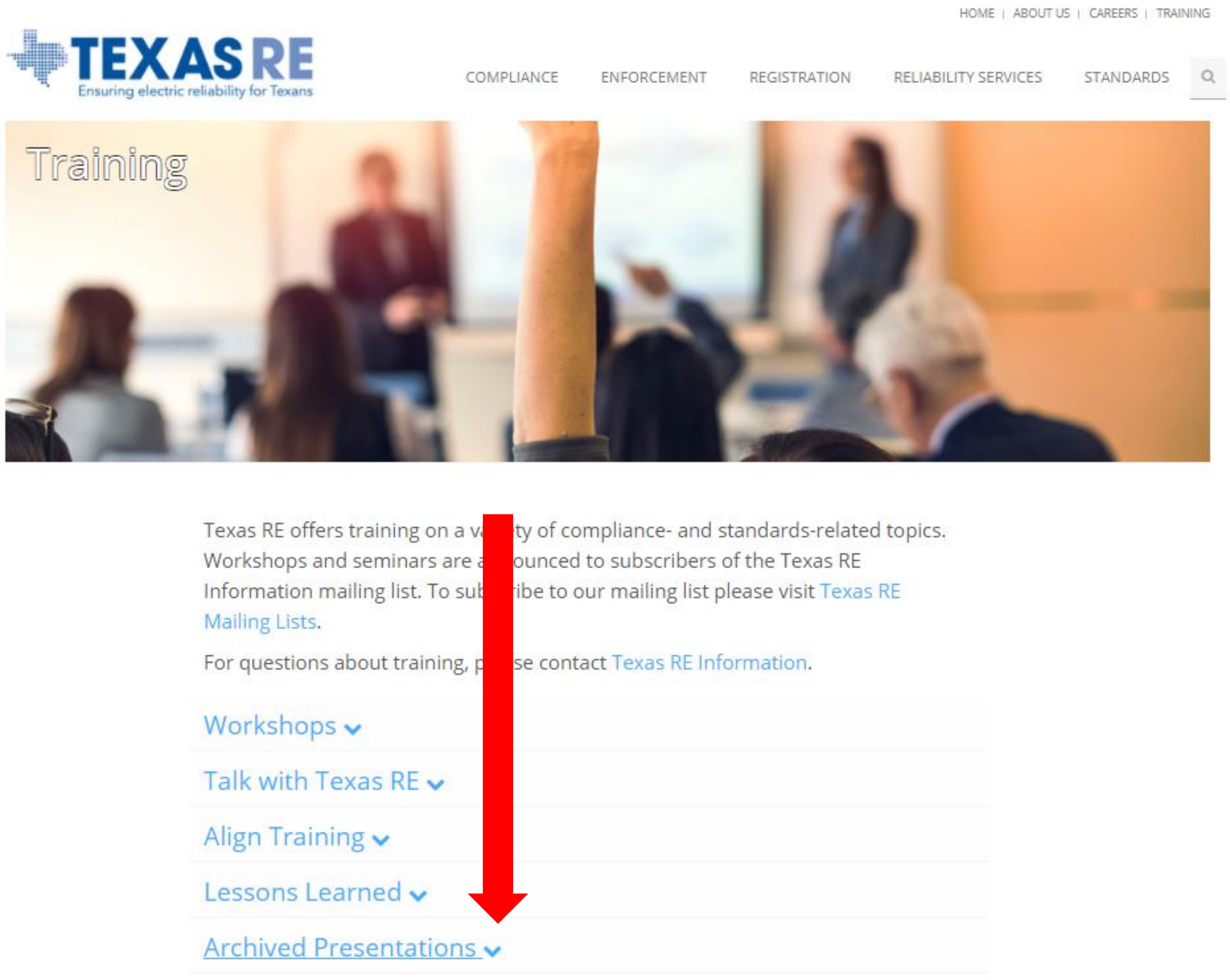
Agenda

Fall Standards, Security, & Reliability Workshop

Time	Topic	Speaker
9:05	Executive Welcome	Jim Albright (Texas RE)
9:15	New BCSI in the Cloud Standards	Kenath Carver (Texas RE)
10:00	FERC Vulnerability and Physical Security Assessment Program	Joseph McClelland (FERC)
10:30	Break	
10:40	New Winterization Requirements	Matt Forrest (NPCC)
11:10	Emerging Cyber and Physical Risks	Tyler Tiller (E-ISAC)
11:40	Entity Ownership Change Considerations	Abby Fellinger and Ashley Nwonuma (Texas RE)
12:10	Lunch	
12:40	Cyber Informed Transmission Planning	Dan Goodlett (NERC)
1:10	Change Management Controls	Kaitlin Van Zee, Paul Hopson, and Eric Newnam (Texas RE)
1:55	Break	
2:05	Emerging Issues with Distributed Energy Resources	Jason Ryan (CenterPoint)
2:35	Grid Forming Inverter Technology: Opportunities for a Changing Grid	Alex Shattuck (NERC)

Presenter Bios

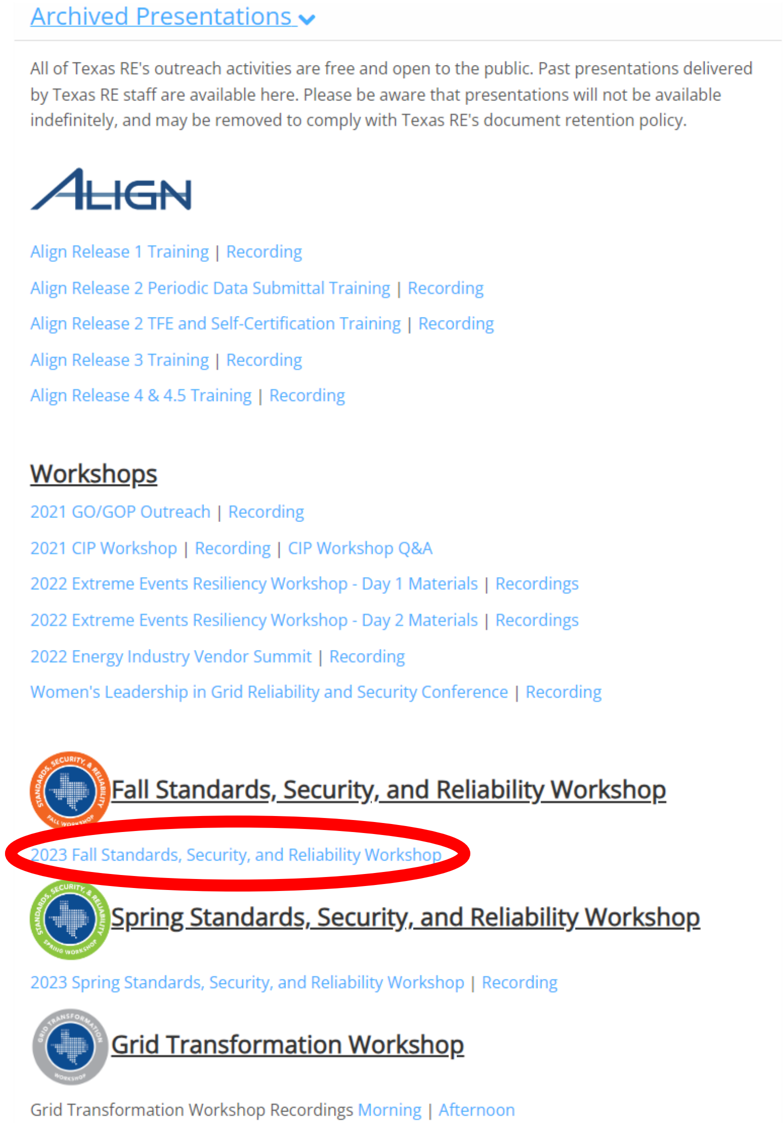
Training Page



Texas RE offers training on a variety of compliance- and standards-related topics. Workshops and seminars are announced to subscribers of the Texas RE Information mailing list. To subscribe to our mailing list please visit Texas RE Mailing Lists.

For questions about training, please contact Texas RE Information.

- Workshops
- Talk with Texas RE
- Align Training
- Lessons Learned
- Archived Presentations



Archived Presentations

All of Texas RE's outreach activities are free and open to the public. Past presentations delivered by Texas RE staff are available here. Please be aware that presentations will not be available indefinitely, and may be removed to comply with Texas RE's document retention policy.

Align Release 1 Training | Recording

Align Release 2 Periodic Data Submittal Training | Recording

Align Release 2 TFE and Self-Certification Training | Recording

Align Release 3 Training | Recording

Align Release 4 & 4.5 Training | Recording

Workshops

2021 GO/GOP Outreach | Recording

2021 CIP Workshop | Recording | CIP Workshop Q&A

2022 Extreme Events Resiliency Workshop - Day 1 Materials | Recordings

2022 Extreme Events Resiliency Workshop - Day 2 Materials | Recordings

2022 Energy Industry Vendor Summit | Recording

Women's Leadership in Grid Reliability and Security Conference | Recording

Fall Standards, Security, and Reliability Workshop

2023 Fall Standards, Security, and Reliability Workshop

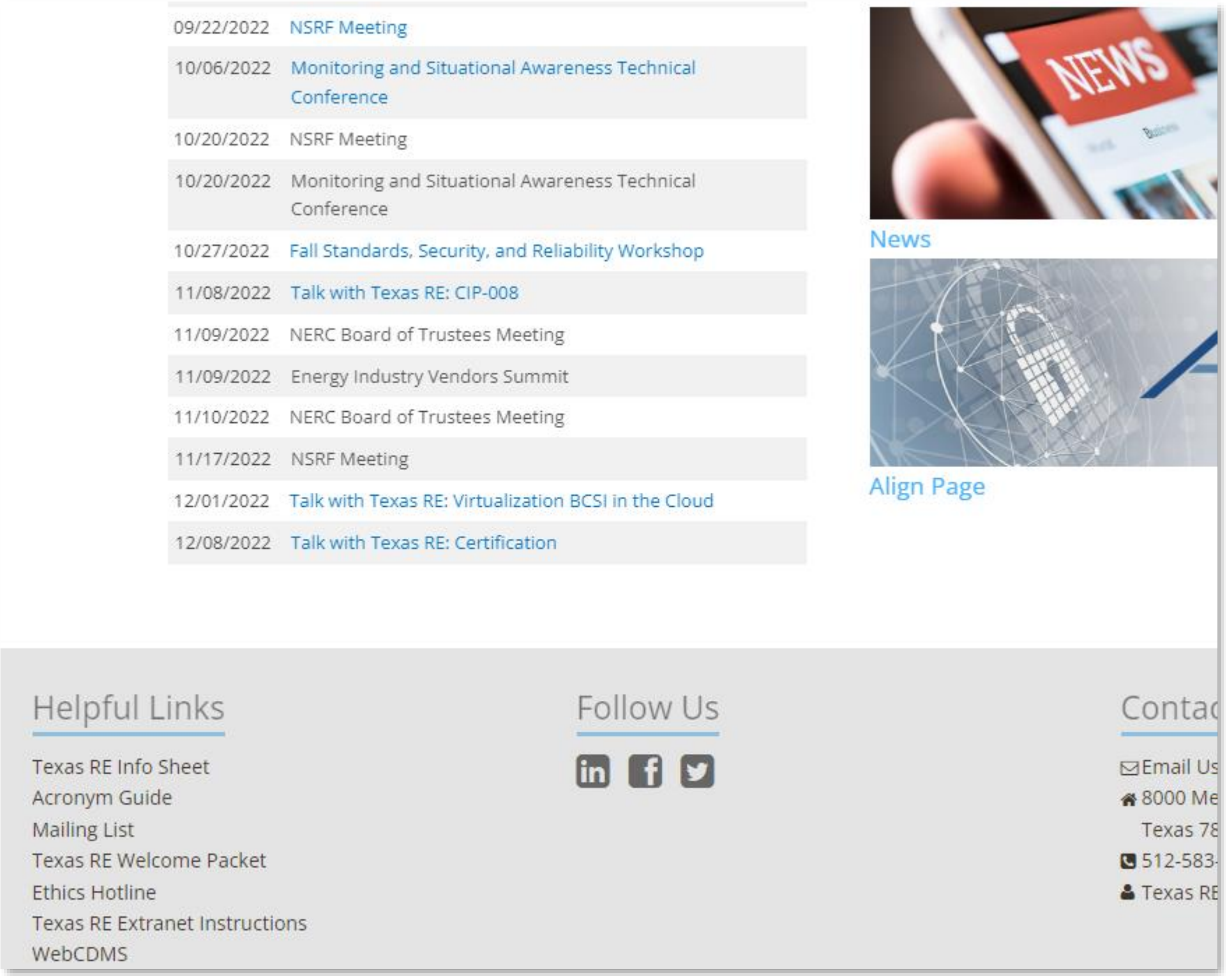
Spring Standards, Security, and Reliability Workshop

2023 Spring Standards, Security, and Reliability Workshop | Recording

Grid Transformation Workshop

Grid Transformation Workshop Recordings Morning | Afternoon

Acronym Guide



09/22/2022	NSRF Meeting
10/06/2022	Monitoring and Situational Awareness Technical Conference
10/20/2022	NSRF Meeting
10/20/2022	Monitoring and Situational Awareness Technical Conference
10/27/2022	Fall Standards, Security, and Reliability Workshop
11/08/2022	Talk with Texas RE: CIP-008
11/09/2022	NERC Board of Trustees Meeting
11/09/2022	Energy Industry Vendors Summit
11/10/2022	NERC Board of Trustees Meeting
11/17/2022	NSRF Meeting
12/01/2022	Talk with Texas RE: Virtualization BCSI in the Cloud
12/08/2022	Talk with Texas RE: Certification

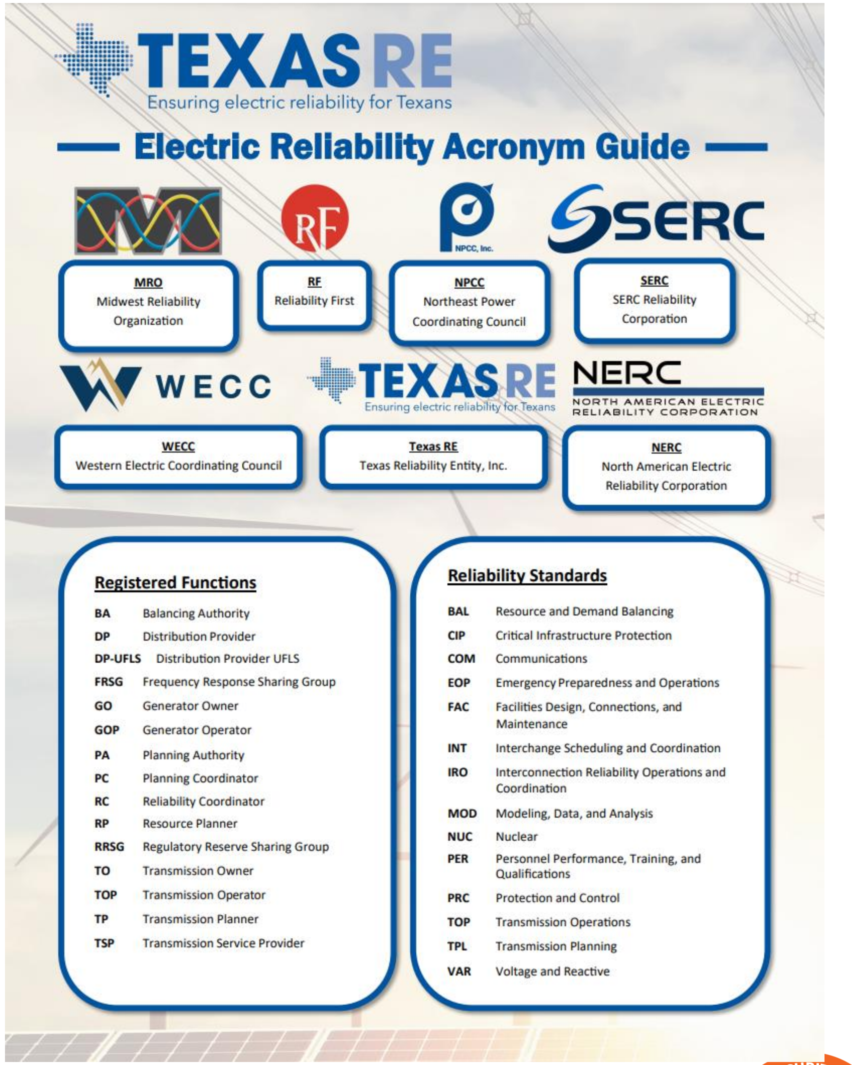
Helpful Links

- Texas RE Info Sheet
- Acronym Guide
- Mailing List
- Texas RE Welcome Packet
- Ethics Hotline
- Texas RE Extranet Instructions
- WebCDMS

Follow Us

Contac

✉Email Us
8000 Me
Texas 78
☎ 512-583-
Texas RE



TEXAS RE

Ensuring electric reliability for Texans

Electric Reliability Acronym Guide

RF
NPCC, Inc.
SERC
WECC
TEXAS RE
Ensuring electric reliability for Texans
NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

MRO	Midwest Reliability Organization
RF	Reliability First
NPCC	Northeast Power Coordinating Council
SERC	SERC Reliability Corporation
WECC	Western Electric Coordinating Council
Texas RE	Texas Reliability Entity, Inc.
NERC	North American Electric Reliability Corporation

Registered Functions

BA	Balancing Authority
DP	Distribution Provider
DP-UFLS	Distribution Provider UFLS
FRSG	Frequency Response Sharing Group
GO	Generator Owner
GOP	Generator Operator
PA	Planning Authority
PC	Planning Coordinator
RC	Reliability Coordinator
RP	Resource Planner
RRSG	Regulatory Reserve Sharing Group
TO	Transmission Owner
TOP	Transmission Operator
TP	Transmission Planner
TSP	Transmission Service Provider

Reliability Standards

BAL	Resource and Demand Balancing
CIP	Critical Infrastructure Protection
COM	Communications
EOP	Emergency Preparedness and Operations
FAC	Facilities Design, Connections, and Maintenance
INT	Interchange Scheduling and Coordination
IRO	Interconnection Reliability Operations and Coordination
MOD	Modeling, Data, and Analysis
NUC	Nuclear
PER	Personnel Performance, Training, and Qualifications
PRC	Protection and Control
TOP	Transmission Operations
TPL	Transmission Planning
VAR	Voltage and Reactive

MCLE Credit

This workshop is accredited for 5.0 Minimum Continuing Legal Education (MCLE) hours. To receive credit you may either:

❑ **Self-report the MCLE course number**

- 174214517

OR

❑ **Email Information@texasre.org your attendee information**

- Name
- Bar Card Number
- Hours Attended

Social Media Links

Linkedin® /texas-reliability-entity-inc

@Texas_RE_Inc

/TexasReliabilityEntity

Questions?

TEXAS RE
Ensuring electric reliability for Texans

STANDARDS, SECURITY, & RELIABILITY
FALL WORKSHOP

Executive Welcome
Jim Albright
Texas RE President & CEO

New BCSI in the Cloud Standards

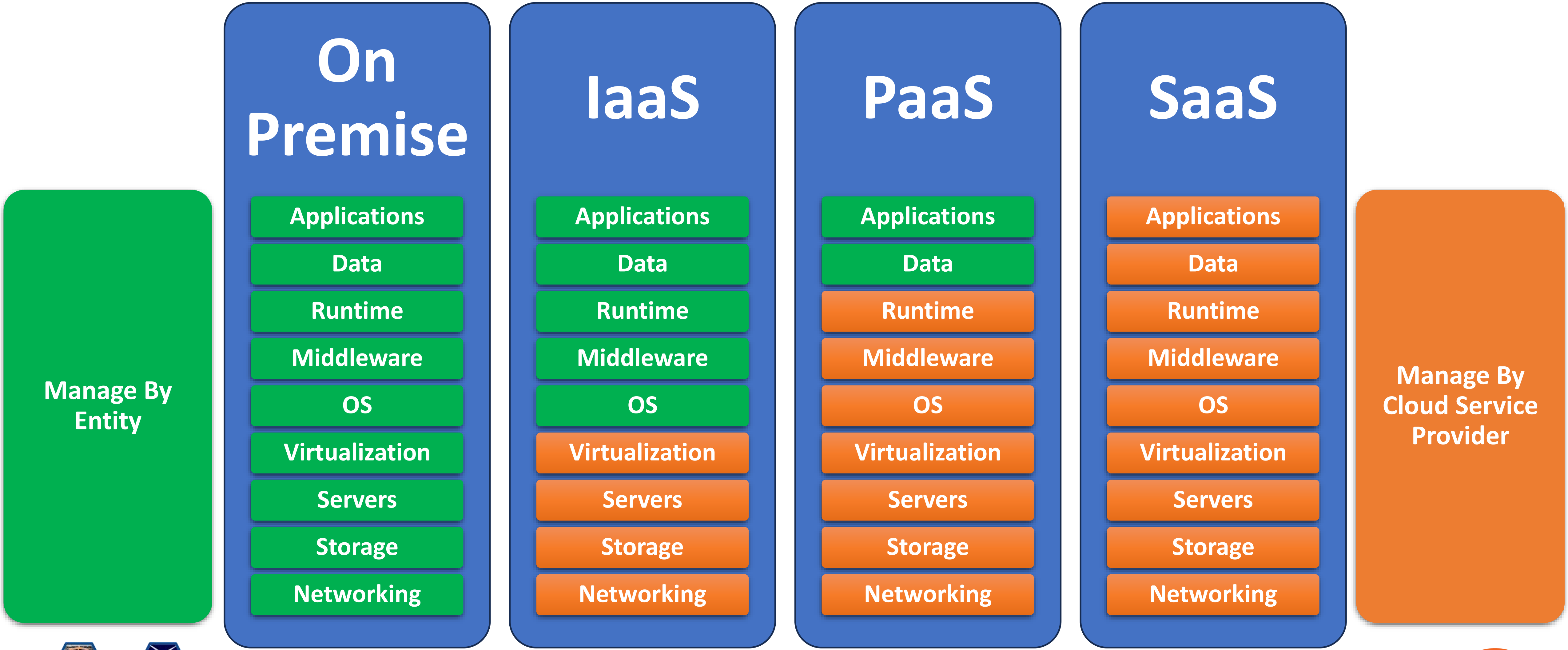
Kenath Carver
Director, Compliance Assessments

October 25, 2023

Project 2019-02 BES Cyber System Information Access Management

Effective: January 1, 2024

Cloud Models

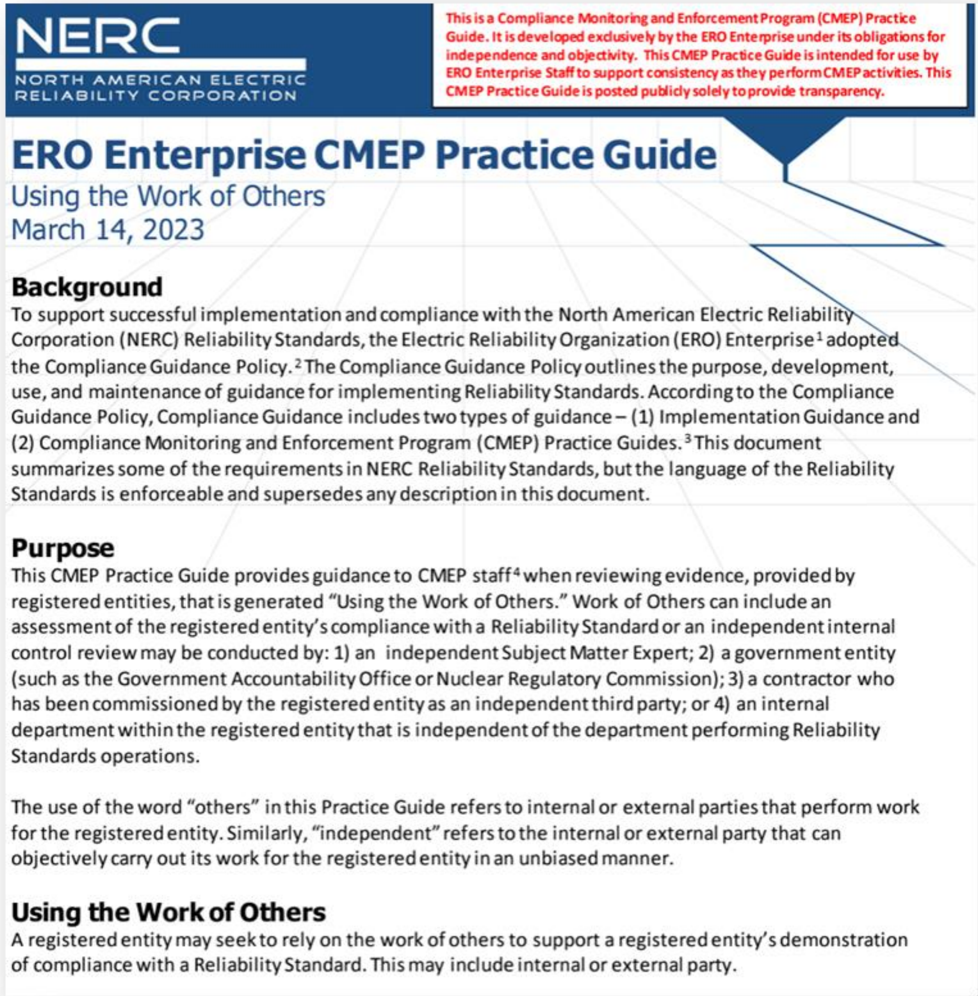


🟩 Manage By Entity

🟧 Manage By Cloud Service Provider

On Premise	IaaS	PaaS	SaaS
🟩 Applications	🟩 Applications	🟩 Applications	🟧 Applications
🟩 Data	🟩 Data	🟩 Data	🟧 Data
🟩 Runtime	🟩 Runtime	🟧 Runtime	🟧 Runtime
🟩 Middleware	🟩 Middleware	🟧 Middleware	🟧 Middleware
🟩 OS	🟩 OS	🟧 OS	🟧 OS
🟩 Virtualization	🟧 Virtualization	🟧 Virtualization	🟧 Virtualization
🟩 Servers	🟧 Servers	🟧 Servers	🟧 Servers
🟩 Storage	🟧 Storage	🟧 Storage	🟧 Storage
🟩 Networking	🟧 Networking	🟧 Networking	🟧 Networking

Using the Work of Others



NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

This is a Compliance Monitoring and Enforcement Program (CMEP) Practice Guide. It is developed exclusively by the ERO Enterprise under its obligations for independence and objectivity. This CMEP Practice Guide is intended for use by ERO Enterprise Staff to support consistency as they perform CMEP activities. This CMEP Practice Guide is posted publicly solely to provide transparency.

ERO Enterprise CMEP Practice Guide

Using the Work of Others
March 14, 2023

Background

To support successful implementation and compliance with the North American Electric Reliability Corporation (NERC) Reliability Standards, the Electric Reliability Organization (ERO) Enterprise[1] adopted the Compliance Guidance Policy.[2] The Compliance Guidance Policy outlines the purpose, development, use, and maintenance of guidance for implementing Reliability Standards. According to the Compliance Guidance Policy, Compliance Guidance includes two types of guidance – (1) Implementation Guidance and (2) Compliance Monitoring and Enforcement Program (CMEP) Practice Guides.[3] This document summarizes some of the requirements in NERC Reliability Standards, but the language of the Reliability Standards is enforceable and supersedes any description in this document.

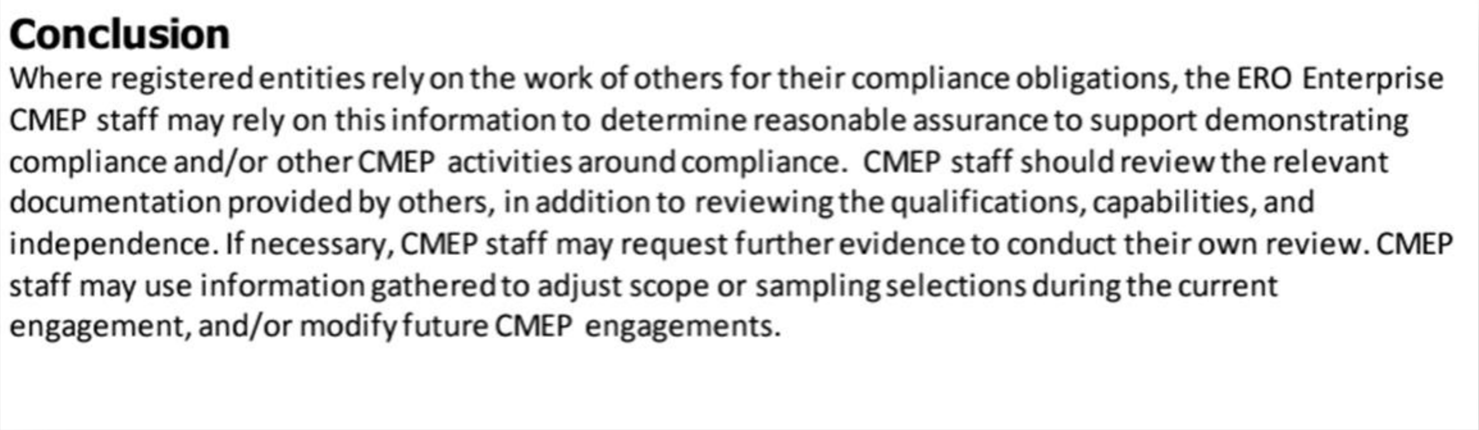
Purpose

This CMEP Practice Guide provides guidance to CMEP staff[4] when reviewing evidence, provided by registered entities, that is generated "Using the Work of Others." Work of Others can include an assessment of the registered entity's compliance with a Reliability Standard or an independent internal control review may be conducted by: 1) an independent Subject Matter Expert; 2) a government entity (such as the Government Accountability Office or Nuclear Regulatory Commission); 3) a contractor who has been commissioned by the registered entity as an independent third party; or 4) an internal department within the registered entity that is independent of the department performing Reliability Standards operations.

The use of the word "others" in this Practice Guide refers to internal or external parties that perform work for the registered entity. Similarly, "independent" refers to the internal or external party that can objectively carry out its work for the registered entity in an unbiased manner.

Using the Work of Others

A registered entity may seek to rely on the work of others to support a registered entity's demonstration of compliance with a Reliability Standard. This may include internal or external party.

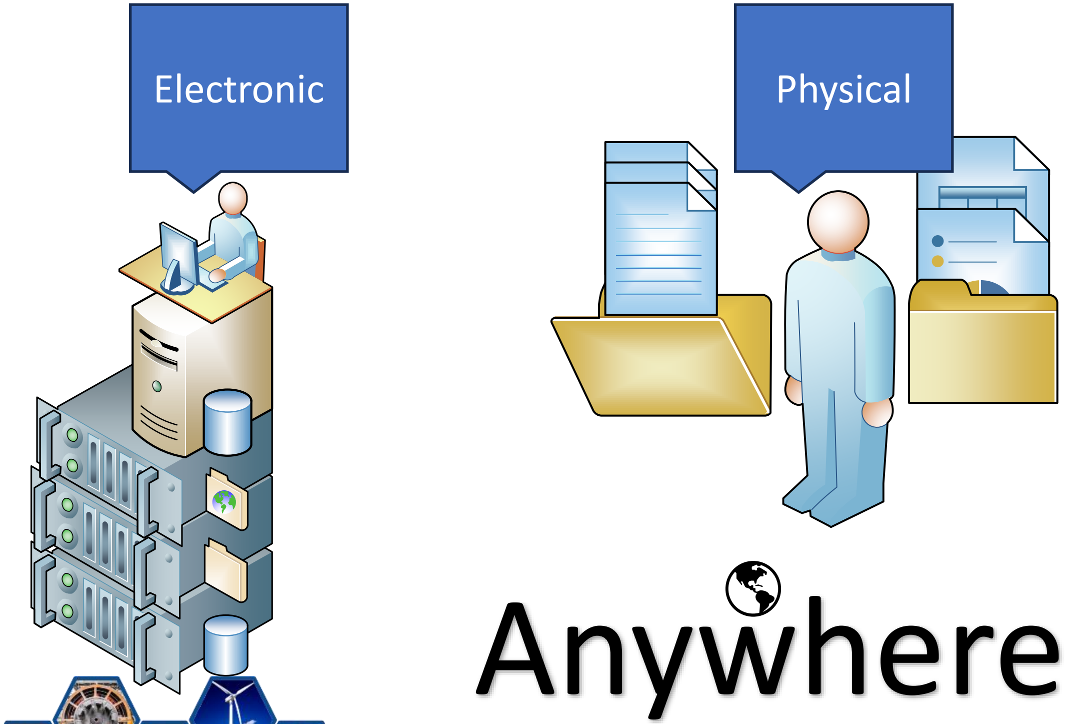


Conclusion

Where registered entities rely on the work of others for their compliance obligations, the ERO Enterprise CMEP staff may rely on this information to determine reasonable assurance to support demonstrating compliance and/or other CMEP activities around compliance. CMEP staff should review the relevant documentation provided by others, in addition to reviewing the qualifications, capabilities, and independence. If necessary, CMEP staff may request further evidence to conduct their own review. CMEP staff may use information gathered to adjust scope or sampling selections during the current engagement, and/or modify future CMEP engagements.

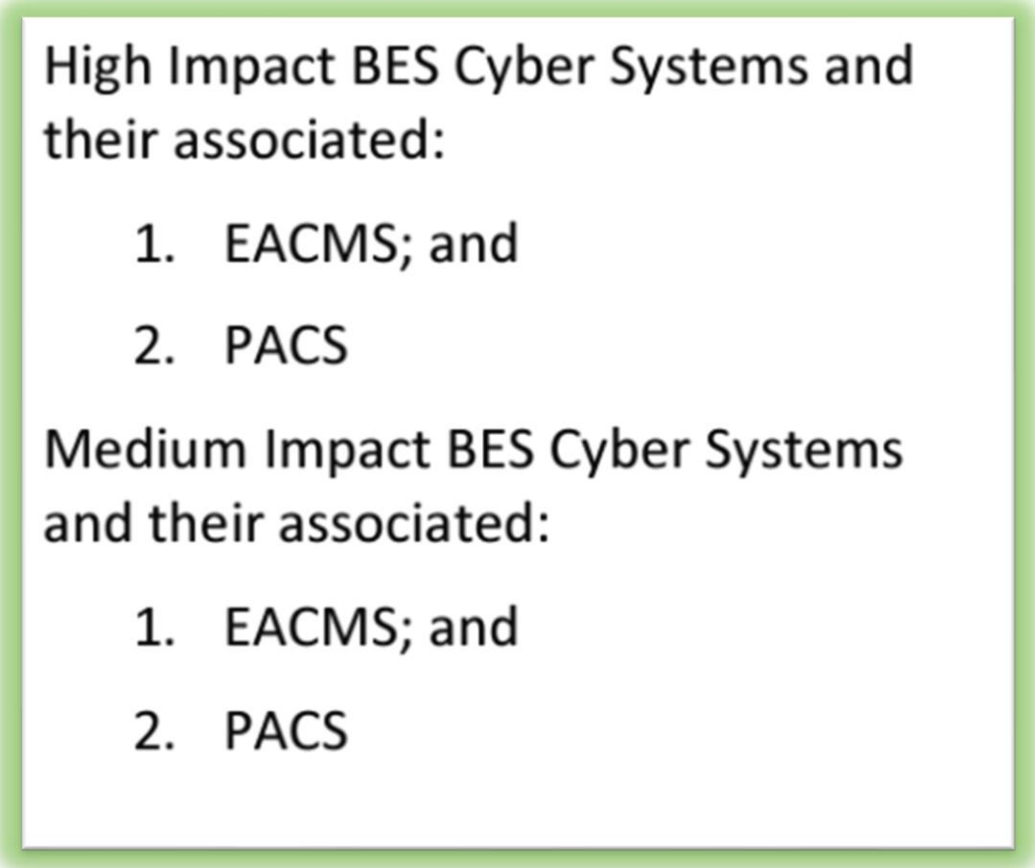
BES Cyber System Information (BCSI)

Information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context, ESP names, or policy statements. Examples of BES Cyber System Information may include, but are not limited to, security procedures or security information about BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber System.



- Information
- Unauthorized Access
- Unauthorized Distribution
- Security Threat
- Security Information
- Not Publicly Available
- Does Not Include Individual Pieces of Information

CIP-011-3 R1



High Impact BES Cyber Systems and their associated:

1. EACMS; and
2. PACS

Medium Impact BES Cyber Systems and their associated:

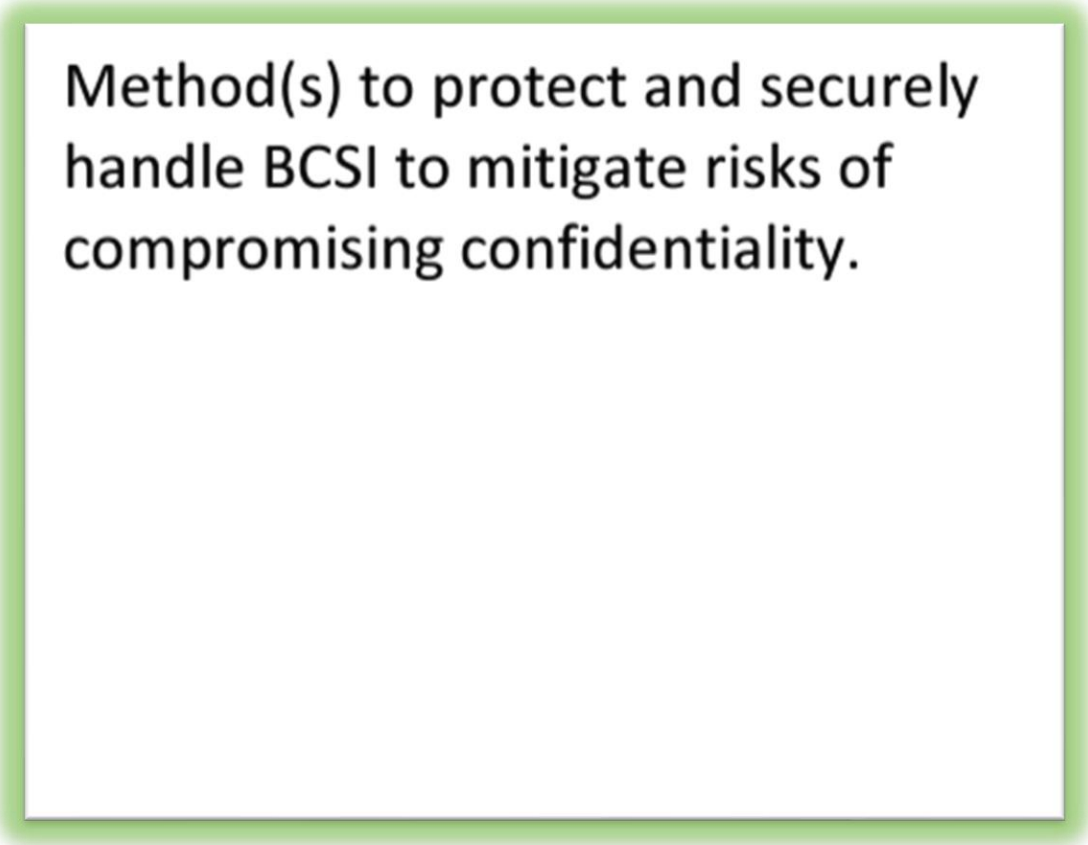
1. EACMS; and
2. PACS

CIP-011-3 R1 Part 1.1

Method(s) to identify BCSI.

- Procedures, Processes, Etc.
- Third-Party Services
- Data Loss Prevention
- Labels, Classification, Metadata
- Vulnerability Assessment
- Training
- BCSI Storage Locations
- Whitelist
- Databases
- Spreadsheets
- Contracts, Service Level Agreements, Etc.

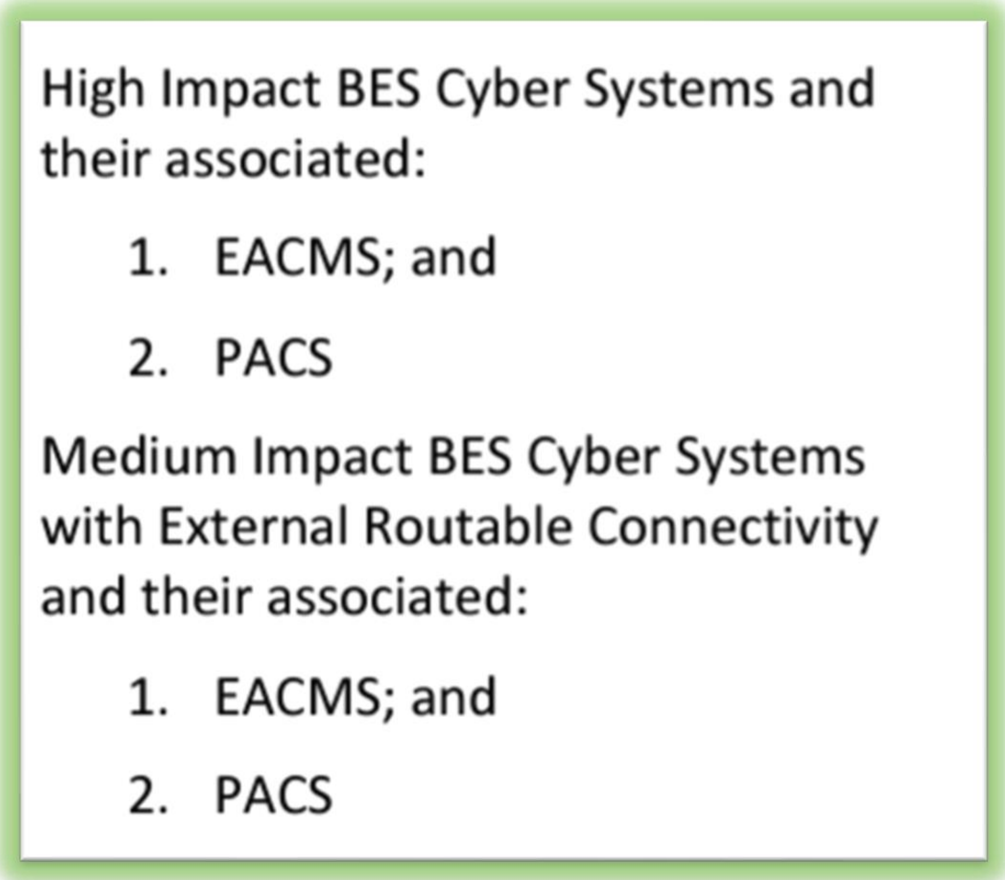
CIP-011-3 R1 Part 1.2



Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality.

- Procedures, Processes, Etc.
- Data Loss Prevention
- Encryption (Storage, Transit, Use)
- Encryption Key Management
- Data Masking, Obfuscation
- Physical Access Controls
- Access Management
- Identification, Authentication
- Vault
- Chain of Custody
- Firewall

CIP-004-7 R6



High Impact BES Cyber Systems and their associated:

1. EACMS; and
2. PACS

Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

1. EACMS; and
2. PACS

CIP-004-7 R6

Access Management Program(s)

- Authorize, verify, and revoke provisioned access

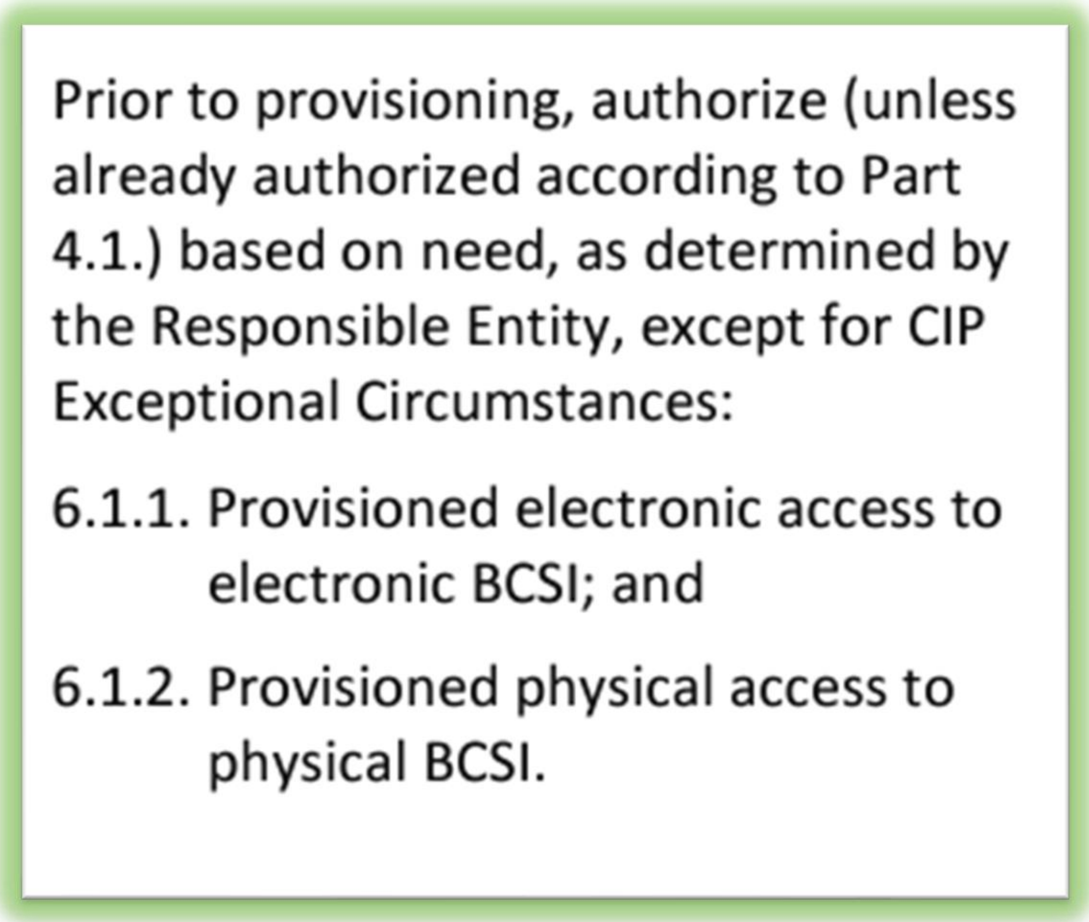
Access

- Individual has both the ability to obtain

Provisioned Access

- Specific actions taken to provide an individual(s) the means to access

CIP-004-7 R6 Part 6.1



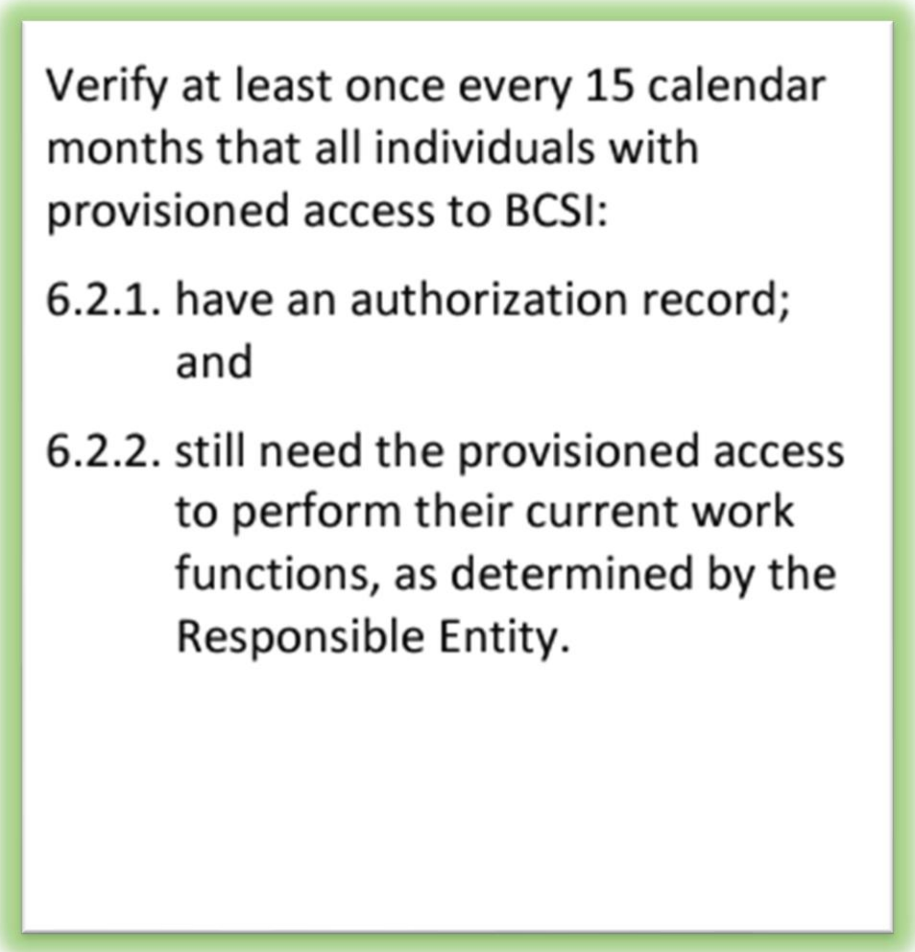
Prior to provisioning, authorize (unless already authorized according to Part 4.1.) based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances:

6.1.1. Provisioned electronic access to electronic BCSI; and

6.1.2. Provisioned physical access to physical BCSI.

- Procedures, Processes, Etc.
- Access Management System
- Records, Reports
- Lists, Logs
- Change Control
- Databases, Spreadsheets
- Third-Party Audit Reports
- Controls Preventing Access

CIP-004-7 R6 Part 6.2



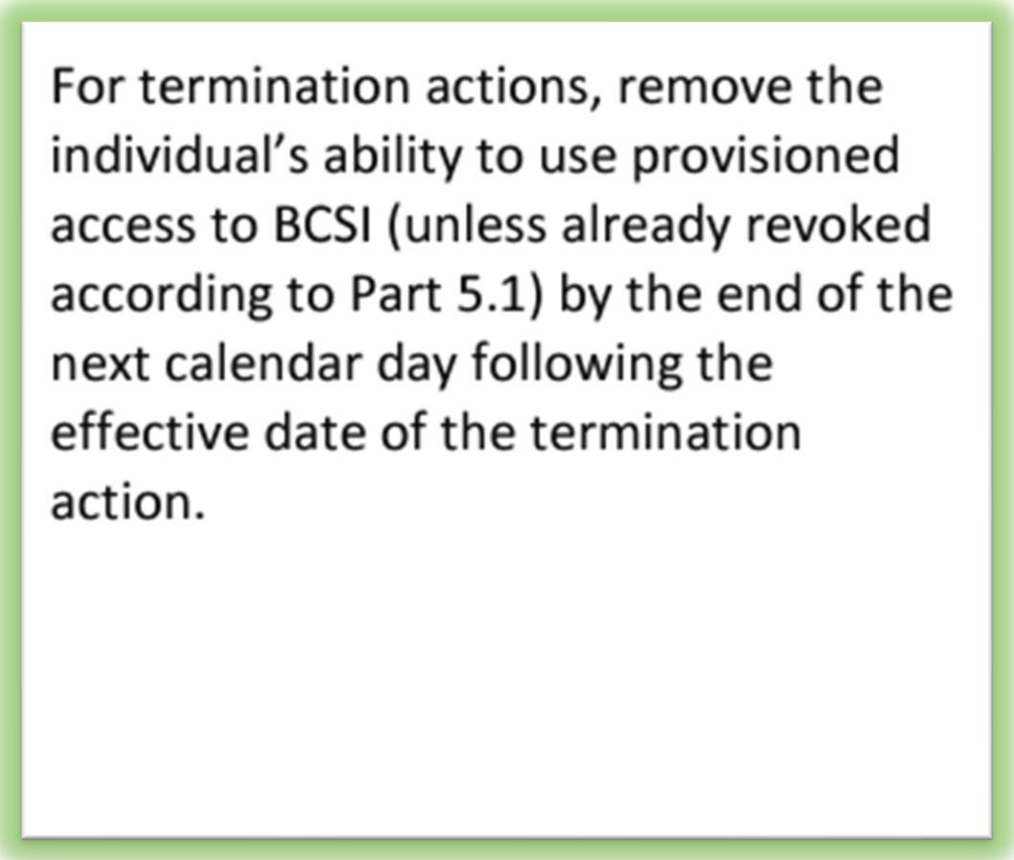
Verify at least once every 15 calendar months that all individuals with provisioned access to BCSI:

6.2.1. have an authorization record; and

6.2.2. still need the provisioned access to perform their current work functions, as determined by the Responsible Entity.

- Procedures, Processes, Etc.
- Review and Verification Based on Need
- Reconciliation Actions
- Lists, Spreadsheets
- Reports
- Third-Party Audit Reports
- Change Control
- Access Management System

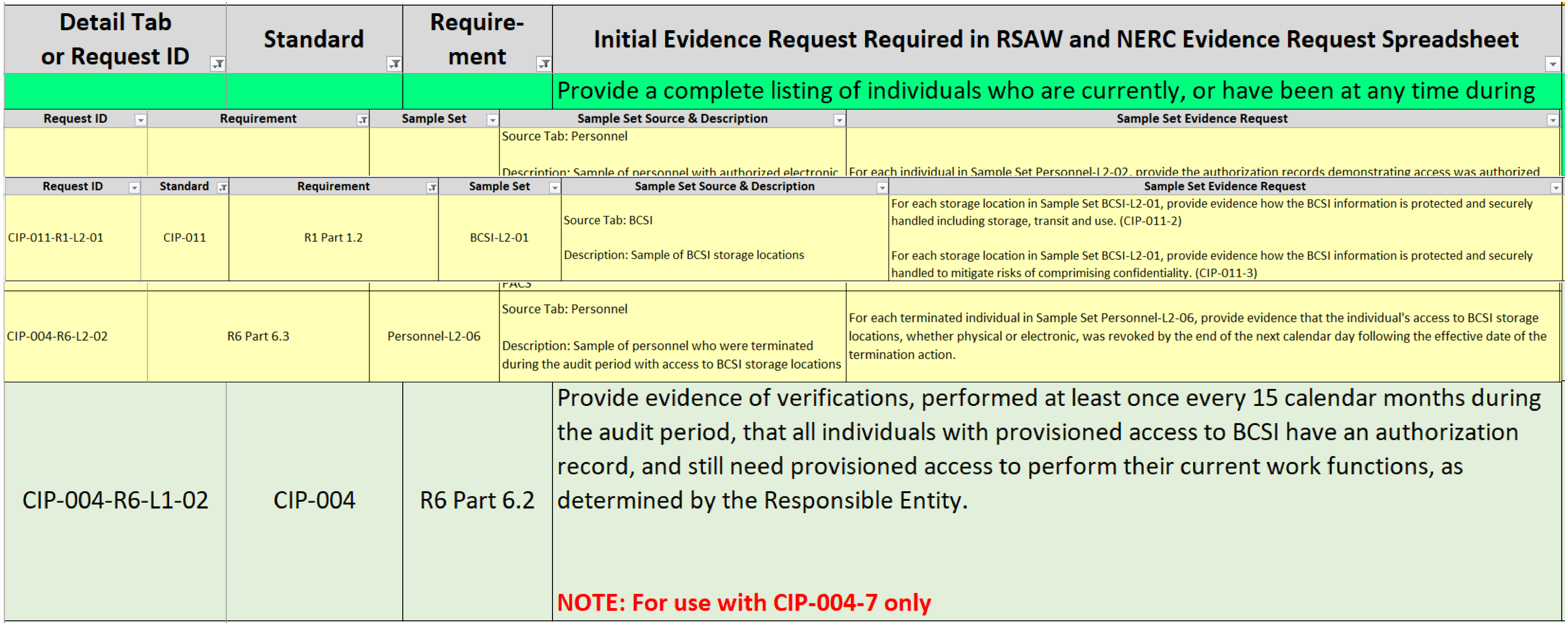
CIP-004-7 R6 Part 6.3



For termination actions, remove the individual's ability to use provisioned access to BCSI (unless already revoked according to Part 5.1) by the end of the next calendar day following the effective date of the termination action.

- Procedures, Processes, Etc.
- Records, Reports, Lists, Spreadsheets, Logs
- Access Management System
- Third-Party Audit Reports

CIP Evidence Request Tool



Detail Tab or Request ID	Standard	Require-ment	Initial Evidence Request Required in RSAW and NERC Evidence Request Spreadsheet
			Provide a complete listing of individuals who are currently, or have been at any time during

Request ID	Requirement	Sample Set	Sample Set Source & Description	Sample Set Evidence Request
			Source Tab: Personnel Description: Sample of personnel with authorized electronic	For each individual in Sample Set Personnel-L2-02, provide the authorization records demonstrating access was authorized

Request ID	Standard	Requirement	Sample Set	Sample Set Source & Description	Sample Set Evidence Request
CIP-011-R1-L2-01	CIP-011	R1 Part 1.2	BCSI-L2-01	Source Tab: BCSI Description: Sample of BCSI storage locations	For each storage location in Sample Set BCSI-L2-01, provide evidence how the BCSI information is protected and securely handled including storage, transit and use. (CIP-011-2) For each storage location in Sample Set BCSI-L2-01, provide evidence how the BCSI information is protected and securely handled to mitigate risks of comprimising confidentiality. (CIP-011-3)

Request ID	Requirement	Sample Set	Sample Set Source & Description	Sample Set Evidence Request
			PACS	
CIP-004-R6-L2-02	R6 Part 6.3	Personnel-L2-06	Source Tab: Personnel Description: Sample of personnel who were terminated during the audit period with access to BCSI storage locations	For each terminated individual in Sample Set Personnel-L2-06, provide evidence that the individual's access to BCSI storage locations, whether physical or electronic, was revoked by the end of the next calendar day following the effective date of the termination action.

Detail Tab or Request ID	Standard	Require-ment	Initial Evidence Request Required in RSAW and NERC Evidence Request Spreadsheet
CIP-004-R6-L1-02	CIP-004	R6 Part 6.2	Provide evidence of verifications, performed at least once every 15 calendar months during the audit period, that all individuals with provisioned access to BCSI have an authorization record, and still need provisioned access to perform their current work functions, as determined by the Responsible Entity. **NOTE: For use with CIP-004-7 only**

Conclusion

IDENTIFY	BCSI
PROTECT & SECURE	Confidentiality
DETERMINE NEED	Electronic or Physical Access
AUTHORIZE ACCESS	Provisioned Electronic or Physical Access
VERIFY ACCESS	15 Calendar Months
REVOKE ACCESS	End of Next Calendar Day

Questions?

TEXAS RE

Ensuring electric reliability for Texans

Public

Texas RE
Fall Standards, Security, & Reliability Workshop
October 25, 2023

Joe McClelland
Director, Office of Energy Infrastructure Security (OEIS)
Federal Energy Regulatory Commission

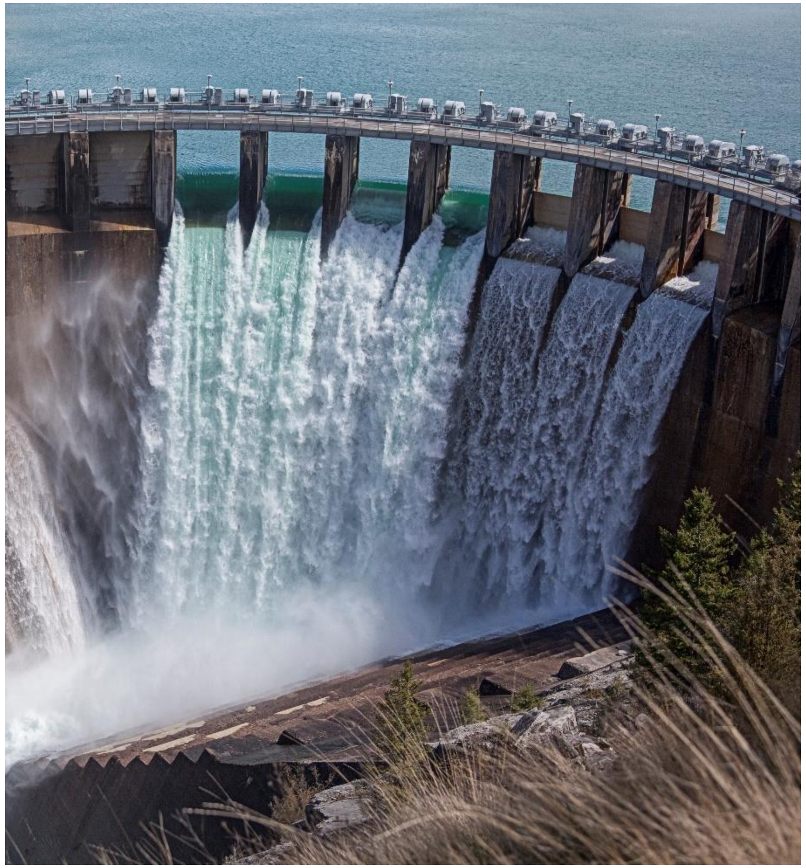
Public

Disclaimer

The views expressed in this presentation are my own and do not necessarily represent the views of any Commissioner or the Commission.

CYBERSECURITY

PHYSICAL SECURITY



FERC Overview

Critical Infrastructure Threats

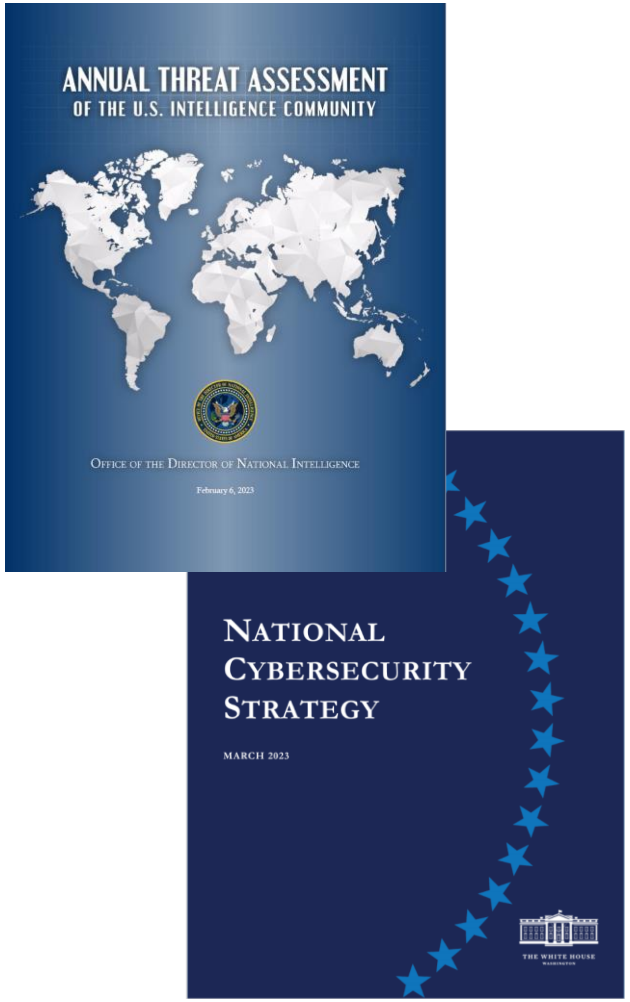
“**China** almost certainly is capable of launching cyber attacks that would disrupt [CI] services within the [US], including against oil and gas pipelines and rail systems.”
[1 p.10]

On July 21, 2021, CISA issued a Cybersecurity Advisory entitled “Chinese Gas Pipeline Intrusion Campaign, 2011 to 2013”[3]

“The [PRC] now presents the broadest, most active, and most persistent threat to both government and private sector networks…”
[2 p.3]

“**Russia** is particularly focused on improving its ability to target [CI], including underwater cables and [ICS], in the [US] and allied and partner countries…”
[1 p.15]

“Russia remains a persistent cyber threat as it refines its cyber espionage, attack, influence, and disinformation capabilities…”
[2 p.3]



ANNUAL THREAT ASSESSMENT
OF THE U.S. INTELLIGENCE COMMUNITY

Office of the Director of National Intelligence

February 6, 2023

NATIONAL CYBERSECURITY STRATEGY

MARCH 2023

THE WHITE HOUSE
WASHINGTON

“The governments of Iran and [North Korea] are similarly growing in their sophistication and willingness to conduct malicious activity in cyberspace.”
[2 p.3]

“**Iran**’s opportunistic approach to cyber attacks makes [CI] owners in the [US] susceptible to being targeted by Tehran, particularly when Tehran believes it must demonstrate that it can push back against the [US] in other domains.”
[1 p.19]

“**[North Korea]** probably possesses the expertise to cause temporary, limited disruptions of some [CI] networks and disrupt business networks in the [US].”
[1 p.21]

Sources:
[1] ODNI: Annual Threat Assessment of the U.S. Intelligence Community
[2] Whitehouse: National Cybersecurity Strategy 2023
[3] CISA: Alert AA21-201A

FERC Two-Pronged Approach

A DIVISION OF NERC

E-ISAC

ELECTRICITY
INFORMATION SHARING AND ANALYSIS CENTER

Office of Energy Infrastructure Security

Identify and Promote voluntary ***Best Practices*** to help Identify and Address Advanced and Targeted Threats to Key Facilities

> **“Regulations will define minimum expected cybersecurity practices or outcomes but the Administration encourages and will support further efforts by entities to exceed these requirements.“**
>
> **National Cybersecurity Strategy, March 2023**

Establish Broad Foundational Reliability and Security **Regulations**

Office of Electric Reliability

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

FERC Two-Pronged Approach (cont.)

Best Practices

Foundational Regulations

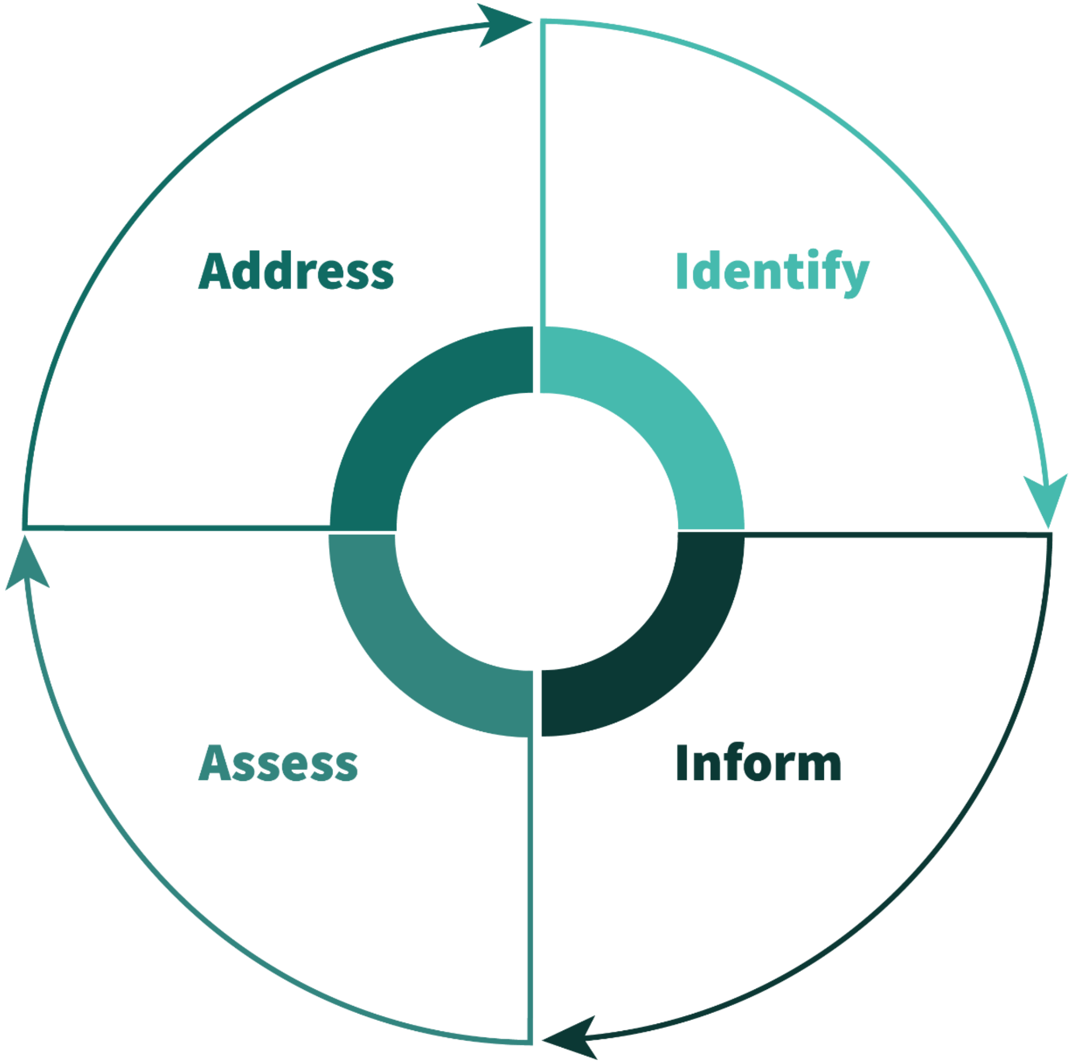
Collaborative Questions for Protective Actions

Security-Focused Discussions

1. Do you know who's targeting your utility's systems and how?

2. Do you know how to stop them?

3. Have you identified the systems that are most critical?



Examples of OEIS Initiatives

IDENTIFY INFORM ASSESS ADDRESS

- OEIS employees are **DHS PCII certified** and are participants in the **DHS CISA Central** collaborating with federal, state, and private sector subject matter experts on threats to energy infrastructure and best practices to stop them.

- OEIS staff maintains **top security clearances** to engage with our federal partners and the **state intelligence centers** to evaluate and address cyber and physical security threats to our jurisdictional energy infrastructure.

- OEIS assists in the development and implementation of United States Government policy and strategy with respect to significant cyber incidents as an active member of the National Security Council's (NSC) Cyber Response Group (CRG)

- OEIS **works collaboratively on cyber and physical security initiatives with DHS, DOE, and other agencies,** to identify processes and systems critical to protect the energy infrastructure against **threats such as those from supply chain**, **EMP events**, **and physical security substation incidents**.

- OEIS leads and participates in analyses and research efforts to better understand and address potential threats for example, working with DOE and the national laboratories to better identify the impacts of ground induced currents (GIC), and E3 currents generated from **EMP events** on the BPS.

Public

Examples of OEIS Initiatives

IDENTIFY INFORM ASSESS ADDRESS

- OEIS partners with **ODNI** to provide classified security threat **analytic exchanges** to the energy sector and state commissions using a **1-day** security clearance.
- OEIS works with **NERC and the E-ISAC** to initiate, develop, and issue **alerts** and **analyses** to the energy sector to quickly address new vulnerabilities and threats.
- **OEIS acts as a nominating authority for the DHS Private Sector Clearance Program**; helping FERC jurisdictional energy infrastructure **owners/operators** and **State Local Tribal & Territorial organizations** to be informed of relevant **classified information.**

- Where possible OEIS **works broadly** to inform industry of threats and mitigations; for example, jointly working with NERC to publish a joint papers on the **SolarWinds breach**. The paper described the ways attacks can propagate, identified the most effective tools and techniques to address this threat, consolidating multiple approaches into one resource. Also, jointly published and conducted a webinar on **Cloud Security Whitepape**r with the NATF to provide guidance to the energy sector about how this service could be **safely used.**

Examples of OEIS Initiatives

IDENTIFY INFORM ASSESS ADDRESS

- Since 2012, OEIS has conducted numerous **IT/OT Network Architecture Assessments and physical security reviews** for electric, ONG pipeline, hydroelectric, and LNG facilities with the utility subject matter experts and principals.
- OEIS assists with the planning, preparation, and organization of several **cyber and physical security tabletop exercises** such as: **Cyber Yankee** which pairs NE National Guard units with utilities to simulate cyber attack and defense, **NERC's GridEx** which simulates nationwide cyber and physical attacks on utility systems, and the interagency **FEMA-led National EMP Exercise** which assessed federal capabilities, roles, and responses to an EMP attack affecting energy infrastructure.
- OEIS has worked with other agencies including DOE, TSA, PHMSA in reviewing the interdependencies of **the natural gas system and the bulk power system including** the effects of security vulnerabilities and **contingencies.**
- OEIS is a team participant with OER, OGC, OEMR, and/or OEPI **on key FERC initiatives** providing subject matter assistance without attribution.

Public

Examples of OEIS Initiatives

IDENTIFY INFORM ASSESS **ADDRESS**

- FERC recently published a final rule providing **incentive-based rate treatment for utilities** making voluntary investments in advanced **cybersecurity technologies** as well as participation in **cybersecurity threat information sharing programs** for the benefit of consumers. Eligible cybersecurity investments include not only a **pre-qualified** list of cybersecurity investments, but also those investments that are done on a **case-by-case** basis, allowing utilities to request incentives for a variety of solutions tailored to their specific situations. The Commission will also allow utilities to seek incentives for early compliance with new cybersecurity reliability standards.

- OEIS works closely with the industry and states, developing products and services that can assist their engagements with utilities. For example, OEIS has developed a **State Regulator's Checklist**, a **Cybersecurity Incident Response List**, and an **IT Program Policy Guide** to assist both the states and industry to better secure energy infrastructure.

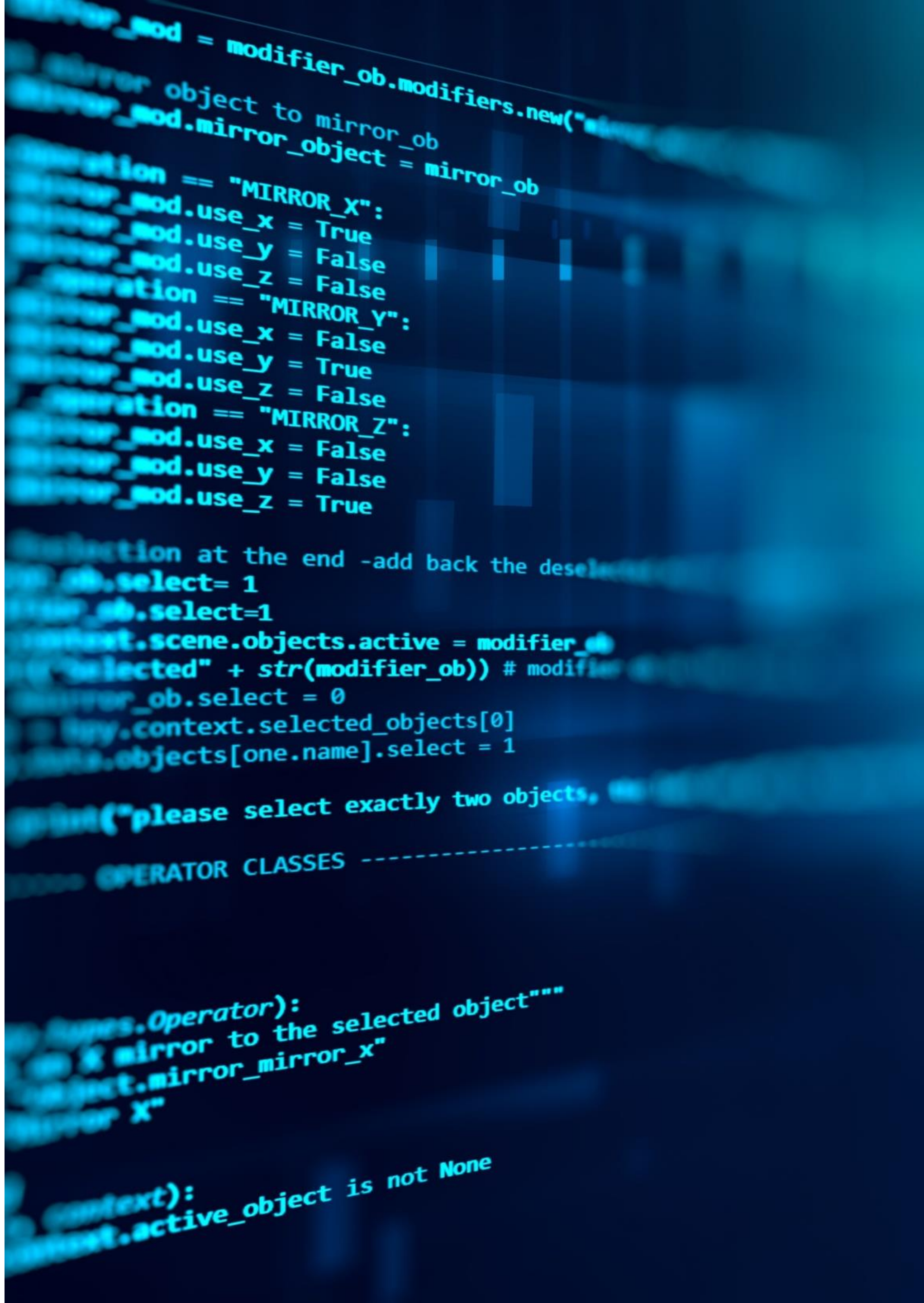
- OEIS has active in voluntary security standards for example, as a **voting participant** assisting with the draft of **API STD1164 2nd Edition cybersecurity standards** and the **DHS ICTSCRM Task Force** to develop **premier ICT supply chain strategies** for voluntary adoption by industry to help better protect energy infrastructure.

- OEIS developed a **cybersecurity 101** training program for **state regulators**; presenting it to multiple states at **four** separate regional conferences.

- OEIS works with **NERC and the E-ISAC** to initiate, develop, and issue **alerts** and **analyses** to the energy sector to quickly address new vulnerabilities and threats.

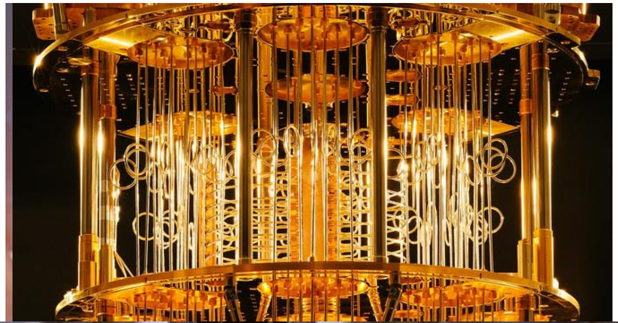
Best Cybersecurity Practices

- Phishing Prevention Training
- Jump Host Hardening
- Identity and Access Management
- Recurring Background Investigations
- Firewall Deny Log Review
- Incident Response Playbooks
- Procurement / Supply Chain
- Continuity of Operations
- Penetration Testing



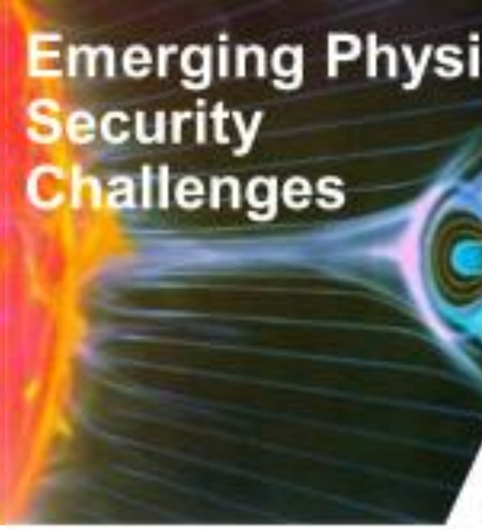
```
_mod = modifier_ob.modifiers.new("
 object to mirror_ob
_mod.mirror_object = mirror_ob
ation == "MIRROR_X":
_mod.use_x = True
_mod.use_y = False
_mod.use_z = False
ation == "MIRROR_Y":
_mod.use_x = False
_mod.use_y = True
_mod.use_z = False
ation == "MIRROR_Z":
_mod.use_x = False
_mod.use_y = False
_mod.use_z = True

tion at the end -add back the dese
_ob.select= 1
_ob.select=1
t.scene.objects.active = modifier_ob
lected" + str(modifier_ob)) # modif
_ob.select = 0
.context.selected_objects[0]
.objects[one.name].select = 1

("please select exactly two objects,

 OPERATOR CLASSES ----------------

.Operator):
 mirror to the selected object"""
t.mirror_mirror_x"
 X"

context):
t.active_object is not None
```

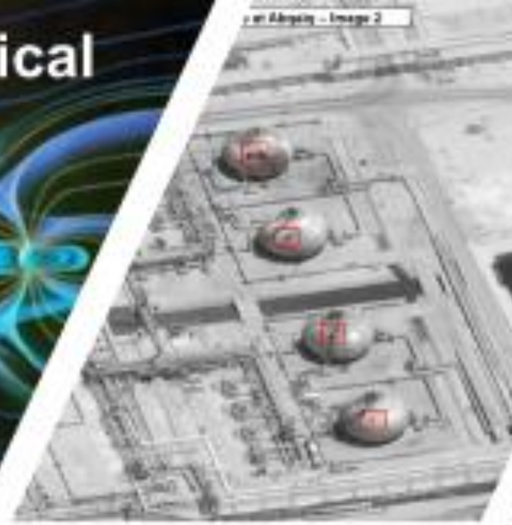
Emerging Cyber Challenges



- Quantum Computing and Cryptography
  - Threat to encryption methods
  - Threat of amplifying known attack methods
- Artificial Intelligence
  - Threat of amplifying known attack methods
  - Can also be used to amplify defense methods
- Internet of Things
  - Actors can gain access to networks and information
- Inverter-Based Resources
  - Introduces expanded attack surface
  - Changing resource mix introduces challenges

Emerging Physical Security Challenges





- Ballistic attacks inside and outside the substation perimeter
- Attacks on control buildings
- Miscellaneous attacks and theft
- Damage to both overhead and underground conductors
- Intrusions without damage and drone flyovers
- Emerging threats…

OEIS Engagement Programs for Physical Security

- Short, medium, and long-term physical security mitigation measures; P2R2 – prevention, protection, response, recovery
- Site visits and walk-down assessments
- Spare equipment recommendations
- Pre-planning, recovery, and restoration recommendations
- Mitigation measures to address new and multi-faceted attacks

PHYSICAL SECURITY

Questions ??

- Contact Information
  - Joe McClelland
  - **<email> joseph.mcclelland@ferc.gov**

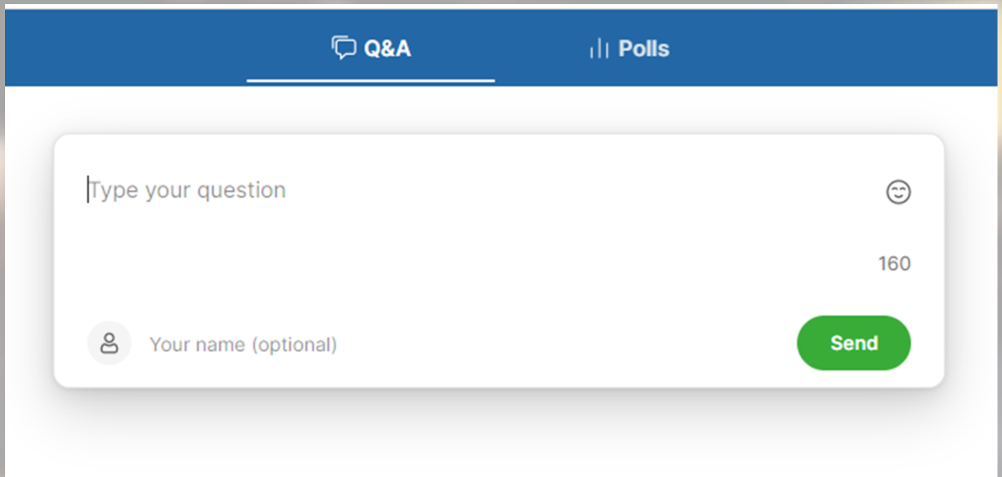
STANDARDS, SECURITY, & RELIABILITY FALL WORKSHOP

Fall Standards, Security, & Reliability Workshop

Return at: 10:40 a.m.

- New BCSI in the Cloud Standards
- FERC Vulnerability and Physical Security Assessment Program
- **New Weatherization Requirements**
- Emerging Cyber and Physical Risks
- Entity Ownership Change Considerations
- Cyber Informed Transmission Planning
- Change Management Controls
- Emerging Issues with Distributed Energy Resources
- Grid Forming Inverter Technology: Opportunities for a Changing Grid

To submit questions during the workshop, please visit **slido.com** and enter today's participant code: **TXRE**



NPCC, Inc.

NPCC Cold Weather Standards and Good Practices

Matt Forrest

Senior O&P Entity Risk Engineer

10/02/2023

Order 182 FERC 61,094

- “It is essential to the reliable operation of the Bulk-Power System to ensure enough generating units will be available during the next cold weather event.” As the November 2021 Report found, the Bulk-Power System “cannot operate reliably without adequate generation. When cold weather events such as Winter Storm Uri occur, with “massive numbers of generating units” failing, grid operators could have no other option than to shed firm customer load to prevent uncontrolled load shedding and cascading outages. And as unfortunately illustrated by Winter Storm Uri, “these firm load shedding events . . . have very real human consequences. Millions went without heat . . . Hundreds died from hypothermia.”

Agenda

- Brief History and most recent events
- Recent Cold Weather Events and Activities
- 2021 Winter Storm Uri
- Resulting Reliability Standards (1st Set)
- 2019 and Later
- Resulting Reliability Standards (2nd Set)
- Cold Weather Standards Under Development
- Cold Weather Good Practices
- Equipment Visuals
- Summary

Brief History

- 2011 – 29,700MW
- 2014 – 19,500MW
- 2018 – 15,800 MW
- 2021 – 61,300 MW
- 2022 – 90,500 MW

- MW values each year represent the incremental coincident unplanned generation outages.

February 2021 Winter Storm Uri

- 1,045 individual BES generating units with multiple failures.

- The Electric Reliability Council of Texas (ERCOT) averaged 34,000 MW of generation unavailability over two consecutive days, from 7:00 a.m. February 15 to 1:00 p.m. February 17, equivalent to nearly half of its all-time winter peak electric load of 69,871 MW.

- Combined 23,418 MW of manual firm load shed.

- More than 4.5 million people in Texas lost power during the Event, and some went without power for as long as four days, while exposed to below-freezing temperatures for over six days.

- At least 210 deaths.

Cold Weather Standards: First Set

Project 2019-06, The South-Central United States Cold Weather Bulk Electronic System Event of January 17, 2018

- The GO plans and procedures must include at a minimum;
  - Necessary and appropriate freeze protection measures,
  - Annual maintenance and inspection of such measures,
  - Generating unit limitations
    - Accurate ambient temperature design specifications
    - Fuel capability and switching capability and concerns
    - Expected performance in cold weather
  - Identify trainer and complete training for individuals responsible for implementing the above plan

Cold Weather Standards Continued Development

- On October 28, 2022, NERC sought FERC approval of EOP-011-3 and EOP-012-2
  - Consistent with key recommendations for standards improvement from “The February 2021 Cold Weather Outages in Texas and the South Central United States” Report (Uri)
    - Implementation of freeze protection measures
    - Enhanced weather preparedness plans
    - Annual training
    - Coordination of manual and automatic load shed
- In the meantime, cold weather event Elliot occurred in December 2022

December 2022, Winter Storm Elliot

- Ongoing review of event but here’s what we know
    - Load shed events in North Carolina and Tennessee
    - Significant load forecasting errors
    - Generation fleet failures, outages and derates
    - Natural gas issues
    - Insufficient reserves

December 2022, Winter Storm Elliot

- Outages adding to 90,500MW coincided with winter peak electricity demands
- 80% occurred at temperatures above the documented minimum operating temperatures
- 1,702 individual generating units
  - Experienced 3,565 outages, derates, or failures to start
  - 825 units were natural gas-fired generators
  - Combination of equipment freezing and fuel supply issues
  - 55 percent of the generating unit outages, derates, and failures to start, were caused by:
    - Freezing Issues - 31%
    - Fuel Issues - 24% (20% of those fuel issues were gas related)

December 2022, Winter Storm Elliot

- Record 13% of Eastern Interconnect capacity failed in Winter Storm Elliott

- Although most of these outages were due to weather impacts on electric distribution facilities operated by local utilities, utilities in parts of the southeast were forced to engage in rolling blackouts and the bulk power system in other regions was significantly stressed.

NERC Level 3 Alert – 2023

- Reiterated cold weather plan requirements
- Identify cold weather critical components
- Published the definition of Cold Weather Reliability Event
- Determine plant capability and upgrades needed to operate at the ECWT
- Identify causes of plant issues due to cold in 2022-2023
- Determine and provide ECWT to RC, BA, TOP and determine which plants are capable in current configuration
- Provide expected available MW to BA and TOP

FERC Order Issued February 16, 2023

- Approved Extreme Cold Weather Reliability Standards EOP-011-3 and EOP-012-1
- Directs NERC to modify Reliability Standard EOP-012-1 to ensure that it captures all bulk electric system generation resources needed for reliable operation and excludes only those generation resources not relied upon during freezing conditions.
- Directs NERC to clarify the language of the applicability section to align with NERC's explanation of the entities that should already be preparing to comply with the Standard and should not need additional implementation time.
- Directs NERC to develop and submit modifications to Reliability Standard EOP-012-1 Requirements R1 and R7 to address concerns related to the ambiguity of generator-defined declarations of technical, commercial, or operational constraints that exempt a generator owner from implementing the appropriate freeze protection measures.

WINTER PLAN KEY CONSIDERATIONS

- Compartmentalize plans around systems or similar systems.
  - Prioritize work orders
    - Consider a cold weather code
    - Ensure work is scheduled to complete prior to a specific date.

  - Keep a winterization items list year-round.

  - Ensure vendors are available and scheduled.

  - Ensure personnel are trained and refresh as needed.

WINTER PLAN KEY CONSIDERATIONS

- Prioritize based on equipment that has the potential to:
  - Cause unit trip or partial outages and derates
  - Impact unit start-up or restart or impact plant monitoring and control
  - Cause equipment or plant damage
  - Adversely impact the environment
  - Cause fuel disruption
  - Reduce plant safety

WINTER PLAN KEY CONSIDERATIONS

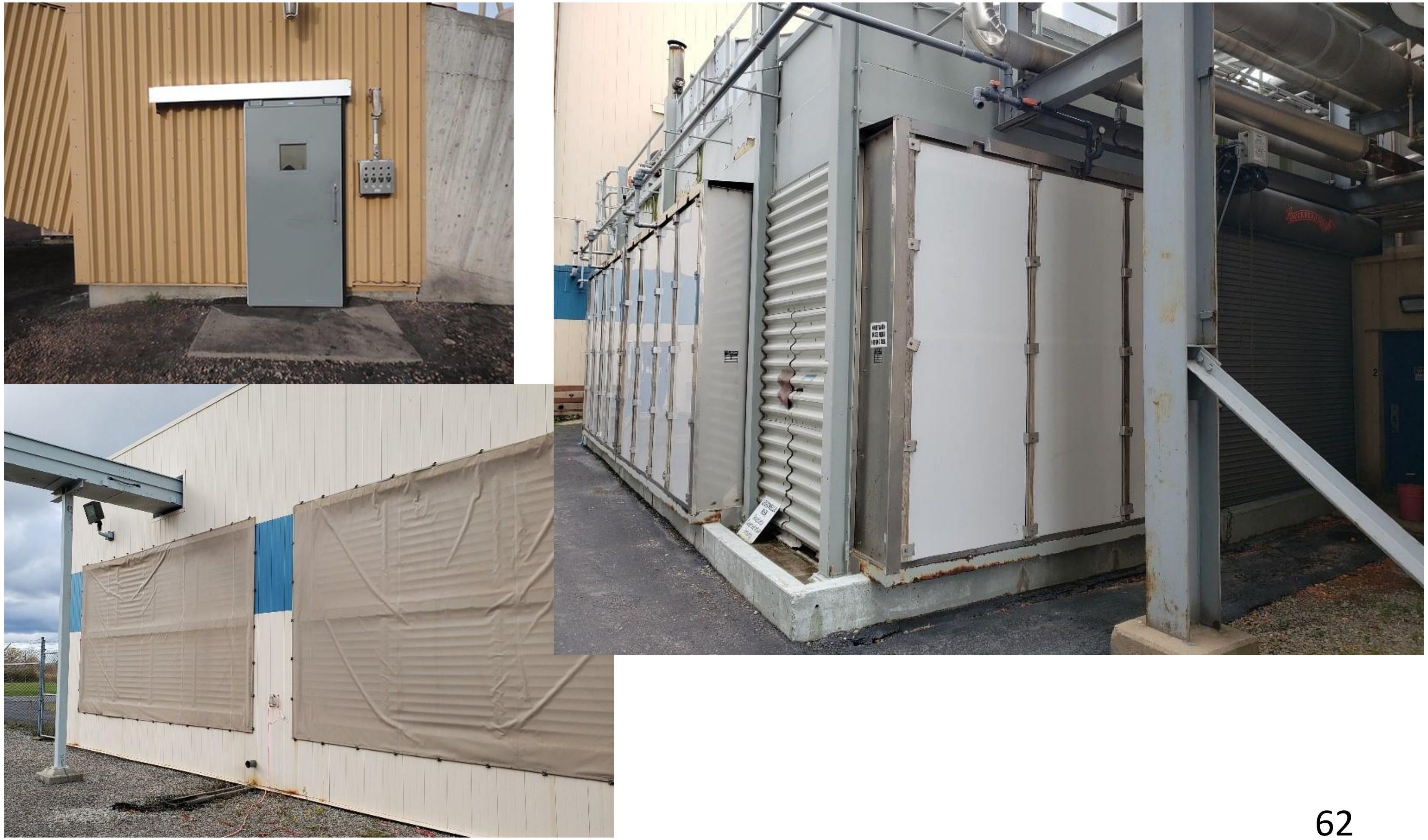
- Developing a plan - Prioritize your review and preparation
  - Building doors, Building Louvers, Building Heat, GT intake, and boiler stack area
  - External Piping, insulation, traps, and heat trace
  - Vital instrumentation
  - Fuel Supply
  - Plant cooling basins, tank heat – top off tanks
  - Main plant condensate, feed, and boiler system, aux boiler
  - Emergency Generator and fuel supply, key loads
  - Station service power
  - Other systems – instrument air, fire protection, water treatment
  - Lessons learned from prior winter events. Corrective Action Plans, Mitigation results, Extent of condition

Cold Weather Preparation – Good Practices

- Winter Preparation Maintenance Practices
  - Entity should implement seasonal inspection and maintenance program
    - Establishes equipment, processes, and due dates
  - Entity should create winter work order prioritization code
    - Tracks all winter items, creates completion percentage reports or walk-down lists
  - Establish an early deadline for completion of winter deficiency items. Don’t wait until the last minute
  - Prioritize work on systems and equipment needed to cope with winter conditions
    - Heat trace, insulation, installation of temporary heaters and other cold weather protection measures.
    - Vendors!!!

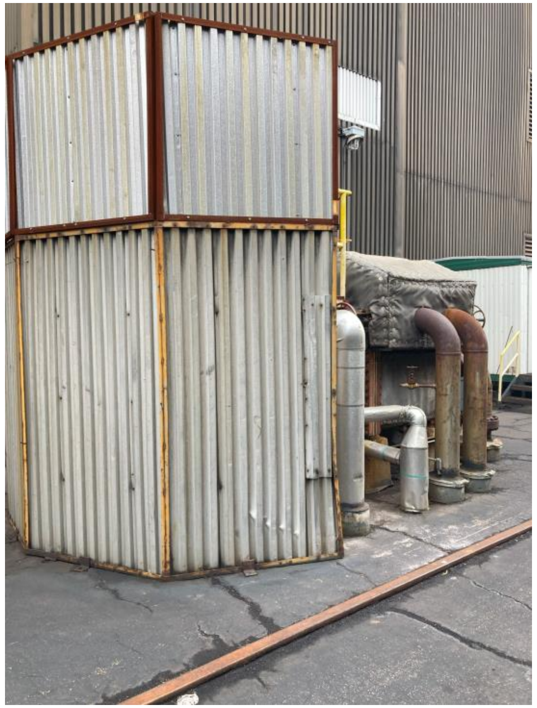
GOOD PRACTICES – Buildings, Doors, Louvers

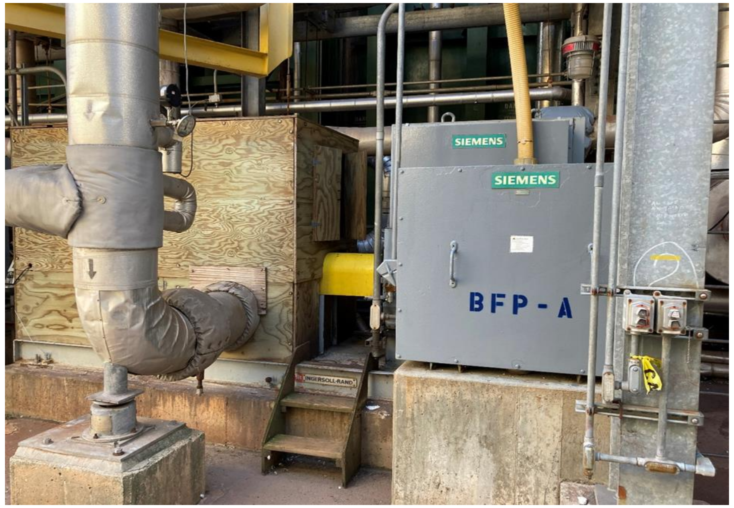
- Building doors and louvers and installed heat are the first line of defense
- Panels and other equipment doors\louvers
  - GT Inlet Filter (High Density Poly Panels)



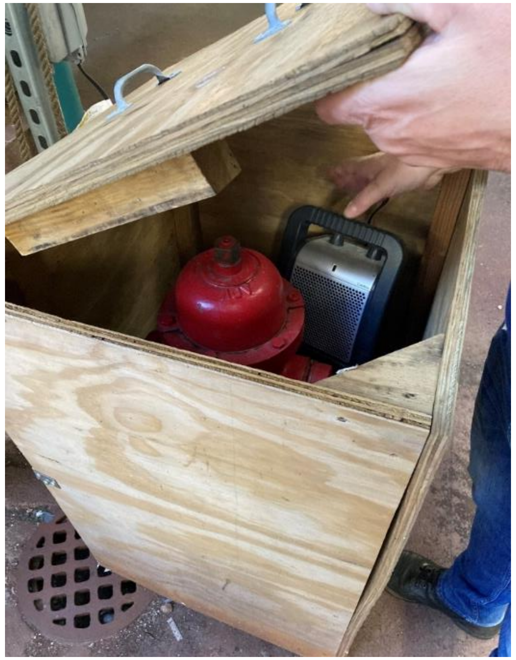
Good Practices - External Equipment Protection

- Inexpensive wind blocks



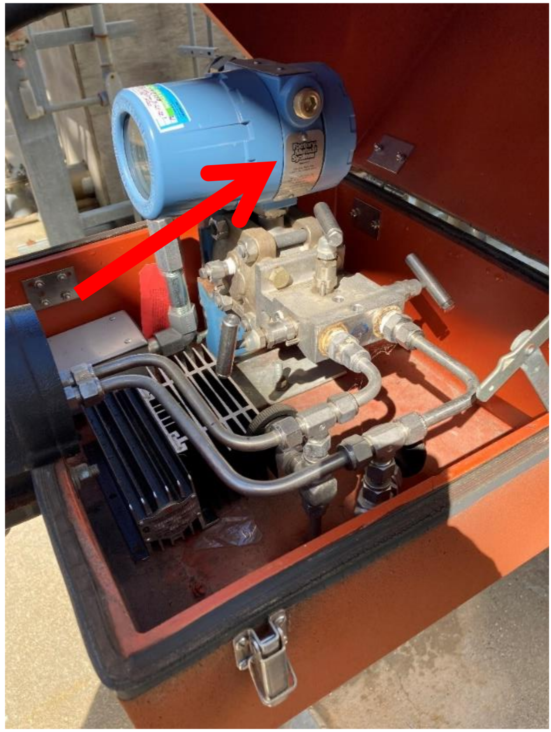


Fabricated Wood Enclosure (May include heat strips or lamps)

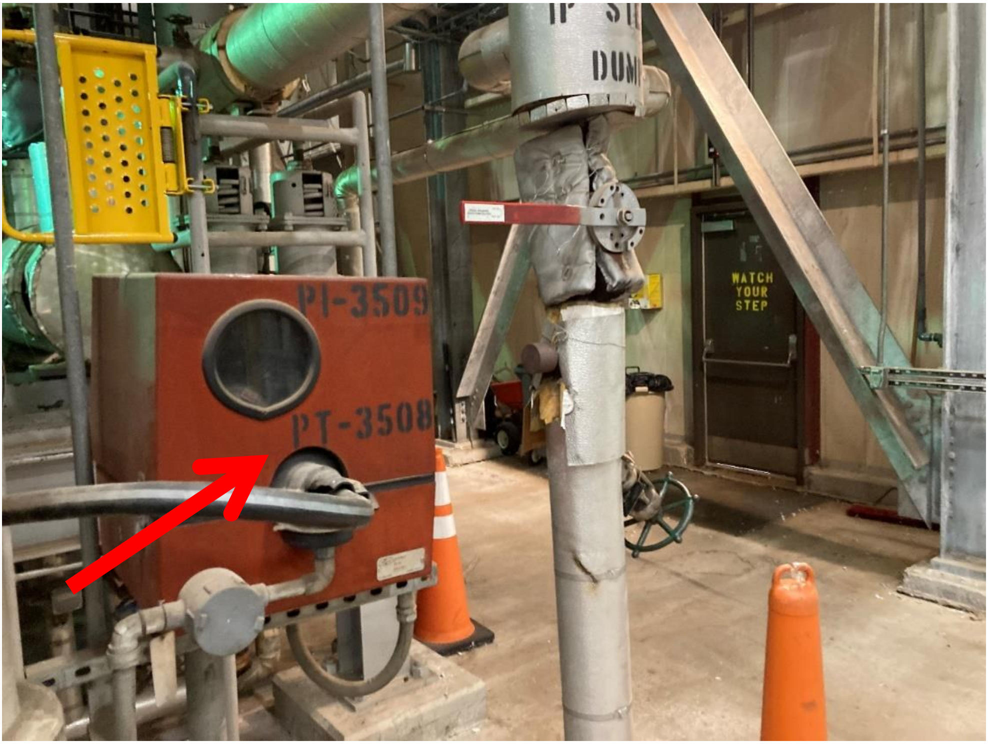


Good Practices - External Equipment Protection

- Heated Enclosure (O'Brien Boxes) for vital instruments



Pressure Transmitter



Heated Pressure Transmitter Enclosure

Good Practices – temporary equipment

- Protective Measures: Pre-staged temporary heaters in areas known to be susceptible to low temperatures

GOOD PRACTICES - Fuel

- Fuel storage and plant run duration on that fuel
- Fuel delivery capability, fuel curtailment likelihood
- Fuel weather protection
  - Heat trace, electric or steam (limitations on each)
  - Bunkering capabilities for solid fuel
- Fuel Switching
  - Manual or auto
    - Is manual on the fly or does it need to be done with plant offline?
  - Support systems needed (DM, Service Air, other)

Cold Weather Preparation – Good Practices

- Plant Operator Rounds and Inspection
  - Perform additional checks during winter months
  - Check single failure equipment and understand plant trip criteria
  - Recruit engineers\maintenance to assist looking for vulnerabilities
  - Monitor Area Temperatures and temporary winter protection
  - Verify building penetrations close and seal properly
  - Look for damaged or missing insulation
  - Utilize IR gun and understand key locations and systems to monitor
  - Verify heat trace functionality and steam trap functionality
  - Maintain list of deficiencies that require additional contingencies
    - Eg: failed steam trap or air receiver required frequent blow down

Good Practices – Rounds and Monitoring

- Provide tools to the operators and plant personnel to assist in monitoring
  - Infrared technology
  - Area temperature indication
  - Equipment specific rounds sheets with high and low limits.
    - Consider Cold Weather Specific Rounds that limit what is checked but increased frequency.
  - Add specific cold weather monitoring points to PI displays.

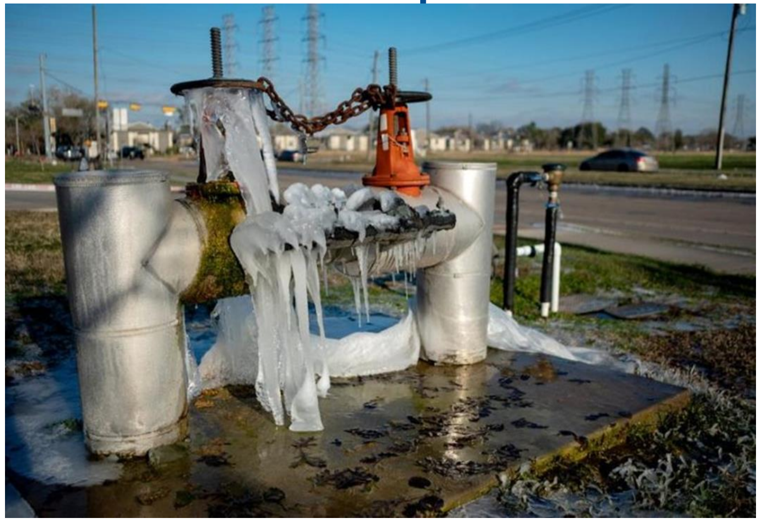
Good Practices – Rounds and Monitoring

- Pair new operators with experienced operators on rounds.
  - Go out in the plant and assume there are discrepancies to find.

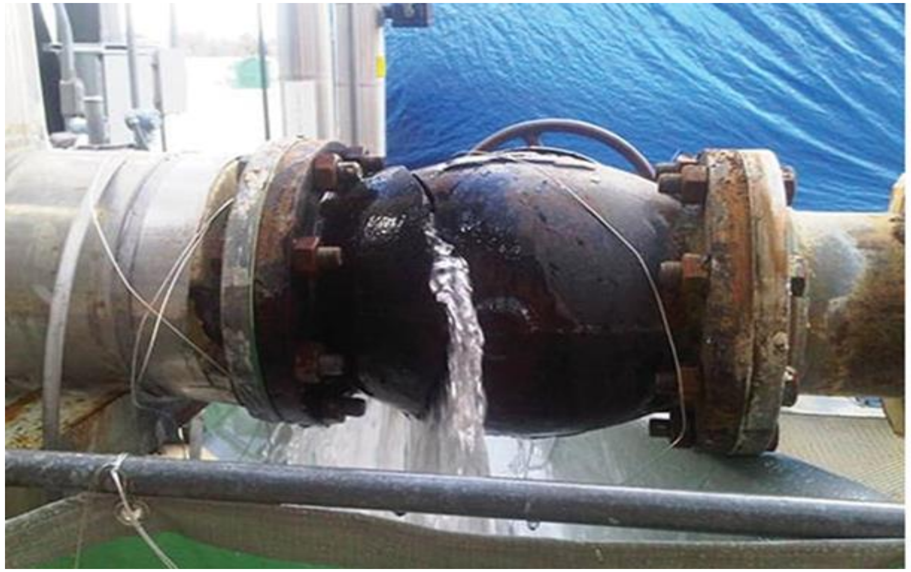
- Teach field operators where plant critical components and instruments are located.
  - Transmitters
  - Steam Traps
  - Known prior trouble areas.
  - Air cooled condensers

Good Practices – Rounds and Monitoring

- Plant Operator Rounds and Inspection (continued)
  - Observe and document deficiencies. Set priority to ensure plant systems are not compromised



Valve Packing Leak



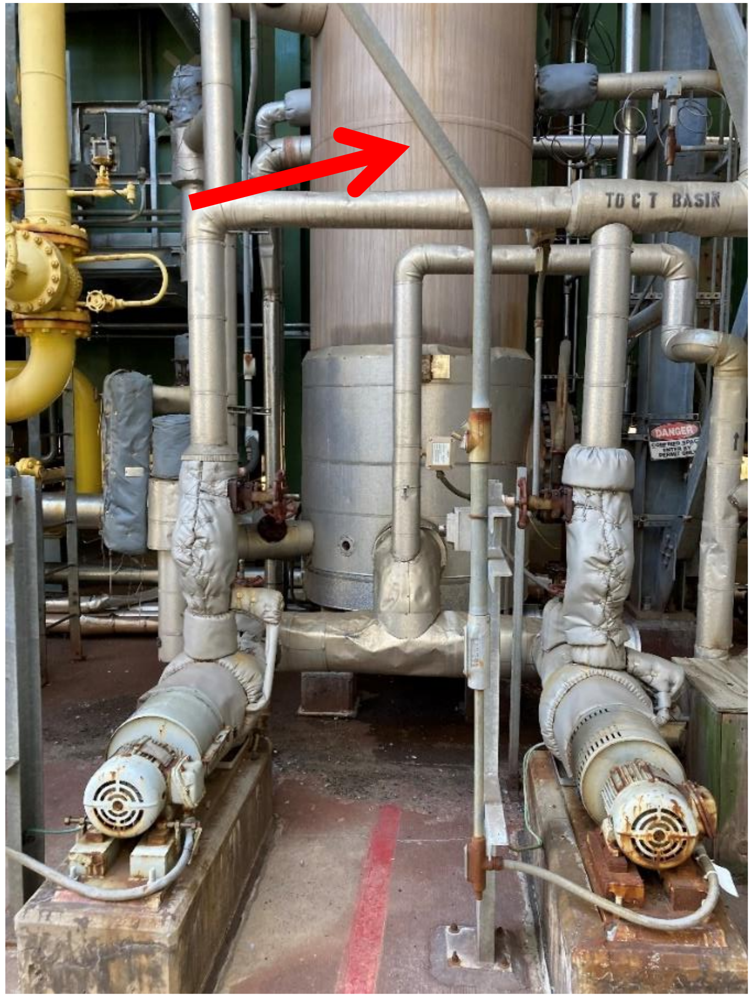
Valve failure due to missing insulation and heat trace

Good Practices Rounds and Monitoring

- Keep high priority areas clear
- Inspect cabinet door seals

Good Practices - Increased Monitoring

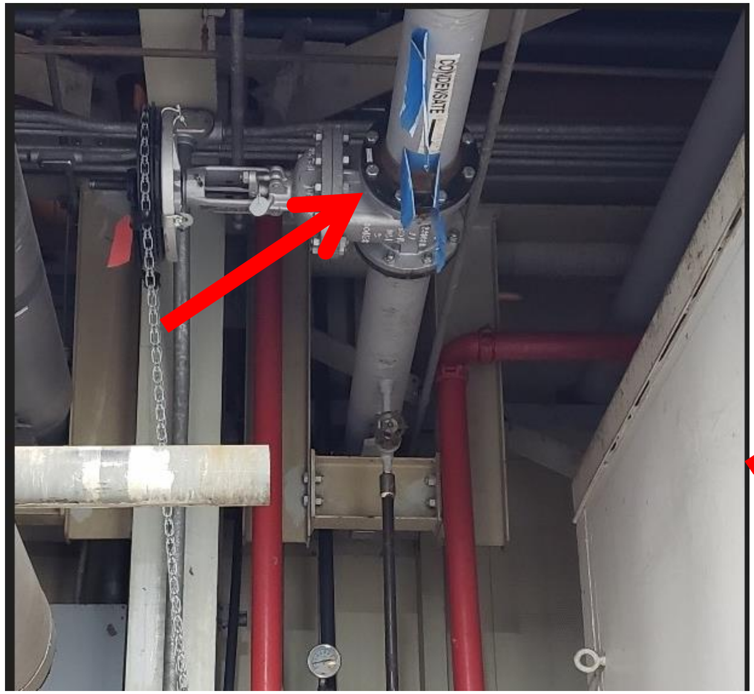
- The down comer is periodically drained until warm water flows from the drain

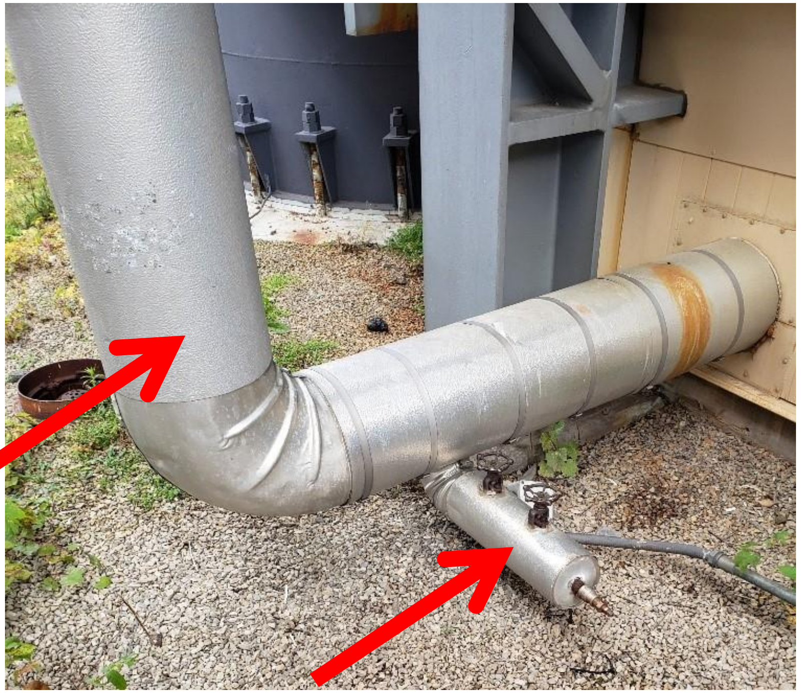


Good Practices – Plant Reconfiguration

- Utilize existing isolation valves and drains to protect external piping

Piping can be isolated inside so only a small segment requires draining.

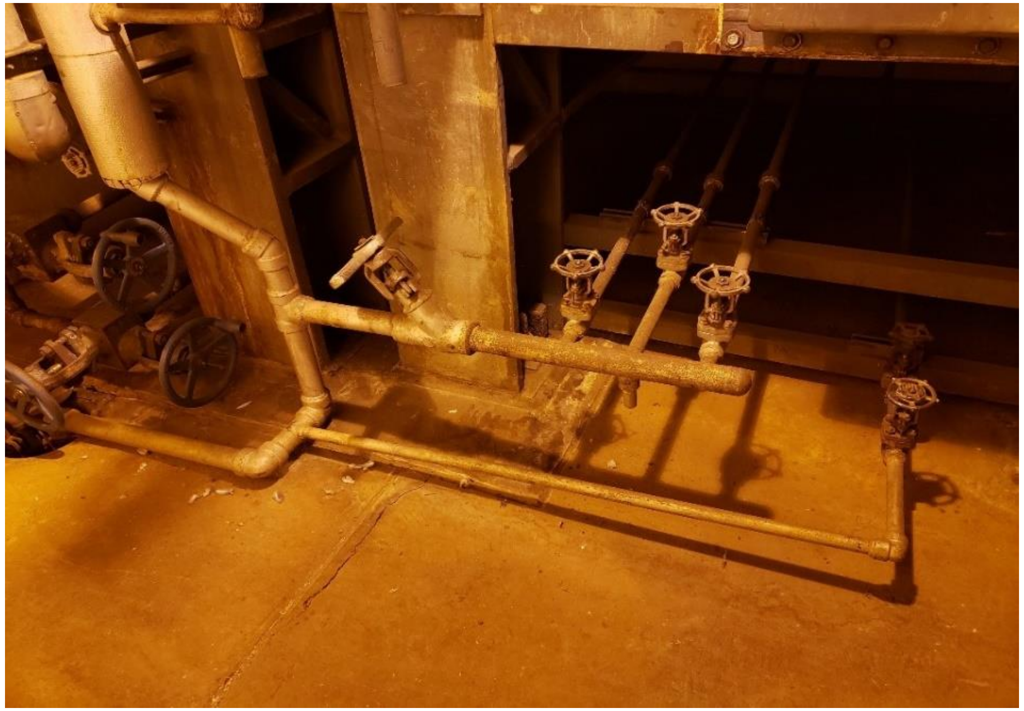




Good Practices – Plant Reconfiguration

- Use Existing Plant Equipment or Systems

Offline Boiler Recirculation Pump



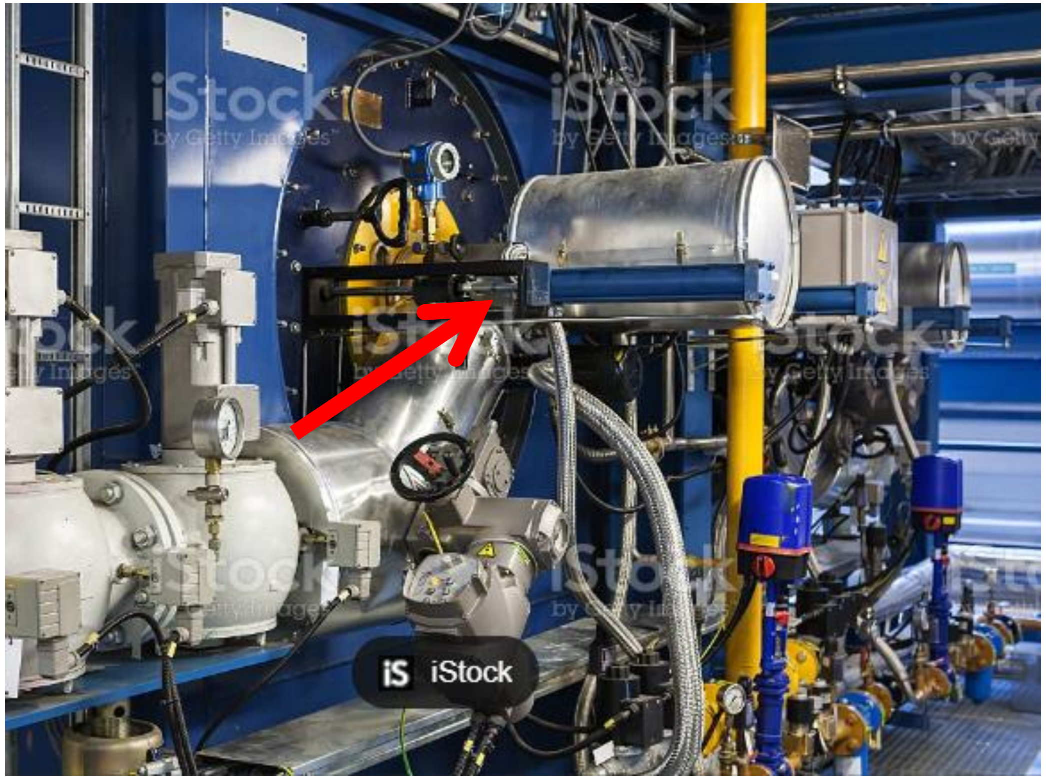
High Pressure Economizer Drain

Good Practices – Repurpose Equipment

- Electric Aux Boiler can be used for more than building heat.
- Use for Steam Seals
- Steam Drum Sparging
- DA tank heating
- Possible connection to small aux generator

Good Practices – Plant Low and No-Load Ops

- Use Existing Plant Equipment or Systems
  - Utilize a low load single burner as a keep warm method

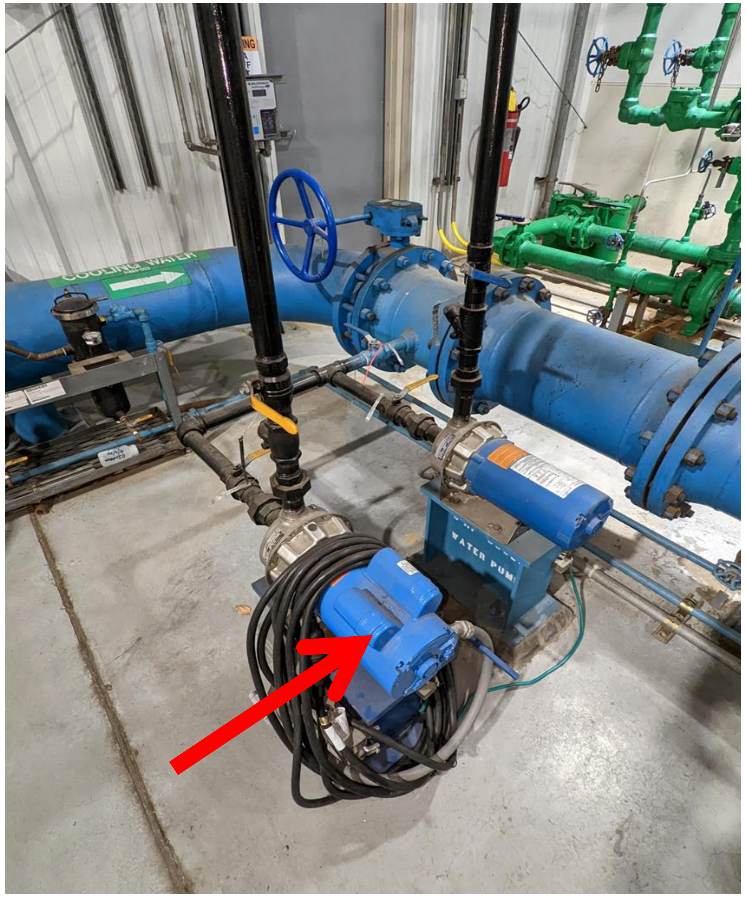


Good Practices – Establish Contingencies

- Taking Manual Control to prevent plant trip
  - Know what vital transmitters affect control and plant trip
  - Operators should immediately recognize control system deviations and be able to correct manually while component troubleshooting occurs
    - Remote manual
    - Local manual
- Total Loss of Offsite power
  - How long can systems remain filled with no heat or circulation?
  - Know what systems need to be drained and when
  - Know how long refill and restart will take from cold plant to sync

Good Practices – Establish Contingencies

- Take advantage of current piping and flow path options for contingency equipment
  - Not all modifications need to break the bank or require extensive work



Additional Considerations

- Utilize ideas from field personnel, don’t plan in a silo
- Take advantage of affiliates and industry forums
  - North American Generator Forum
  - North American Transmission Forum
- Annual cold weather plan, maintenance program, operator awareness, and corrective action program
  - Training, training, more training
  - Improve CW Plan each year

Recap of GO\GOP Recommendations

- Five GO\GOP related recommendations from Project 2021-07 Extreme CW Grid Operations, Preparedness, and Coordination
  - GO are to identify and protect cold-weather-critical components and systems for each generating unit
  - GO are to design new or retrofit existing generating units to operate to a specified ambient temperature and weather conditions
  - GO and GOP are to conduct annual unit-specific cold weather preparedness plan training
  - GO that experience outages, failures to start, or derates due to freezing are to review the generating unit’s outage, failure to start, or derate and develop and implement a corrective action plan for the identified equipment and evaluate whether the plan applies to similar equipment for its other generating units
  - GO are to account for the effects of precipitation and accelerated cooling effect of wind when providing temperature data

Resource Documents

[2019-06 SDT Responses]

[2019-06 Project Page]

[ERO Enterprise CMEP Practice Guide Cold Weather Preparedness]

[Major Events Reports]

[Lessons Learned]

[Reliability and Security Guidelines]

[Generating Unit Winter Weather Readiness]

https://www.ferc.gov/media/february-2021-cold-weather-outages-texas-and-south-central-united-states-ferc-nerc-and

[Presentation | FERC-NERC-Regional Entity Joint Inquiry Into Winter Storm Elliott | Federal Energy Regulatory Commission]

Wind Turbine Cold Weather Challenges and Coping Strategies

Matt Forrest

Senior O&P Risk Assessment Engineer

October, 2023

NPCC, Inc.

Wind Turbine Unique Challenges

- Multiple generators (often hundreds) across a single site
- Routine maintenance is usually performed under warranty contract by OEMs and often consists of annual and semi-annual work orders. Cold weather preparation is often spread out across the year vs performed seasonally
- Wind sites have limited power sources to provide station service
- Wind turbines can be adversely impacted by precipitation prior to reaching cold weather interlock setpoints

Challenges – Multiple Generators

- If there are cold weather mitigation efforts that require a seasonal effort, this challenges wind sites to prioritize manpower to focus on the completion of the mitigating efforts vs responding to faulted turbines or other site projects
- Seasonal efforts such as installation of insulating blankets, disconnecting damper linkages, plugging in temporary heaters require dedicated time and crews for each machine
- When turbines fault due to any circumstances that impact an entire feeder string or the site, each turbine and its systems need to be assessed and brought back online individually

Challenges – OEM Maintenance Intervals

- Cold weather preparation items are interspersed with other routine maintenance work orders and are usually not tracked by individual work orders or cold weather/seasonal labels

- Though it is likely that all cold weather mitigation that is included in routine maintenance is covered, it is difficult for the turbine owners to track and plan specific cold weather items

Challenges – Limited Station Service

- This challenge ties in with the challenge of multiple, often hundreds of individual generators
- Wind sites do not always have a separate station service the backs up the back-feed for house power from the main gen lead line(s)
- Even if sites do have a separate station service line, the line may only accommodate admin power and not be sufficient to provide up to 5–7 MW of turbine auxiliary power
- Lower voltage station service lines are often lost due to inclement weather before the loss of the main gen lead which leaves that station in a total loss of offsite power

Challenges – Limited Station Service cnt'd

- Without power it is difficult to properly diagnose individual turbine faults
  - Not all turbines will share the same faults or have faults that fit into a remote reset category when offsite power is restored
  - This issues, combined with the multiple individual generators does not facilitate rapid restoration of the site
- Even after power is restored, turbines require time for heaters to return lubricating oil, hydraulic fluid, and generator windings to a point that permissives for turbine operation can be met

Challenges - Precipitation

- Turbine blade icing
  - At a minimum icing distorts the blade lifting surface and diminishes turbine output as a result
  - Can add additional load to bearings
  - Requires operator action to secure turbines until icing is shed
    - Verification of ice shedding is required to be local at the turbine
    - Shedding may take days or weeks

Challenges - Precipitation

- Frost and freezing fog:
  - Can lead to icing
  - Clogs filters which can cause turbines to fault on high temperature due to lack of air flow

Automatic Functions Limitations

- Though turbines do have low and high temperature limits and automatic faults that are activated when those limits are reached, other weather-related issues impact turbine generation before the setpoint limits are reached
- Turbines will fault on low temperature or high wind speed but will often have automatic resets and restart after a nominal setpoint deadband
- Blade icing algorithms
  - Alerts operators that operator action may be required to attempt to limit additional icing
  - Actuates automatic anti icing protocols on some turbines

Operator Intervention and Mitigating Strategies

- In anticipation of severe cold weather, wind farm operators can implement strategies to try to increase their availability
  - Wind sites may opt to secure turbines during precipitation events that may lead or accompany extended cold weather periods. This limits potential blade icing which is exacerbated by the blades moving and being more active in collecting ice buildup
  - As a result of keeping turbines offline during precipitation and prior to extended or extreme cold weather, a wind site may then be made more available to mitigate grid needs

Wind Conclusions

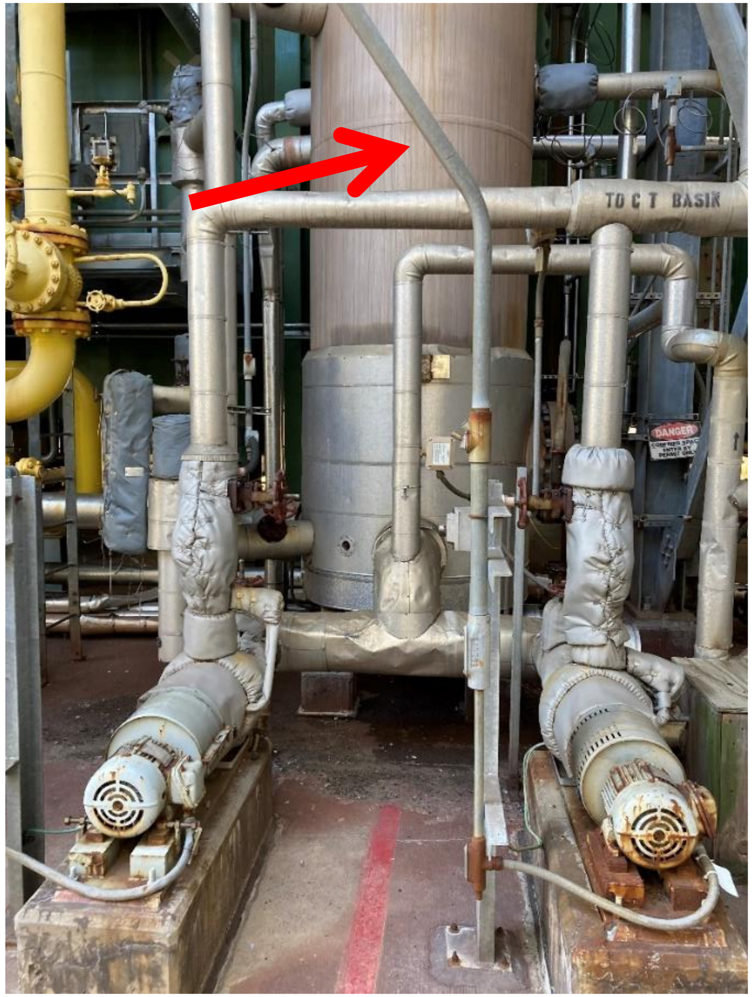
- Wind facilities have unique challenges that drive alternate cold weather and precipitation measures
- A combination of automatic interlocks and permissives, operator actions, and mitigating operating plans is required to help increase reliability and availability during cold weather periods

Questions and Answers

APPENDIX – ADDITIONAL PHOTOS

Good Practices - Increased Monitoring and Operator Action

- The down comer is periodically drained until warm water flows from the drain



Cold Weather Preparation – Good Practices

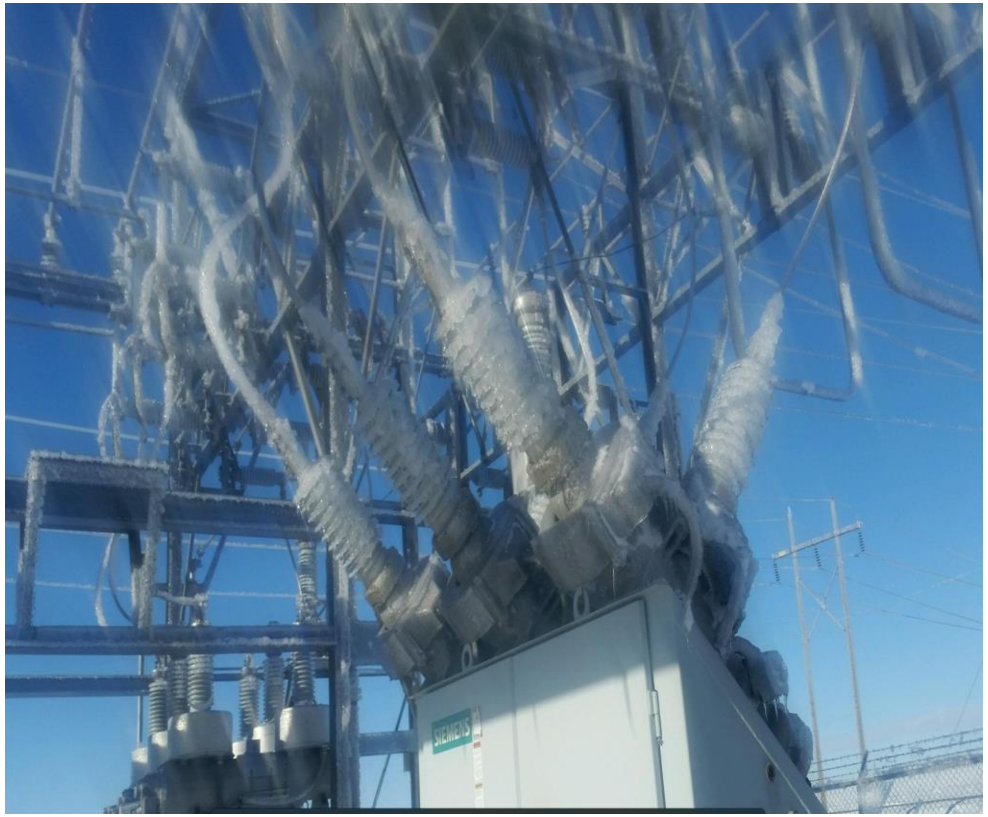
- Verify the operability of tank heating systems
- Keep tanks full and warm to increase “thermal inertia” in your favor
- Ensure that temporary water treatment trailers are winterized to ensure a continued make-up water source.

Cold Weather Preparation – Good Practices

- Vital Equipment and Instrumentation
  - Cover and heat exposed instrument racks

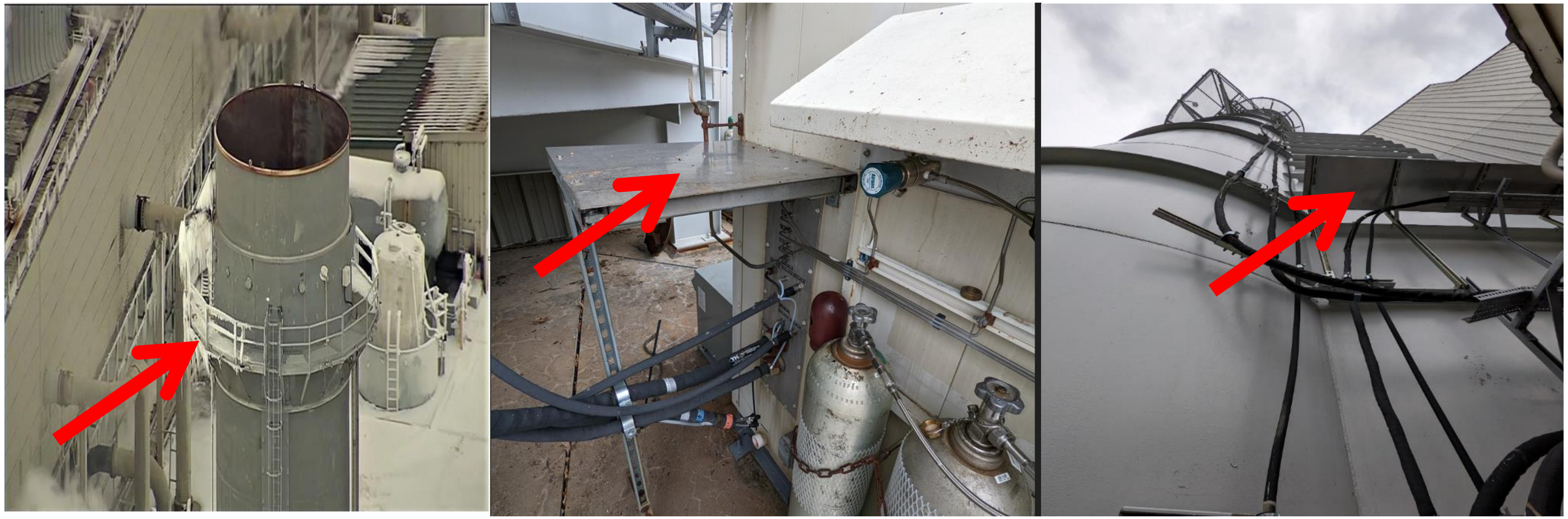
Cold Weather Preparation – Good Practices

- Snow and Ice Considerations
  - Cause multitude of problems in power block and substation
  - Cause short circuits on insulators resulting in loss of offsite power sources.



Frozen insulators can short equipment

Cold Weather Preparation – Good Practices



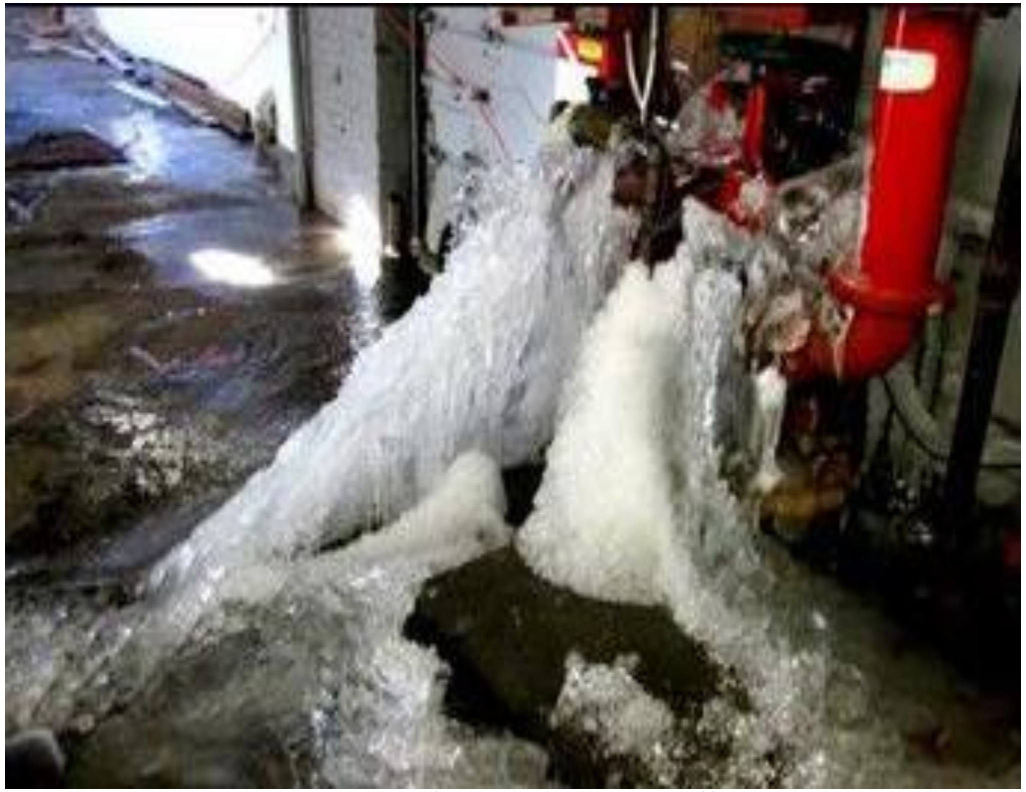
Shrouds installed to prevent falling ice damage

Snow and Ice Considerations

- Falling ice can cause equipment damage or personnel injury

Cold Weather Preparation – Good Practices

- Other Considerations



Frozen Fire Protection in unheated stair well

Cold Weather Preparation – Good Practices

E-ISAC
ELECTRICITY
INFORMATION SHARING AND ANALYSIS CENTER

Emerging Cyber & Physical Risks

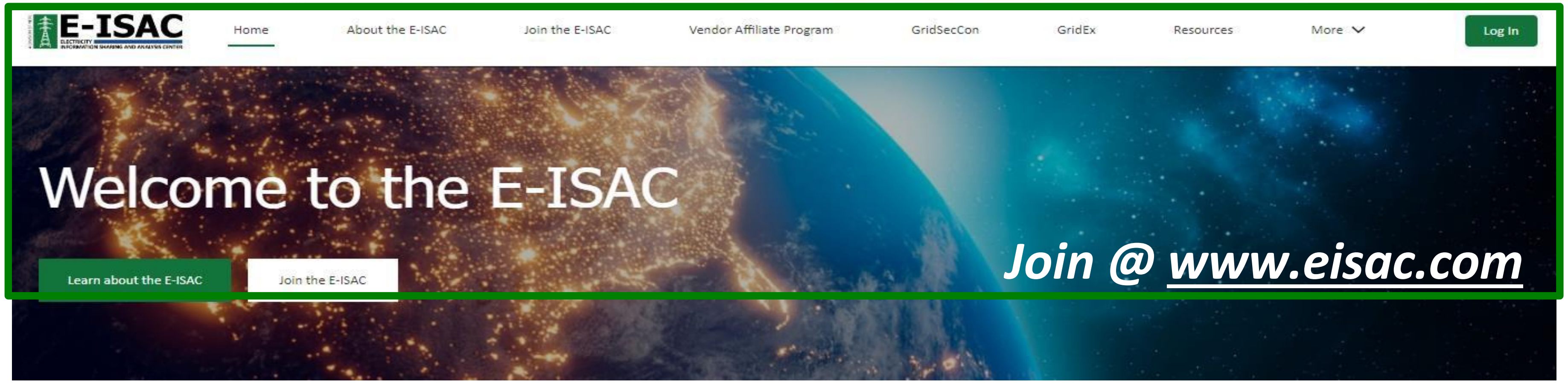
Texas RE Fall Standards, Security, and Reliability Workshop

Tyler Tiller, Security Advisor, E-ISAC
October 25, 2023

TLP: CLEAR

RESILIENCY | RELIABILITY | SECURITY

E-ISAC Products & Services



Welcome to the E-ISAC

Join @ www.eisac.com

- All-Points Bulletins
- Cyber Threat Intel Reports
- Small and Medium Utility Report
- Cybersecurity Risk Information
- Sharing Program (CRISP)
- GridEx VII & GridSecCon
- 24/7 Monitoring dark web, social media, member reports
- Physical Security Threat Reports and Resource Guide
- Vendor Affiliate Program
- Cross-sector sharing via ISACs

Thank you for sharing!

General Physical Threat Environment

DHS Homeland Threat Assessment 2024

- …the threat of violence from individuals radicalized in the US will remain high… marked by lone offenders or small group attacks that occur with little warning.
- DVEs and criminal actors with unclear motivations are increasingly calling for and carrying out physical attacks against critical infrastructure, particularly the energy sector.
  - DVEs see such attacks as a means to advance their ideologies and achieve their sociopolitical goals.
- DVEs, particularly RMVEs promoting accelerationism—an ideology that seeks to destabilize society and trigger a race war—have encouraged mobilization against lifeline and other critical functions, including attacks against the energy, communications, and public health sectors.
- Unidentified actors have attacked electric cooling components, substations, and transformers, though the impact on the energy sector’s ability to provide localized services has been minimal.

Physical Response

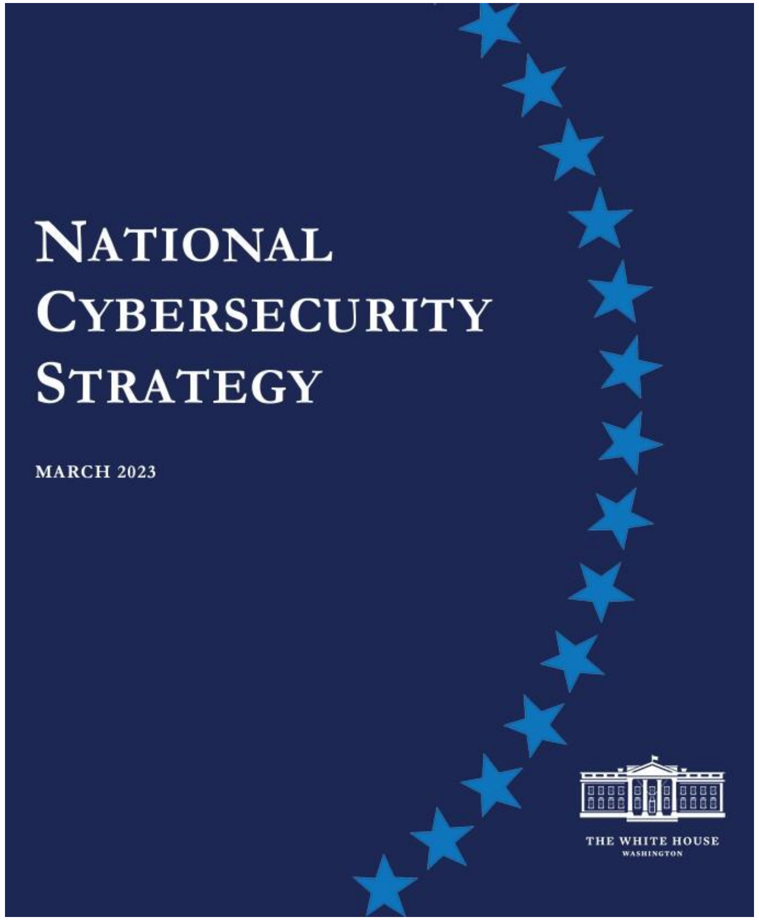
- **Regular engagement with members, partners, and stakeholders**
  - Intelligence community classified briefings
  - Cross-sector collaboration
  - Threat assessments
  - Physical security roadshows

- **E-ISAC mitigation tools and resources**
  - Physical Security Resource and Risk Management Guide
  - Identifying Possible Avenues of Approach and Firing Positions at Substations
  - Online Threat Monitoring Report
  - Drone Detection Pilot
  - White Papers (UAS, Copper Theft, and Wind Farm Security)
  - Design Basis Threat and VISA Workshops

National Cybersecurity Strategy

Five Pillars

1. Defend Critical Infrastructure
2. Disrupt and Dismantle Threat Actors
3. Shape Market Forces to Drive Security and Resilience
4. Invest in a Resilient Future
5. Forge International Partnerships to Pursue Shared Goals



NATIONAL CYBERSECURITY STRATEGY

MARCH 2023

THE WHITE HOUSE
WASHINGTON

Cyber Threats – Nation State

China

- Broadest, most active, and persistent cyber espionage threat
- “Volt Typhoon” targeting U.S. utility and other critical infrastructure sectors
- “Redfly” compromised the grid of an Asian country with ShadowPad malware
- Continued exploitation of MS Cloud, Citrix, Fortinet, VMware, Log4j vulnerabilities
- Improved tradecraft and evasion techniques

Russia

- Remains a top cyber threat for espionage, influence, and attack
- Focusing on offensive ICS capabilities

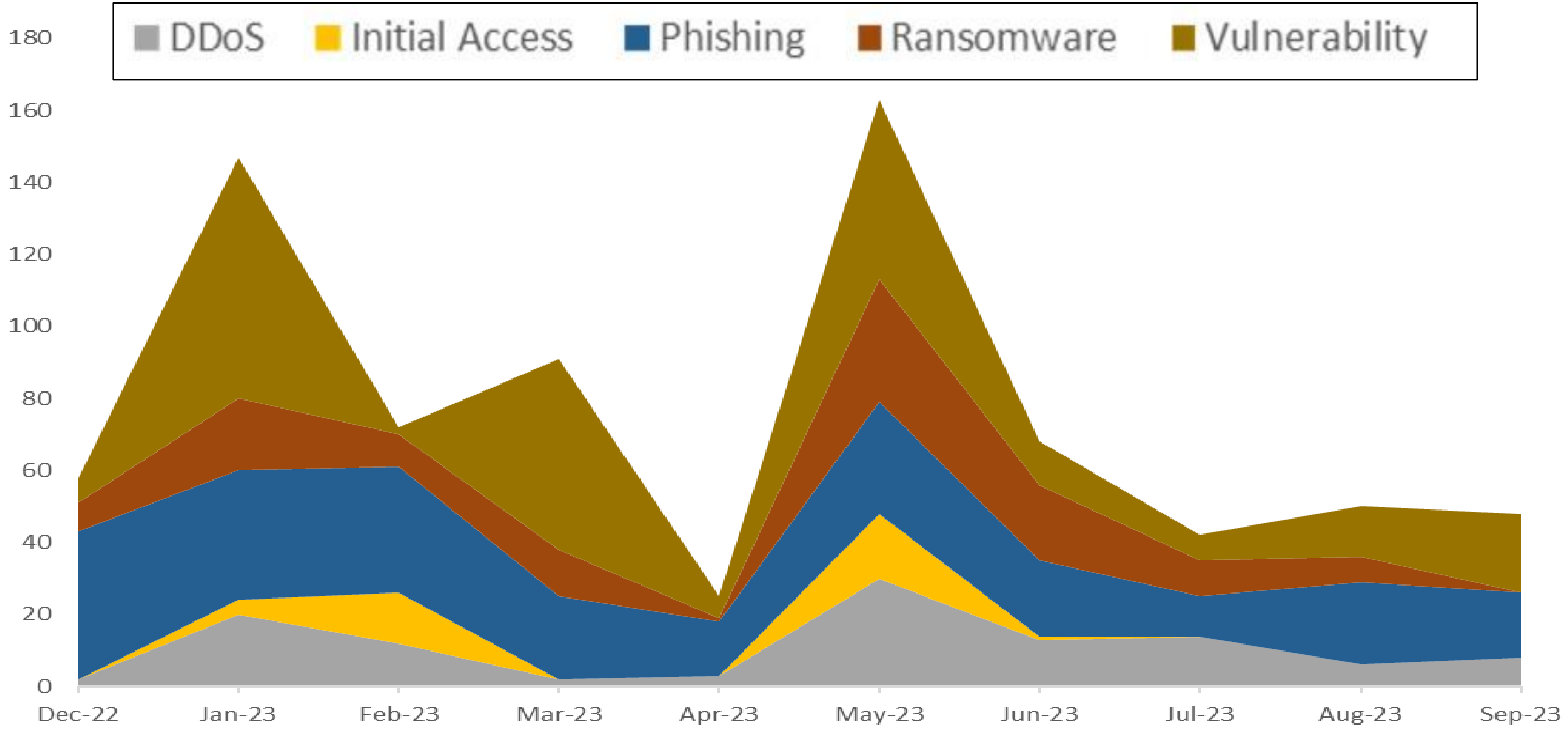
Broad Cyber Threat Themes

- Credentials stolen and used
- Vendors breached and data taken
- Endpoints evaded
- Living off the land
- Zero days used
- Legacy vulnerabilities exploited

Cyber Threats – Ransomware and Vulnerabilities

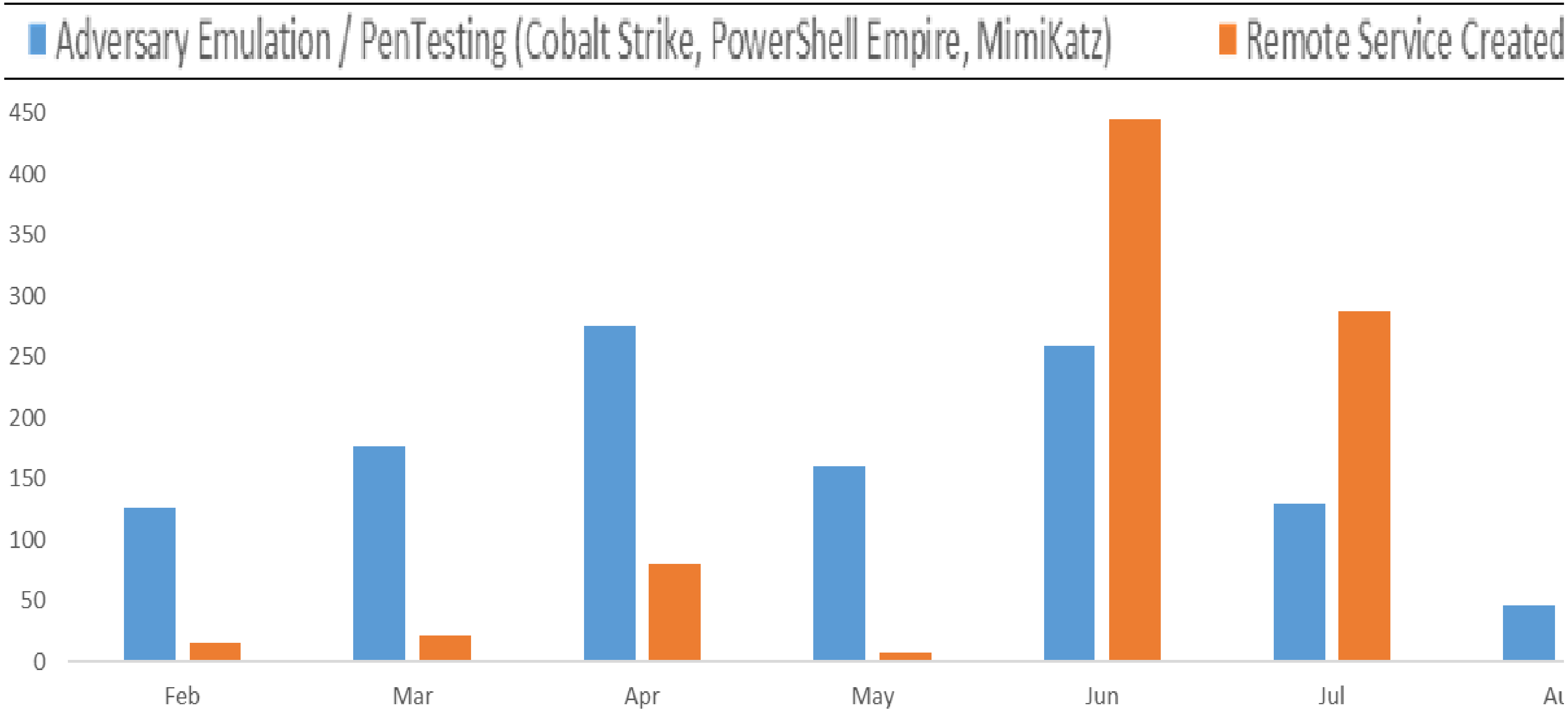
- **MOVEit File Transfer Supply Chain Compromise**
  - CL0P ransomware gang extortion campaign
  - U.S. Government and Service Providers impacted
- **BlackCat/ALPHV ransomware attacks (MGM International)**
  - Attack against retail/hospitality sector involving help-desk impersonation
  - Maintain awareness of compromise of other vendors
- **Prominent Vulnerabilities**
  - Rockwell Automation ControlLogix Communication Module
  - Trend Micro Endpoint Security Remote Code Execution Vulnerability
  - Juniper Remote Code Execution

Membership Sharing IT



Public

OT Trends



Source: Neighborhood Keeper

Questions and Answers

STANDARDS, SECURITY, & RELIABILITY
FALL WORKSHOP

Entity Ownership Change Considerations

Ashley Nwonuma
Enforcement Attorney
&
Abby Fellinger
Manager, Registration & Certification Program

Change Management Issues

We have seen many noncompliance root cause issues stem from issues with entity ownership changes.

An entity’s compliance obligation begins on the day the entity is registered with NERC unless the Requirement or other authoritative document specifies another date for compliance. Entities should be audit-ready on the day of NERC registration.

Common Issues Surrounding Ownership Changes

Most noncompliance issues concern standards that require retaining proper documentation.

The root cause given for those violations center on not receiving the documentation from the previous owners.

Most common standards with documentation components:

- FAC-008-5 – Facility Ratings
- PRC-005-6 – Protection System, Automatic Reclosing, and Sudden Pressure Relaying Maintenance
- MOD-025-2 – Verification and Data Reporting of Generator Real and Reactive Power Capability and Synchronous Condenser Reactive Power Capability
- CIP-003-8 – Cyber Security – Security Management Controls

Best Practices During Ownership Changes

During due diligence period, acquisition team should consider NERC compliance obligations of the facility being purchased.

The entity’s compliance department should be involved early in the due diligence process.

- Allow between 6-12 months before NERC registration to prepare a new GO for compliance. This timeframe will vary depending on the maturity of the existing compliance program.

Best Practices During Ownership Changes

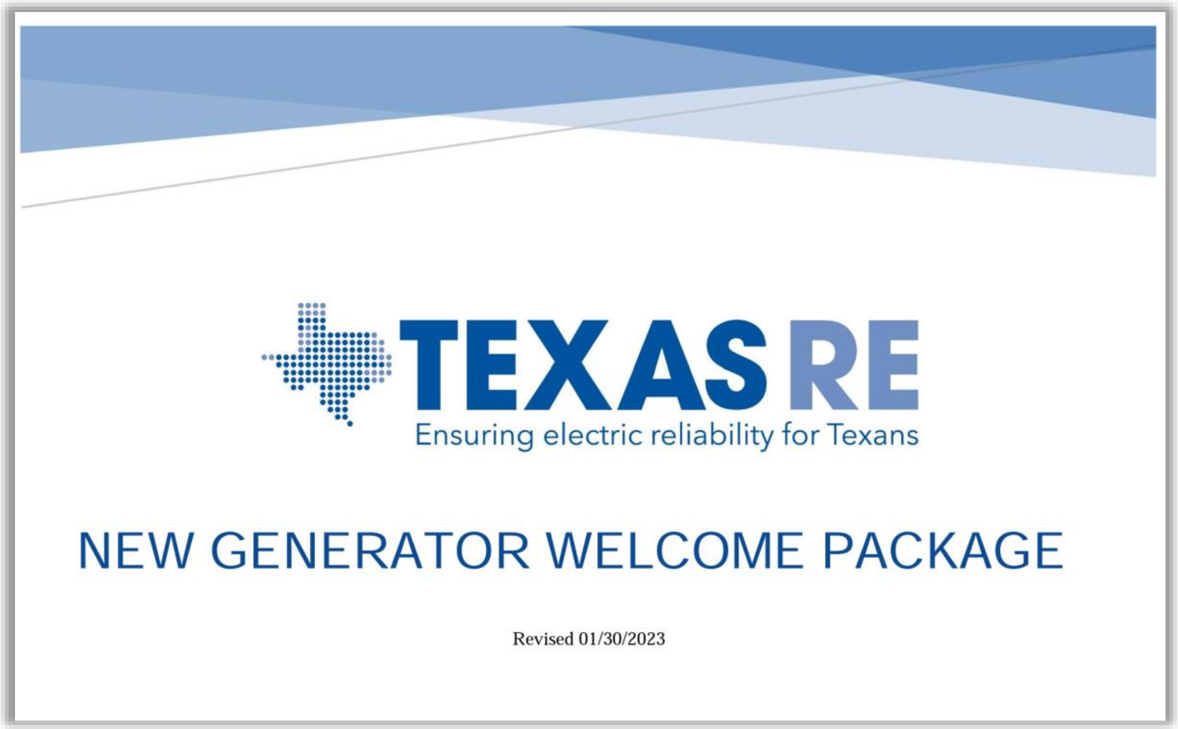
Include NERC compliance requirements in due diligence and in closing checklists.

Use New Generator Welcome Package as a jumping-off point to create checklists and to inform what questions to ask during the due diligence period.

Consider having entities self-report before acquisition as a pre-closing condition.

Designate a storage location for keeping documentation.

Texas RE New Generator Welcome Package



TEXAS RE
Ensuring electric reliability for Texans

NEW GENERATOR WELCOME PACKAGE

Revised 01/30/2023

Texas RE Generator Welcome Package

- Originally published in 2021
- Developed to assist entities plan development and implementation of their compliance program to address key responsibilities and obligations
- Includes best practices for GOs and GOPs

Areas of Focus

Considerations & Planning

Internal Controls Overview

GO GOP Roadmap

Internal Controls Consideration Tables

Example Self-Certification Questions

And recommended reading!

Considerations

Considerations in Preparation of Registration

- An entity should be audit-ready on the day it is registered with NERC.
- Preparing a new GO or GOP for compliance may take 6-12 months of preparation before NERC registration.
- Consider developing a method of tracking preparations through the first year after registration to ensure all initial compliance tasks are completed.
- Implement a strong compliance program and utilize operational best practices.
- Write detailed procedures and process documents that define the entity’s businesses processes with compliance built in.
- Although a documented procedure is not always required, entities are encouraged to establish strong operational business processes with preventative, detective, and corrective internal controls for applicable NERC Reliability Standards and Requirements. The business processes should be designed around the GO's and GOP's needs.
- Similar to developing processes, an entity should develop internal controls appropriate for its organization.

Planning Examples

Planning Stages

Pre-Registration Activity Examples

- ✓ Review the interconnection agreement and service agreements
- ✓ Identify the roles and responsibilities pertaining to the service agreements
- ✓ Determine applicability of the NERC Standards
- ✓ Write procedures where required
- ✓ Perform initial compliance activities where required
- ✓ Commissioning equipment and Facilities
- ✓ Develop processes for compliance activities due following NERC registration (i.e., time-based and event-driven compliance activities)

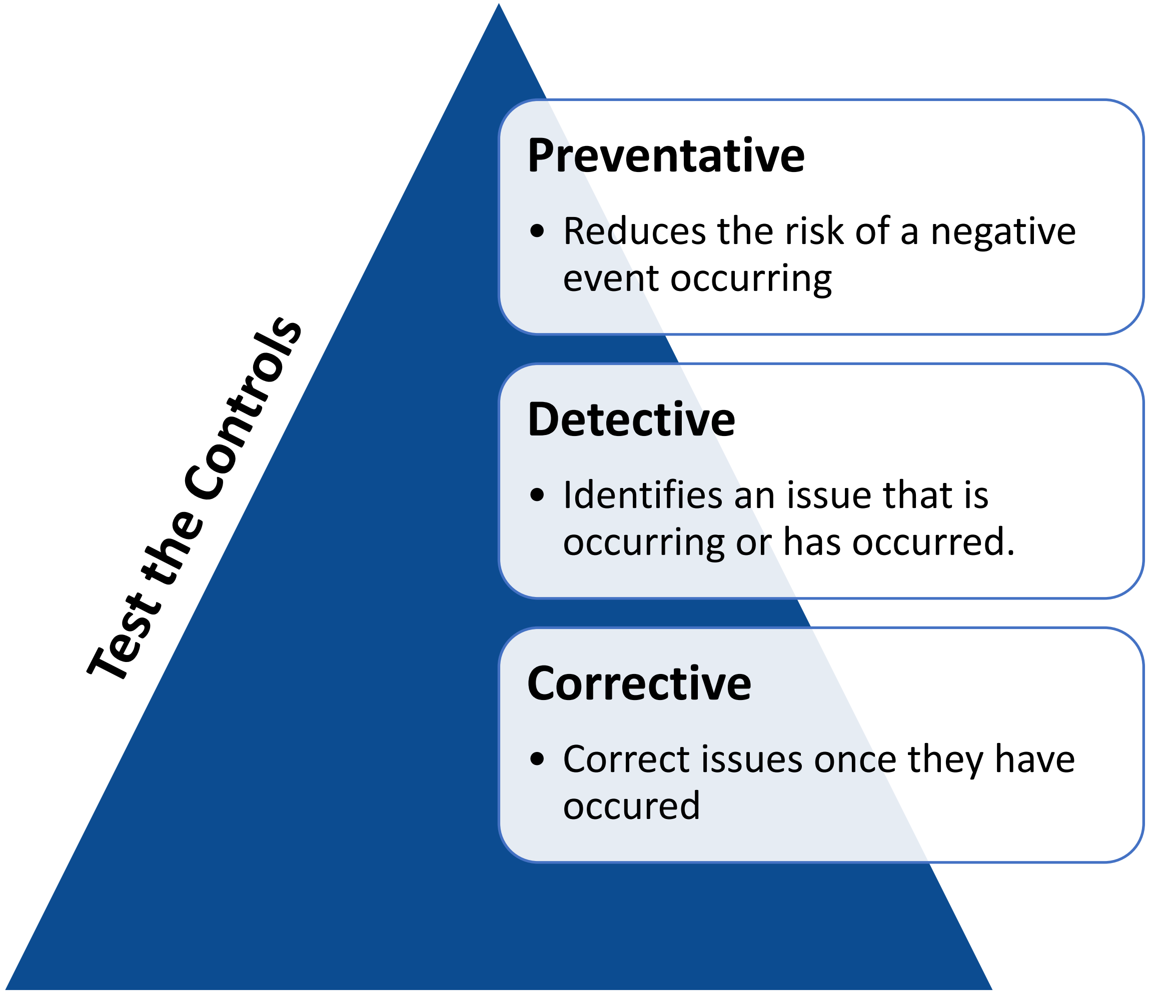
NERC Registration Activity Examples

- ✓ Review the Rules of Procedure (ROP), Appendix 5A, and Appendix 5B
- ✓ Submit NERC registration package to the Regional Entity
- ✓ Retain NCR letter for records

Post-Registration Activity Examples

- ✓ Perform, or prepare to perform, event-driven compliance activities (e.g., PRC-004-6, VAR-002-4.1) and retain appropriate evidence
- ✓ Identify key milestone dates (e.g., commissioning, Commercial Operations Date) to establish due dates for initial performance of time-based compliance activities (e.g., MOD-025-2, MOD-026-1, MOD-027-1)
- ✓ Perform initial, time-based compliance activities and retain appropriate evidence
- ✓ If applicable, set up entity for NERC Alerts, MIDAS reporting, GADS, DADS, and TADS

Internal Controls



Preventative

- Reduces the risk of a negative event occurring

Detective

- Identifies an issue that is occurring or has occurred.

Corrective

- Correct issues once they have occured

GO GOP Roadmap

Procedural

EOP-004-4 R1
EOP-011-2 R7
FAC-003-4 R3
FAC-008-5 R1, R2
PRC-005-6 R1, R2
PRC-027-1 R1

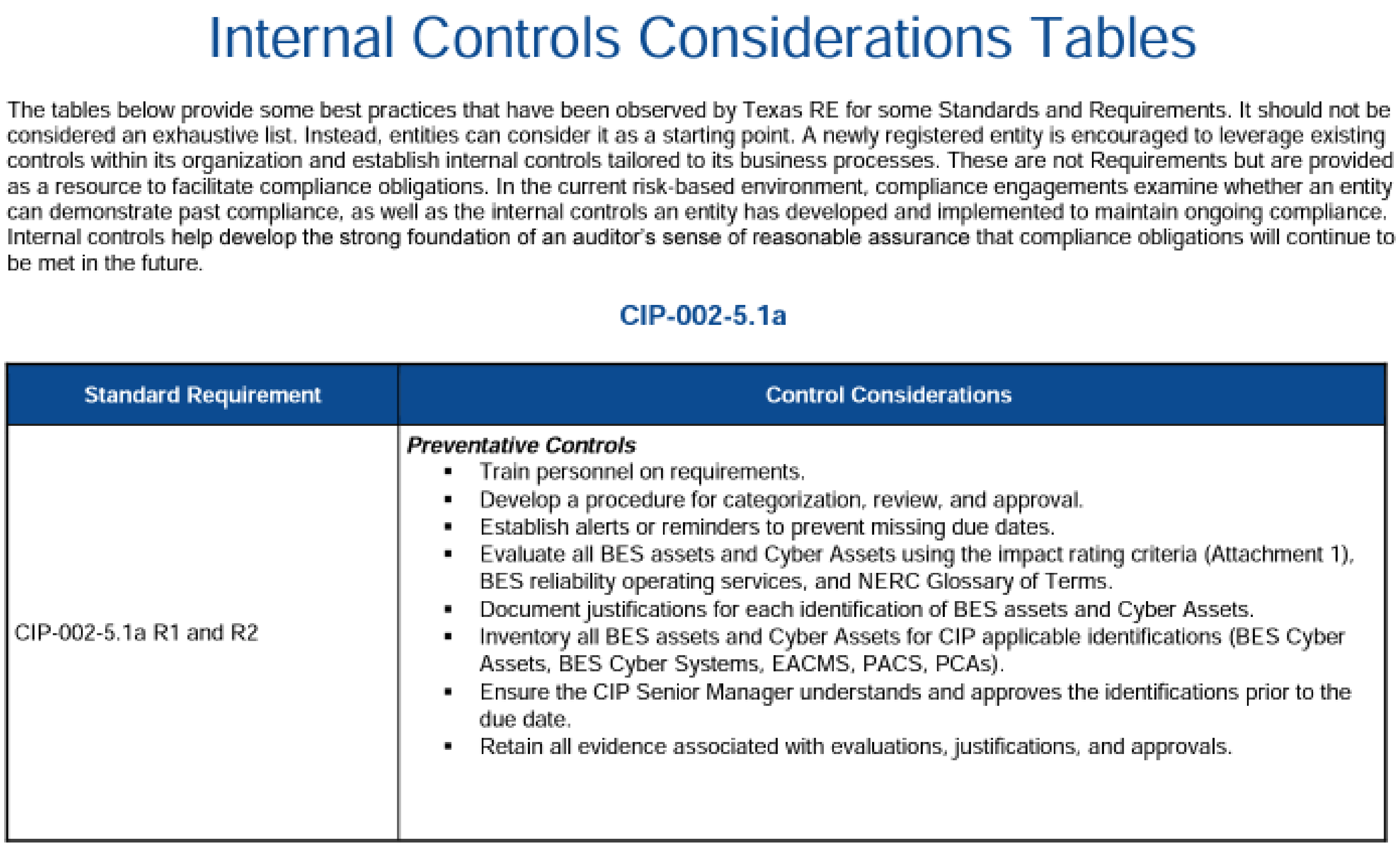
Initial Performance

BAL-001-TRE-2 R6, R7
CIP-002-5.1a R1, R2
CIP-003-8 R1 – R4
CIP-012-1 R1
COM-001-3 R3, R12
COM-002-4 R3
EOP-011-2 R8
FAC-008-5 R6
IRO-010-4 R3
MOD-032-1 R2
PER-005-2 R6
PER-006-1 R1
PRC-019-2 R1
PRC-024-3 R1
PRC-025-2 R1
PRC-027-1 R2
TOP-003-5 R5
VAR002-4.1 R1, R2

Time-Based Performance

FAC-001-3 R2
FAC-003-4 R6, R7
MOD-025-2 R1, R2
MOD-026-1 R2
MOD-027-1 R2
PRC-005-6 R3, R4
PRC-012-2 R8
PRC-027-1 R2

Internal Controls Considerations Tables



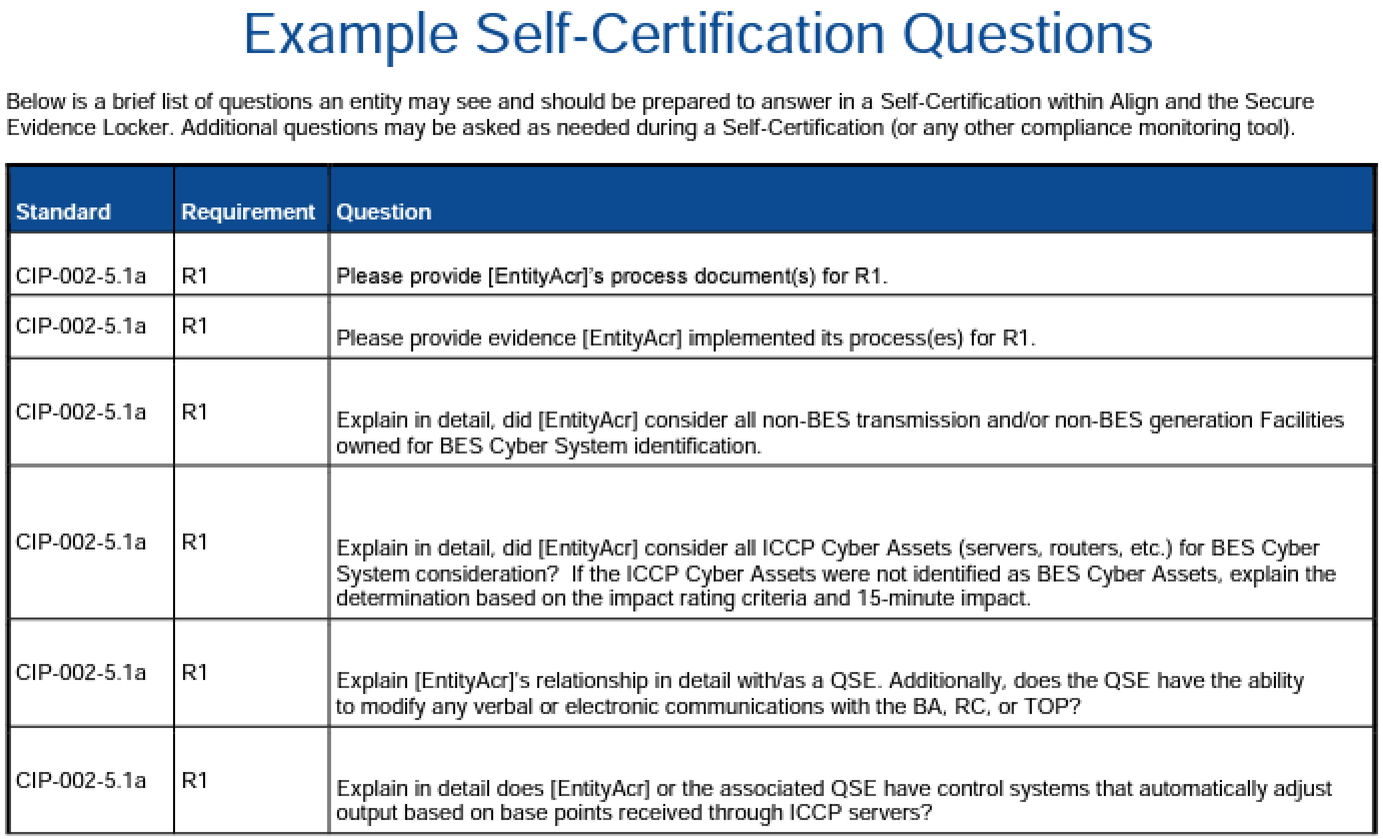
Internal Controls Considerations Tables

The tables below provide some best practices that have been observed by Texas RE for some Standards and Requirements. It should not be considered an exhaustive list. Instead, entities can consider it as a starting point. A newly registered entity is encouraged to leverage existing controls within its organization and establish internal controls tailored to its business processes. These are not Requirements but are provided as a resource to facilitate compliance obligations. In the current risk-based environment, compliance engagements examine whether an entity can demonstrate past compliance, as well as the internal controls an entity has developed and implemented to maintain ongoing compliance. Internal controls help develop the strong foundation of an auditor's sense of reasonable assurance that compliance obligations will continue to be met in the future.

CIP-002-5.1a

Standard Requirement	Control Considerations
CIP-002-5.1a R1 and R2	***Preventative Controls*** ▪ Train personnel on requirements. ▪ Develop a procedure for categorization, review, and approval. ▪ Establish alerts or reminders to prevent missing due dates. ▪ Evaluate all BES assets and Cyber Assets using the impact rating criteria (Attachment 1), BES reliability operating services, and NERC Glossary of Terms. ▪ Document justifications for each identification of BES assets and Cyber Assets. ▪ Inventory all BES assets and Cyber Assets for CIP applicable identifications (BES Cyber Assets, BES Cyber Systems, EACMS, PACS, PCAs). ▪ Ensure the CIP Senior Manager understands and approves the identifications prior to the due date. ▪ Retain all evidence associated with evaluations, justifications, and approvals.

Example Self-Certification Questions



Example Self-Certification Questions

Below is a brief list of questions an entity may see and should be prepared to answer in a Self-Certification within Align and the Secure Evidence Locker. Additional questions may be asked as needed during a Self-Certification (or any other compliance monitoring tool).

Standard	Requirement	Question
CIP-002-5.1a	R1	Please provide [EntityAcr]'s process document(s) for R1.
CIP-002-5.1a	R1	Please provide evidence [EntityAcr] implemented its process(es) for R1.
CIP-002-5.1a	R1	Explain in detail, did [EntityAcr] consider all non-BES transmission and/or non-BES generation Facilities owned for BES Cyber System identification.
CIP-002-5.1a	R1	Explain in detail, did [EntityAcr] consider all ICCP Cyber Assets (servers, routers, etc.) for BES Cyber System consideration? If the ICCP Cyber Assets were not identified as BES Cyber Assets, explain the determination based on the impact rating criteria and 15-minute impact.
CIP-002-5.1a	R1	Explain [EntityAcr]'s relationship in detail with/as a QSE. Additionally, does the QSE have the ability to modify any verbal or electronic communications with the BA, RC, or TOP?
CIP-002-5.1a	R1	Explain in detail does [EntityAcr] or the associated QSE have control systems that automatically adjust output based on base points received through ICCP servers?

Texas RE aims to perform Self-Certifications on newly registered entities within approximately 18 to 24 months following registration. These Self-Certifications are performed to ensure the registered entity has a foundation in place to contribute to the reliability of the BES and maintain compliance with the NERC Reliability Standards.

Registered entities are encouraged to review the example Self-Certification questions and be prepared to answer these questions if the Requirement is included in the scope of a Self-Certification.

Expectation for Registration Changes to Texas RE

Reach out to Texas RE at least 30 days prior to the effective date of any of the registration changes listed below.

Add/Remove a Function

Deactivation/ Deregistration

Entity Function Transfer

Entity Assets Transfer/Merger/ Sale

Entity Name Change

Consolidate NCR Numbers

Change in JRO/CFR

Documentation may be required via the Centralized Organization Registration ERO System (CORES).

Resources for New Entities and New Contacts

Texas RE Generator Welcome Package

Texas RE Welcome Packet

ERO Enterprise 101 Informational Package

ERO Enterprise Entity Onboarding Checklist

ERO Enterprise Registration Procedure

Contact Information

Abby Fellinger

Manager, Registration and Certification Program

(512) 583-4927

abby.fellinger@texasre.org | registration@texasre.org

Ashley Nwonuma

Enforcement Attorney

(512) 583-4973

ashley.nwonuma@texasre.org

Questions?

TEXAS RE

Ensuring electric reliability for Texans

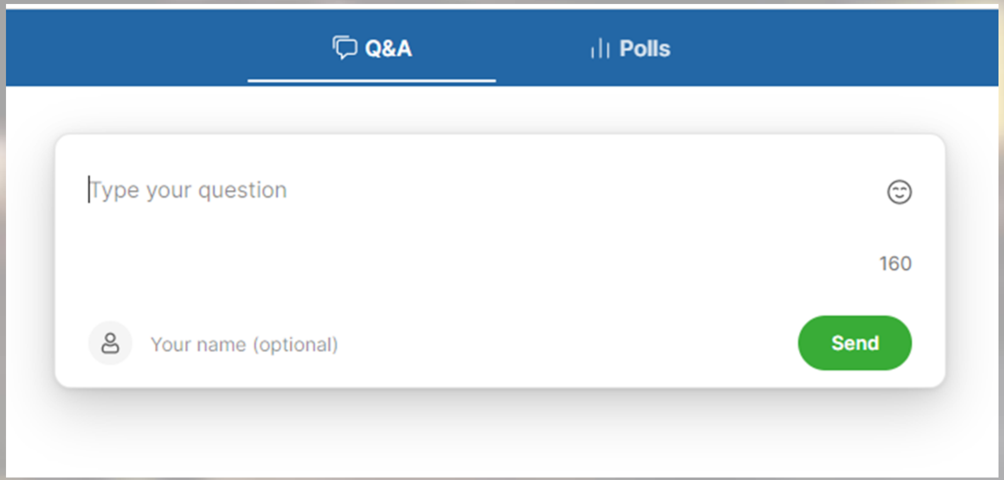
STANDARDS, SECURITY, & RELIABILITY FALL WORKSHOP

Fall Standards, Security, & Reliability Workshop

Return at: 12:40 p.m.

- New BCSI in the Cloud Standards
- FERC Vulnerability and Physical Security Assessment Program
- New Weatherization Requirements
- Emerging Cyber and Physical Risks
- Entity Ownership Change Considerations
- **Cyber Informed Transmission Planning**
- Change Management Controls
- Emerging Issues with Distributed Energy Resources
- Grid Forming Inverter Technology: Opportunities for a Changing Grid

To submit questions during the workshop, please visit **slido.com** and enter today's participant code: **TXRE**



NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

ERO Enterprise Cyber-Informed Transmission Planning

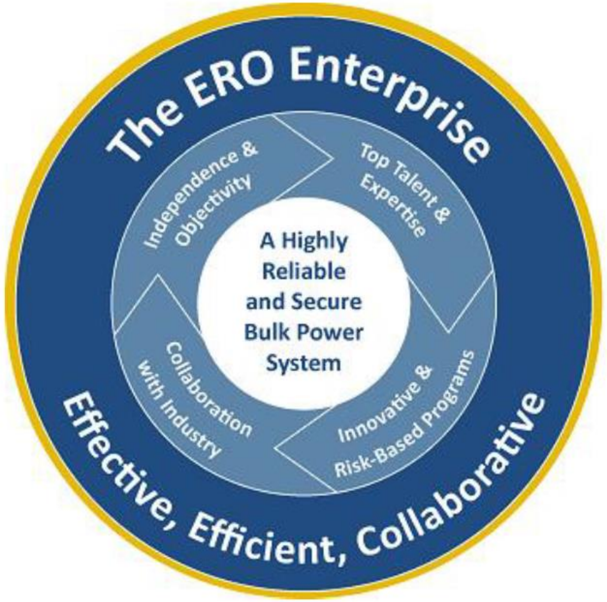
Security Integration

October 25, 2023

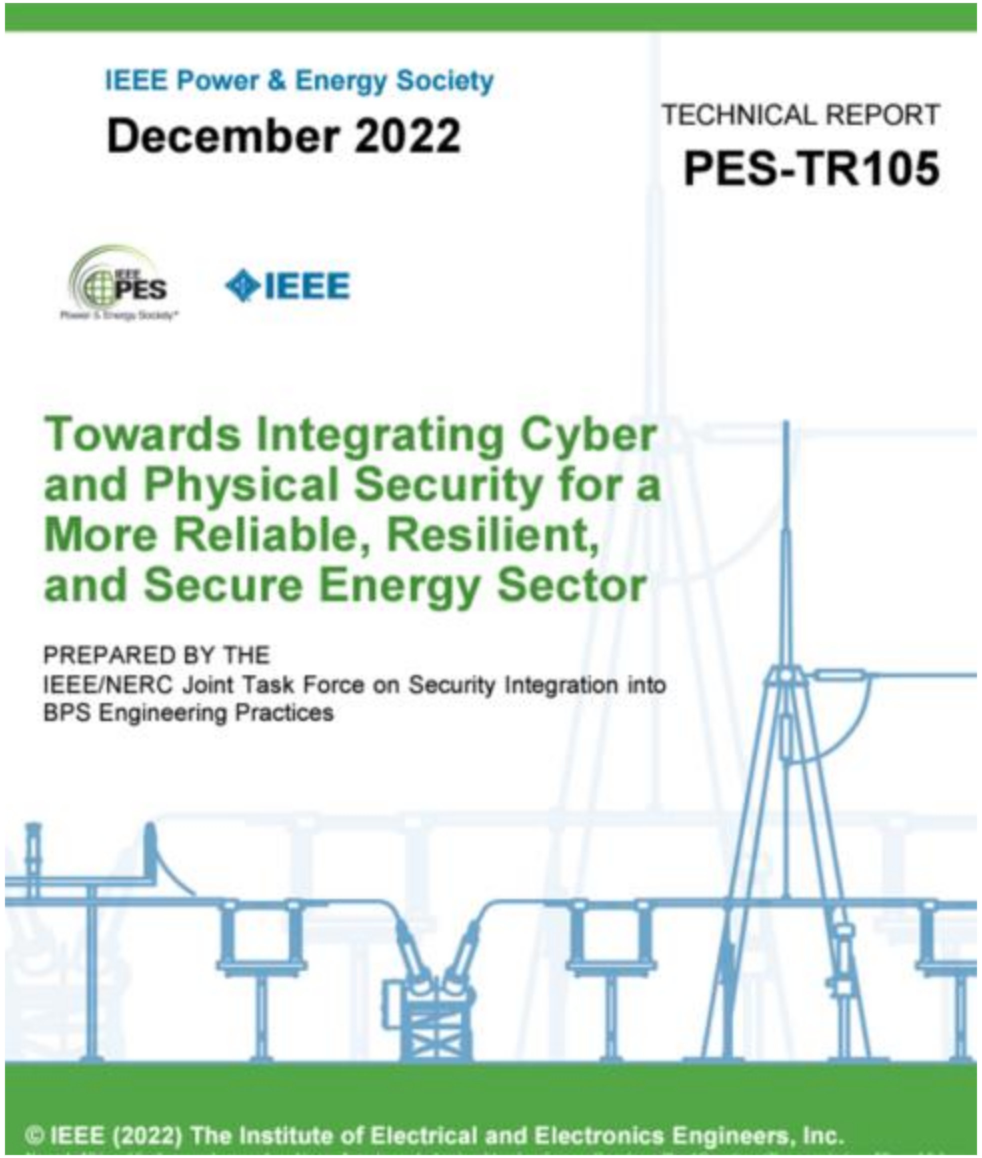
RELIABILITY | RESILIENCE | SECURITY

Security Integration

- The incorporation of cyber and physical security aspects into conventional planning, design, and operations engineering practices.
- 2021 ERO Risk Priorities Report
  - www.nerc.com/comm/RISC
- Security Integration and Technology Enablement Subcommittee (SITES)
  - www.nerc.com/comm/RSTC/Pages/SITES.aspx
- Security Working Group
  - https://www.nerc.com/comm/RSTC/Pages/SWG.aspx


The ERO Enterprise
Independence & Objectivity
Top Talent & Expertise
A Highly Reliable and Secure Bulk Power System
Collaboration with Industry
Innovative & Risk-Based Programs
Effective, Efficient, Collaborative

NERC / IEEE Technical Report 105



IEEE Power & Energy Society

December 2022

TECHNICAL REPORT

PES-TR105

Towards Integrating Cyber and Physical Security for a More Reliable, Resilient, and Secure Energy Sector

PREPARED BY THE
IEEE/NERC Joint Task Force on Security Integration into BPS Engineering Practices

- Threats, Planning, Design, Operations, Emerging Technology

Cyber-Informed Transmission Planning

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

MIDWEST RELIABILITY ORGANIZATION NPCC, Inc. RELIABILITY FIRST SERC TEXAS RE WECC

Cyber-Informed Transmission Planning

Roadmap for Integrating Cyber Security into Transmission Planning Activities

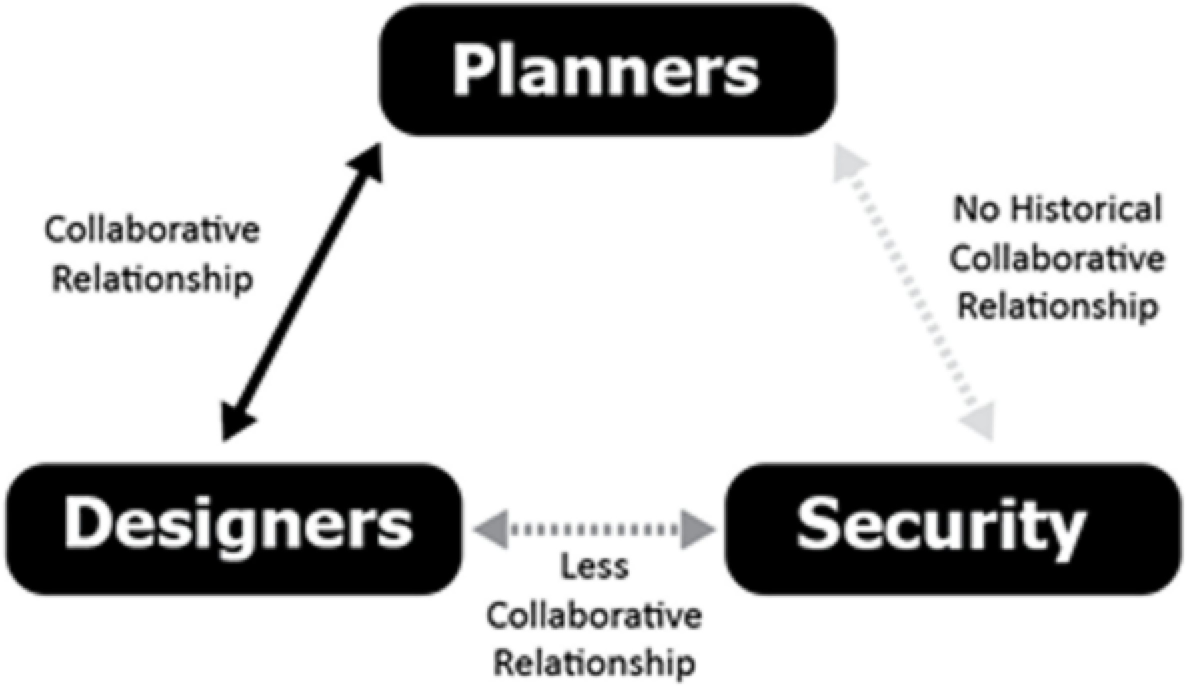
May 2023

- [ERO_Enterprise_Whitepaper_Cyber_Planning]
  - Released May 2023

- Develop cyber-informed planning approaches
  - CITPF
  - Scenarios

Historical Interactions

- Lacking Interaction
- Cybersecurity not part of engineering activities

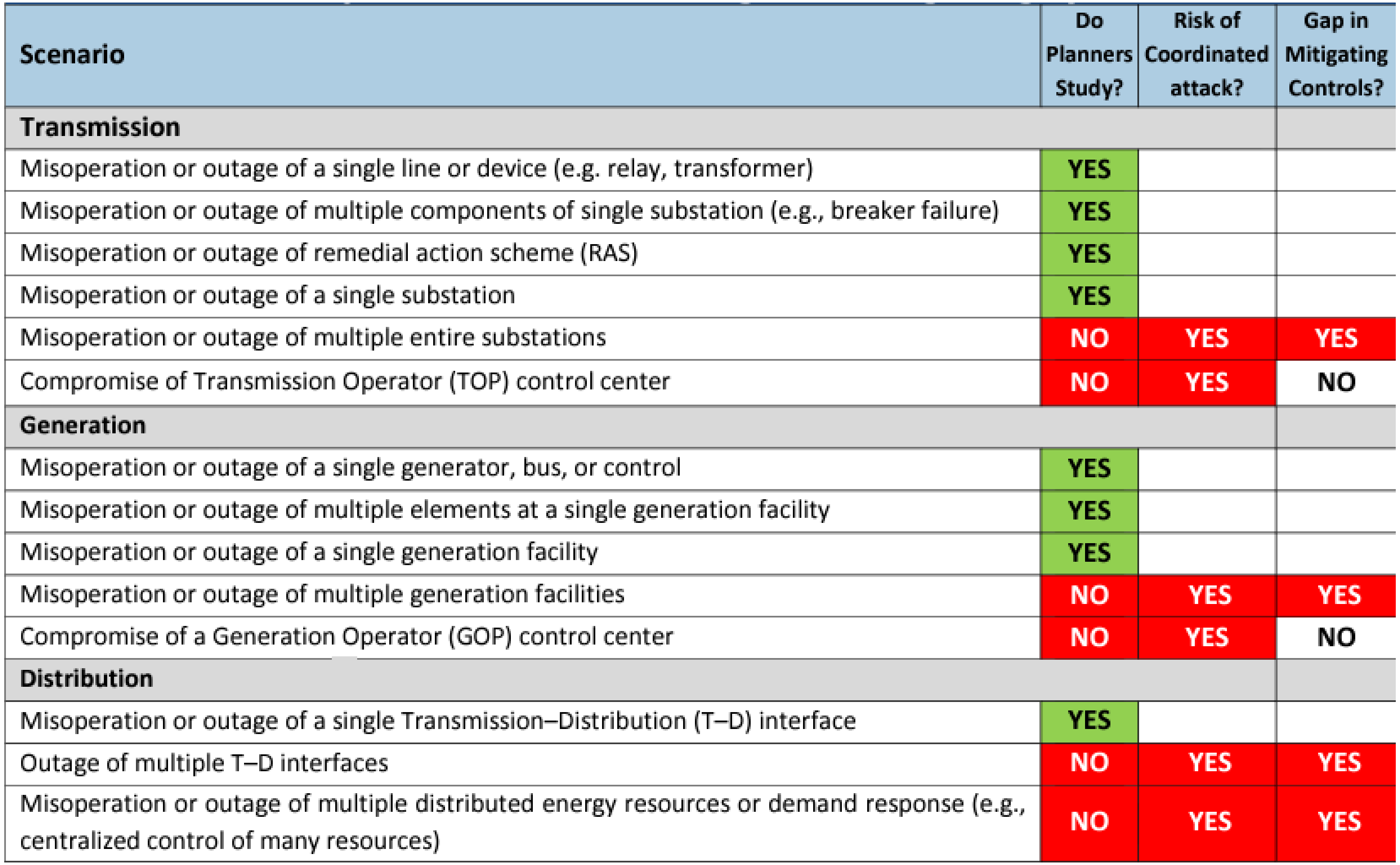

Planners
Collaborative Relationship
No Historical Collaborative Relationship
Designers
Security
Less Collaborative Relationship

White paper – Some Key Areas of Focus

- Align terminology
- Identify security control gaps
- Map threats, vulnerabilities, and attack scenarios to contingency definitions utilizing the methodology and framework
- Conduct planning studies (Pilot Projects)
- Drive enhancements to NERC standards

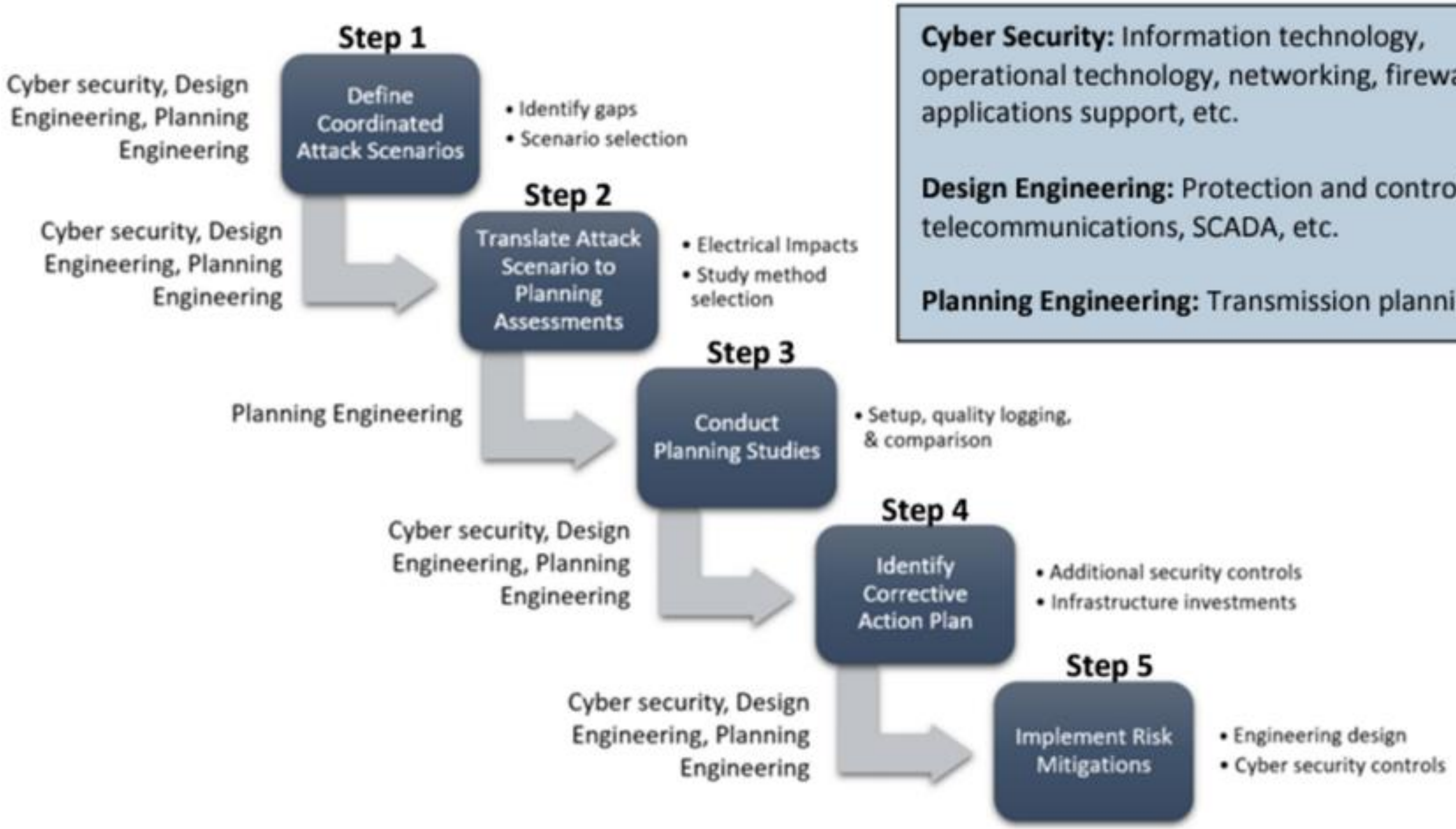
Public

Existing Gaps in Planning Studies



Scenario	Do Planners Study?	Risk of Coordinated attack?	Gap in Mitigating Controls?
Transmission			
Misoperation or outage of a single line or device (e.g. relay, transformer)	YES		
Misoperation or outage of multiple components of single substation (e.g., breaker failure)	YES		
Misoperation or outage of remedial action scheme (RAS)	YES		
Misoperation or outage of a single substation	YES		
Misoperation or outage of multiple entire substations	NO	YES	YES
Compromise of Transmission Operator (TOP) control center	NO	YES	NO
Generation			
Misoperation or outage of a single generator, bus, or control	YES		
Misoperation or outage of multiple elements at a single generation facility	YES		
Misoperation or outage of a single generation facility	YES		
Misoperation or outage of multiple generation facilities	NO	YES	YES
Compromise of a Generation Operator (GOP) control center	NO	YES	NO
Distribution			
Misoperation or outage of a single Transmission–Distribution (T–D) interface	YES		
Outage of multiple T–D interfaces	NO	YES	YES
Misoperation or outage of multiple distributed energy resources or demand response (e.g., centralized control of many resources)	NO	YES	YES

Framework


Step 1
Define Coordinated Attack Scenarios
Cyber security, Design Engineering, Planning Engineering
• Identify gaps
• Scenario selection
Step 2
Translate Attack Scenario to Planning Assessments
Cyber security, Design Engineering, Planning Engineering
• Electrical Impacts
• Study method selection
Step 3
Conduct Planning Studies
Planning Engineering
• Setup, quality logging, & comparison
Step 4
Identify Corrective Action Plan
Cyber security, Design Engineering, Planning Engineering
• Additional security controls
• Infrastructure investments
Step 5
Implement Risk Mitigations
Cyber security, Design Engineering, Planning Engineering
• Engineering design
• Cyber security controls

Cyber Security: Information technology, operational technology, networking, firewalls, applications support, etc.

Design Engineering: Protection and controls, telecommunications, SCADA, etc.

Planning Engineering: Transmission planning

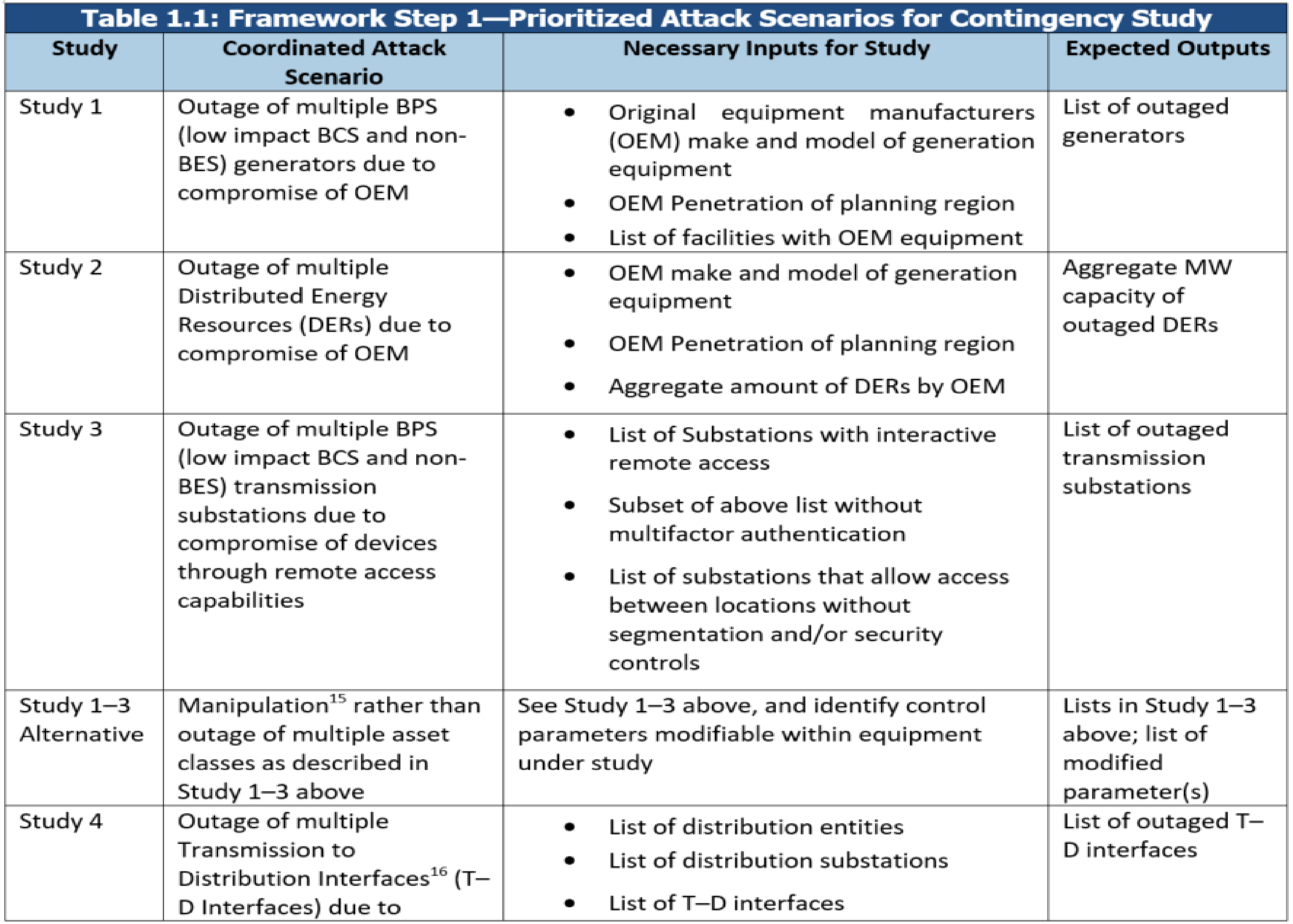


Table 1.1: Framework Step 1—Prioritized Attack Scenarios for Contingency Study

Study	Coordinated Attack Scenario	Necessary Inputs for Study	Expected Outputs
Study 1	Outage of multiple BPS (low impact BCS and non-BES) generators due to compromise of OEM	• Original equipment manufacturers (OEM) make and model of generation equipment • OEM Penetration of planning region • List of facilities with OEM equipment	List of outaged generators
Study 2	Outage of multiple Distributed Energy Resources (DERs) due to compromise of OEM	• OEM make and model of generation equipment • OEM Penetration of planning region • Aggregate amount of DERs by OEM	Aggregate MW capacity of outaged DERs
Study 3	Outage of multiple BPS (low impact BCS and non-BES) transmission substations due to compromise of devices through remote access capabilities	• List of Substations with interactive remote access • Subset of above list without multifactor authentication • List of substations that allow access between locations without segmentation and/or security controls	List of outaged transmission substations
Study 1–3 Alternative	Manipulation[15] rather than outage of multiple asset classes as described in Study 1–3 above	See Study 1–3 above, and identify control parameters modifiable within equipment under study	Lists in Study 1–3 above; list of modified parameter(s)
Study 4	Outage of multiple Transmission to Distribution Interfaces[16] (T–D Interfaces) due to	• List of distribution entities • List of distribution substations • List of T–D interfaces	List of outaged T–D interfaces

Pilot Projects - Conduct Planning Studies

Q: What are the goals / objectives of the project?

Q: What are the timelines and milestones for the pilot projects?

Q: Who will monitor the progress?

Q: What type of entity are we looking for the pilot (ISO/RTO, small/medium/large utility, some in the market, vertically integrated?)

Q: What will be the expectations from the participants, white paper, report, etc?

Q: How many participants are we looking at?

Pilot Activities & Responsibilities		
Activity	Primary Driver	Involved
Identify Pilot Project Partners	Regional Entity	Registered Entity
Introductory scope call with entity	Regional Entity	NERC Staff / Registered Entity
Entity conducts pilot study with regular touchpoints	Registered Entity	Regional Entity
Entity requests Q/A support during pilot	Registered Entity	Regional Entity / NERC Staff
Post-pilot sessions identifying lessons learned	Regional Entity	NERC Staff / Registered Entity
Final lessons learned report	NERC Staff	Regional Entity(s)

Recommendations

- Enhancing Security Integration Across the Electricity Ecosystem
- Engage and Share with E-ISAC
- Adopt the CITPF
- Use or refine attack scenarios
- Cyber-Informed Transmission Planning Pilots
- Future Enhancements to TPL-001
- Physical Security Considerations
- Security Integration for Blackstart Studies
- Simulation Tools Enhancements
- Secure Planning Assessment Models and Studies

Questions and Answers

STANDARDS, SECURITY, & RELIABILITY

FALL WORKSHOP

Change Management Controls

Eric Newnam
O&P Compliance Engineer III

Paul Hopson
Compliance Team Lead

Kaitlin Van Zee
Director, Enforcement & Registration

Change Management Controls

EOP-011-2 R7 and R8

- Eric Newnam, O&P Compliance Engineer III

CIP-003-8 and CIP-012-1

- Paul Hopson, CIP Compliance Team Lead

How Internal Controls are Viewed in Enforcement

- Kaitlin Van Zee, Director, Enforcement & Registration

Changes that May Affect EOP-011-2

Equipment Changes

- Associated risk
- Cold Weather Preparedness FAQ
- What controls have we seen

Weather Changes

- Associated risk
- Cold Weather Preparedness FAQ
- What controls have we seen

Personnel Changes

- Associated risk
- Cold Weather Preparedness FAQ
- What controls have we seen

Standard Changes

- Associated risk
- Cold Weather Preparedness FAQ
- What controls have we seen

Associated Risks for Equipment Changes

- □ **Operating During Emergencies/Backup & Recovery**
  - Entities must take appropriate actions during an emergency, system event, or unexpected conditions that could result in instability, uncontrolled separation, or cascading outages within an Interconnection. This can include the following:
    - ○ Ensure proper operation, availability, and utilization of facilities and tools during a system event, emergency, or unexpected condition
- □ **Unplanned equipment changes**
- □ **Equipment failure during weather event**
- □ **Availability of operation consumables during weather event**
- □ **Fuel supplies during weather event**

Cold Weather Preparedness FAQ – Equipment Changes

Q4: Why is there so much emphasis placed on fuel switching capability?

- Fuel switching is one method that generators can use to alleviate the strain when a particular fuel source is in short supply.

Q17: What specifically is required to document for EOP-11-2 R7.3.1, especially on the Capability and Availability sub-requirement?

- Capability and availability should directly correlate to the RC/BA/TOP data specifications provided in IRO-010-4 and TOP-003-5. **This is not a one-time submission**. The expectation is that this is maintained and updated based on changing conditions and based on data specification regardless of whether RC/TOP requested it as part of IRO-010-4 and TOP-003-5.

Q18: Currently, we only document the design temperature for wind turbine and for the inverter and related equipment supporting the inverters. Is that sufficient?

- Registered entities should consider all systems, not just a subset.

The Cold Weather Preparedness FAQ is available on Texas RE's Resource Hub

Equipment Changes

What Controls Have We Seen?

- Yearly inspection prior to the winter months to ensure:
  - Equipment changes have been accounted for.
  - Replacement parts are fully stocked.
  - Consumable supplies are fully stocked.
  - Fuel supply is confirmed, and alternate is in place.

Associated Risks for Weather Changes

❑ **Operating During Emergencies/Backup & Recovery**

- Entities must take appropriate actions during an emergency, system event, or unexpected conditions that could result in instability, uncontrolled separation, or cascading outages within an Interconnection. This can include the following:
  - ○ Ensure proper operation, availability, and utilization of facilities and tools during a system event, emergency, or unexpected condition

❑ **Weather changes constantly**

❑ **Texas has set many new weather records in the past few years**

Weather Changes

Q5: We have individual plans and training for each of our locations. Is this the intended approach?

- The language in EOP-011-2 R7 allows for **one or more cold weather preparedness plans**. This language provides flexibility for the entity to determine whether a single plan or multiple plans are necessary. For training, EOP-011-2 R8 states that **generating unit-specific training** is to be provided.

Q7: What criteria is acceptable for use in defining a “cold weather event” for our facility?

- Since there are different interpretations of “cold weather” across the ERO due to geographic location and climate, it would not be feasible to define a universal term. Each entity should use their own weather resource(s) and operating experience to establish the appropriate cold weather conditions.

Q15: What would be acceptable as criteria around local forecasted cold weather, timing for forecast, timing of notification of a forecasted cold weather (for example, Friday’s OPA is for Monday), and applicability of cold weather?

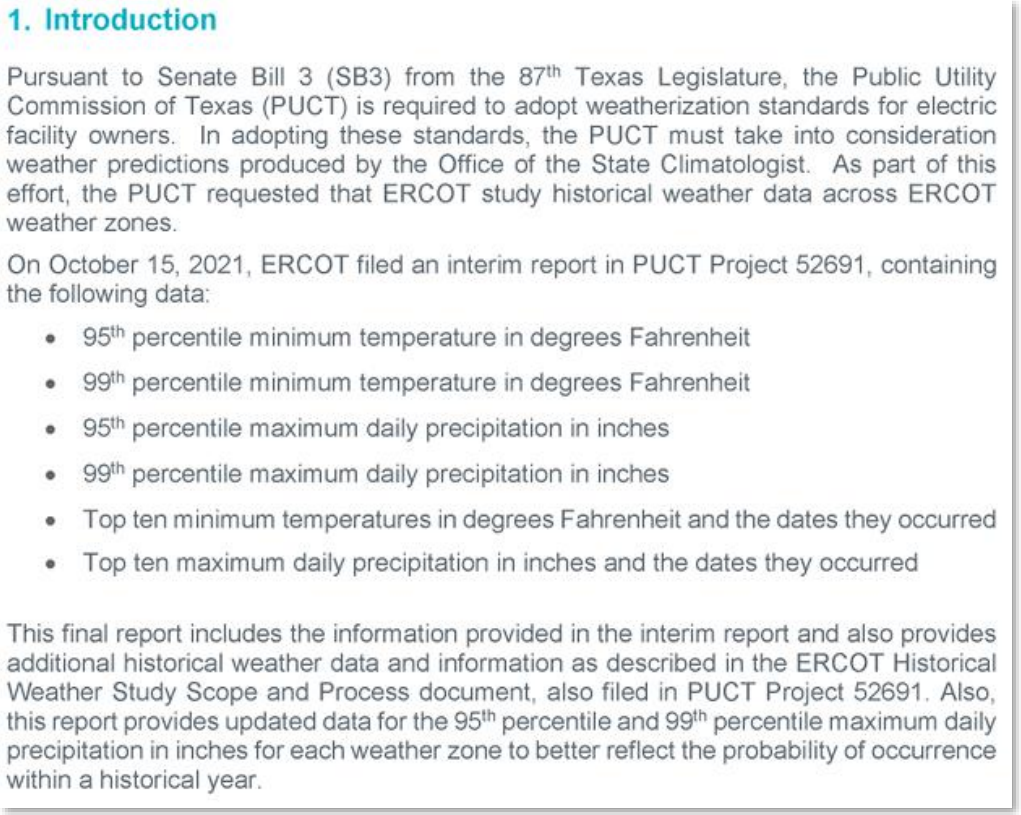
- Compliance will be determined by facts and circumstances, and ERO Enterprise staff will be interested in how an entity makes a good faith effort to obtain the best data possible if their location makes data collection challenging.

Q16: Regarding checklist maintenance, how does NERC view cold weather events that happen after appropriate completion of pre-season inspection & maintenance checks?

- Registered entities need to follow their plans. Registered entities should also review "Project 2021-07 Extreme Cold Weather Grid Operations, Preparedness, and Coordination" and the subsequent FERC Order Approving Extreme Cold Weather Reliability Standards.

The Cold Weather Preparedness FAQ is available on Texas RE’s Resource Hub

ERCOT Historical Weather Study Final Report Version 1.1



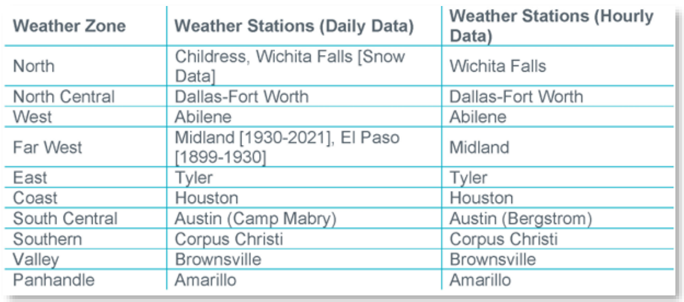
1. Introduction

Pursuant to Senate Bill 3 (SB3) from the 87th Texas Legislature, the Public Utility Commission of Texas (PUCT) is required to adopt weatherization standards for electric facility owners. In adopting these standards, the PUCT must take into consideration weather predictions produced by the Office of the State Climatologist. As part of this effort, the PUCT requested that ERCOT study historical weather data across ERCOT weather zones.

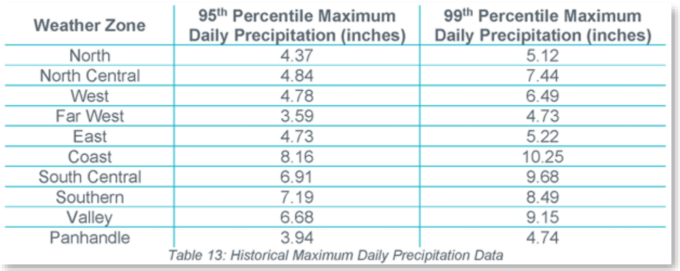
On October 15, 2021, ERCOT filed an interim report in PUCT Project 52691, containing the following data:

- 95th percentile minimum temperature in degrees Fahrenheit
- 99th percentile minimum temperature in degrees Fahrenheit
- 95th percentile maximum daily precipitation in inches
- 99th percentile maximum daily precipitation in inches
- Top ten minimum temperatures in degrees Fahrenheit and the dates they occurred
- Top ten maximum daily precipitation in inches and the dates they occurred

This final report includes the information provided in the interim report and also provides additional historical weather data and information as described in the ERCOT Historical Weather Study Scope and Process document, also filed in PUCT Project 52691. Also, this report provides updated data for the 95th percentile and 99th percentile maximum daily precipitation in inches for each weather zone to better reflect the probability of occurrence within a historical year.

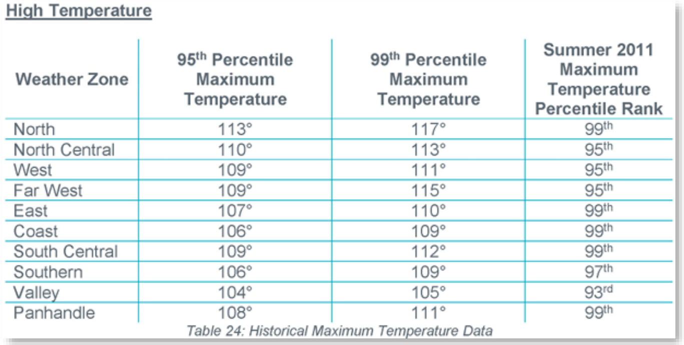


Weather Zone	Weather Stations (Daily Data)	Weather Stations (Hourly Data)
North	Childress, Wichita Falls [Snow Data]	Wichita Falls
North Central	Dallas-Fort Worth	Dallas-Fort Worth
West	Abilene	Abilene
Far West	Midland [1930-2021], El Paso [1899-1930]	Midland
East	Tyler	Tyler
Coast	Houston	Houston
South Central	Austin (Camp Mabry)	Austin (Bergstrom)
Southern	Corpus Christi	Corpus Christi
Valley	Brownsville	Brownsville
Panhandle	Amarillo	Amarillo



Weather Zone	95th Percentile Maximum Daily Precipitation (inches)	99th Percentile Maximum Daily Precipitation (inches)
North	4.37	5.12
North Central	4.84	7.44
West	4.78	6.49
Far West	3.59	4.73
East	4.73	5.22
Coast	8.16	10.25
South Central	6.91	9.68
Southern	7.19	8.49
Valley	6.68	9.15
Panhandle	3.94	4.74

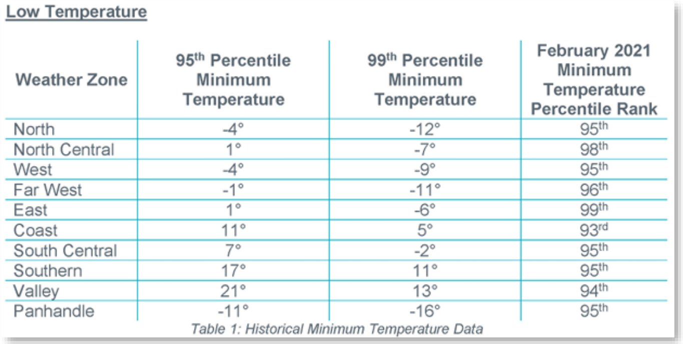
Table 13: Historical Maximum Daily Precipitation Data



High Temperature

Weather Zone	95th Percentile Maximum Temperature	99th Percentile Maximum Temperature	Summer 2011 Maximum Temperature Percentile Rank
North	113°	117°	99th
North Central	110°	113°	95th
West	109°	111°	95th
Far West	109°	115°	95th
East	107°	110°	99th
Coast	106°	109°	99th
South Central	109°	112°	99th
Southern	106°	109°	97th
Valley	104°	105°	93rd
Panhandle	108°	111°	99th

Table 24: Historical Maximum Temperature Data



Low Temperature

Weather Zone	95th Percentile Minimum Temperature	99th Percentile Minimum Temperature	February 2021 Minimum Temperature Percentile Rank
North	-4°	-12°	95th
North Central	1°	-7°	98th
West	-4°	-9°	95th
Far West	-1°	-11°	96th
East	1°	-6°	99th
Coast	11°	5°	93rd
South Central	7°	-2°	95th
Southern	17°	11°	95th
Valley	21°	13°	94th
Panhandle	-11°	-16°	95th

Table 1: Historical Minimum Temperature Data

ERCOT/PUC

- ❑ ERCOT Historical Weather Study Final Report Version 1.1
- ❑ Interchange - Filings (texas.gov)

Weather Changes

What Controls Have We Seen?

- Periodic review of the process to ensure:
  - Historical weather data is updated.
  - Lessons learned are incorporated into process.
  - Adjustments are made for the forecasted weather.

Associated Risk for Personnel Changes

- □ **Operating During Emergencies/Backup & Recovery**
  - Entities must take appropriate actions during an emergency, system event, or unexpected conditions that could result in instability, uncontrolled separation, or cascading outages within an Interconnection. This can include the following:
    - **Ensure personnel are sufficiently prepared** and have adequate access to the procedures, processes, tools, and facilities necessary to respond appropriately and effectively during a system event, emergency, or unexpected condition.
- □ **Changes in personnel (including third parties)**

Cold Weather Preparedness FAQ – Personnel Changes

Q8: How detailed do our generating unit annual inspection and maintenance freeze protection measures need to be in our Plan?

- A plan should provide sufficient detail so that the responsible personnel implementing the plan can understand what actions are needed.

Q13: Is there an annual/periodic training expectation for maintenance and/or operations personnel? Can the plan include flexibility on the frequency of training based on identified changes that would be material and therefore only then require refresher training?

- **Cold weather preparedness plans are cyclic in nature and training should follow that cycle**. Consideration should be given to administering training based on changes to the plan or facility.

Q24: If personnel become responsible for carrying out tasks in the cold weather preparedness plan during a winter season, and they previously have not received training, are they required to have training before performing the actions?

- The registered entity is responsible for the cold weather program including training of both employees and contractors as needed and per the cold weather plan.

The Cold Weather Preparedness FAQ is available on Texas RE's Resource Hub

Personnel Changes

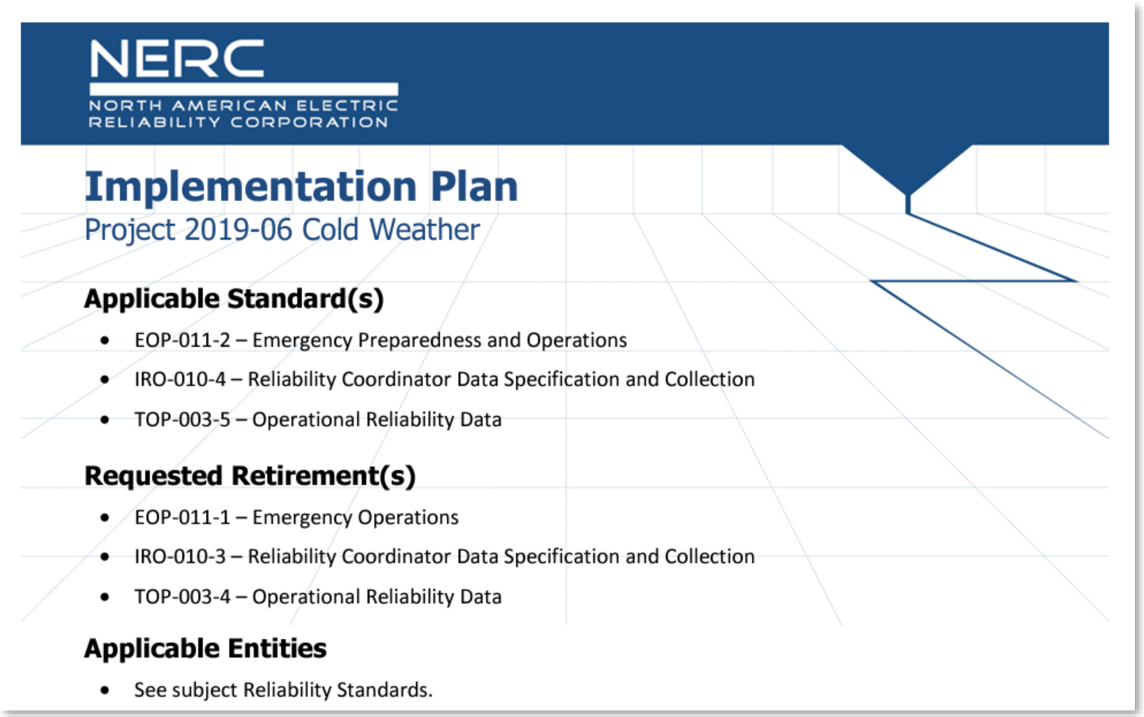
What Controls Have We Seen?

- Yearly training prior to the winter months to ensure:
  - Staff training is up to date .
  - Staff know who is responsible for what.
  - Staff know where to get weather alerts.
  - Staff know who to contact.
- Questions to ask about your internal controls.
  - How do you ensure that your third-party contractors (QSE, inspectors, etc.) are doing what they are supposed to do per the plan?
  - Do you have controls in place to check what you are giving third-party contractors and what you get back?
    - Do third-party contractors provide you records?
    - What level of information is capture in those records?
    - Is it sufficient to ensure that third-party contractors are implementing the plan?

Associated Risk with Standard Changes

- ❑ **Emergency Operations Planning**
  - Entities must have the necessary facilities, tools, processes, and procedures in place to prevent or respond to system events, emergencies, or unexpected conditions. **<u>Failure to develop adequate plans may result in gaps in processes</u>**, procedures, and tools, which may lead to a compromise of the integrity and reliability of the BPS.
- ❑ **Not being aware of changes in the standard language**
- ❑ **Not being aware of implementation plan**
- ❑ **Not being aware of responsibilities**

Standard Changes



NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Implementation Plan

Project 2019-06 Cold Weather

Applicable Standard(s)

- EOP-011-2 – Emergency Preparedness and Operations
- IRO-010-4 – Reliability Coordinator Data Specification and Collection
- TOP-003-5 – Operational Reliability Data

Requested Retirement(s)

- EOP-011-1 – Emergency Operations
- IRO-010-3 – Reliability Coordinator Data Specification and Collection
- TOP-003-4 – Operational Reliability Data

Applicable Entities

- See subject Reliability Standards.

□Initial Performance of Periodic Requirements

- Responsible Entities shall develop, maintain, and implement the Operating Plan(s) required by Reliability Standard EOP-011-2. For the cold weather preparedness plan(s) for generating unit(s) required under Requirement R7, the Responsible Entity shall perform annual inspection and maintenance of generating unit freeze protection measures under Requirement R7 Part 7.2 and conduct generating unit specific training for its maintenance and operations personnel under Requirement R8.

Standard Changes

Future Standard EOP-012-1

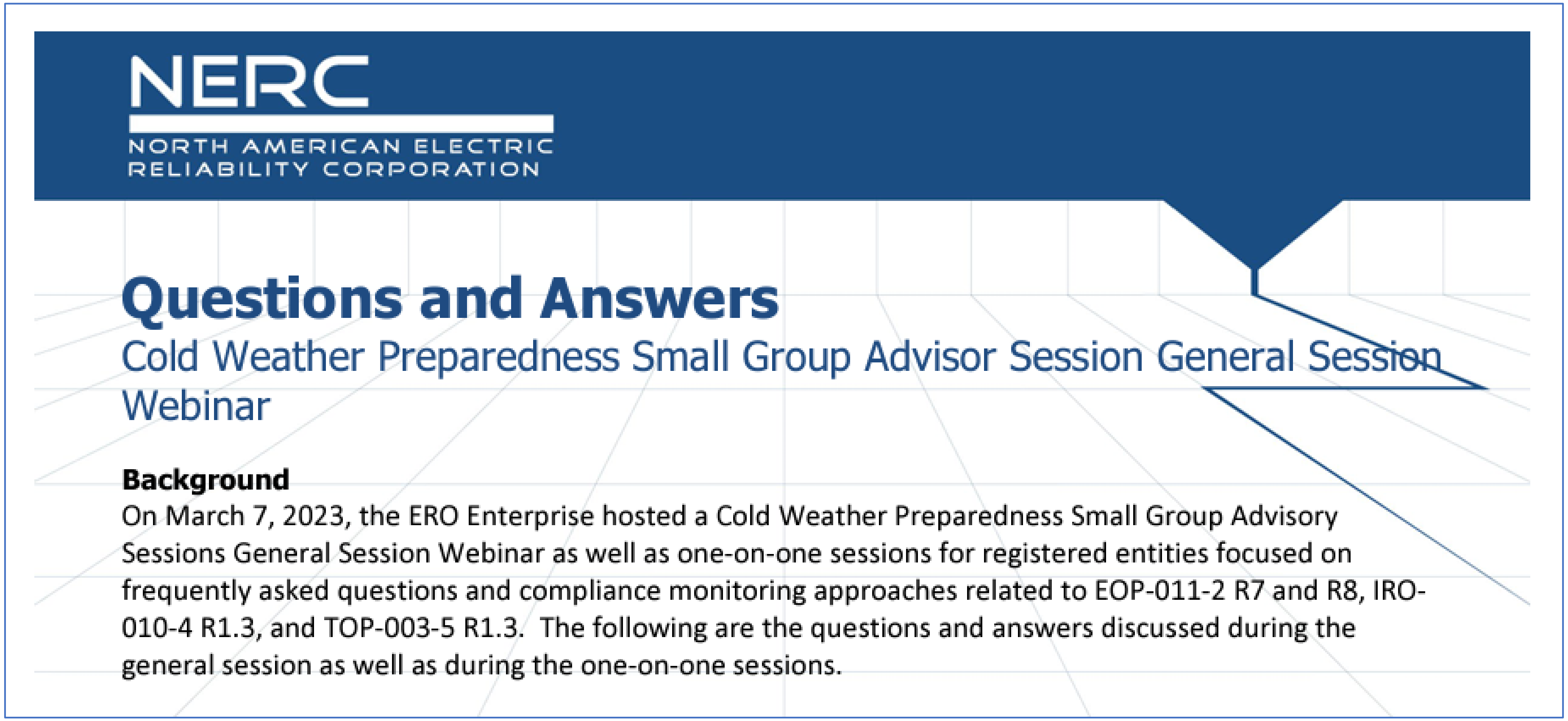
- Effective October 01, 2024
- Replacing EOP-011-2 R7 and R8
- EOP-012-1 – Extreme Cold Weather Preparedness and Operations
- Project 2021-07 Extreme Cold Weather Implementation Plan

Standard Changes

What Controls Have We Seen?

- Periodic review of the process to ensure:
  - Correct version of the Standard is addressed
  - Initial training/inspection was completed per the implementation plan
  - That all connected Standards are addressed correctly

Useful Documents



NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Questions and Answers

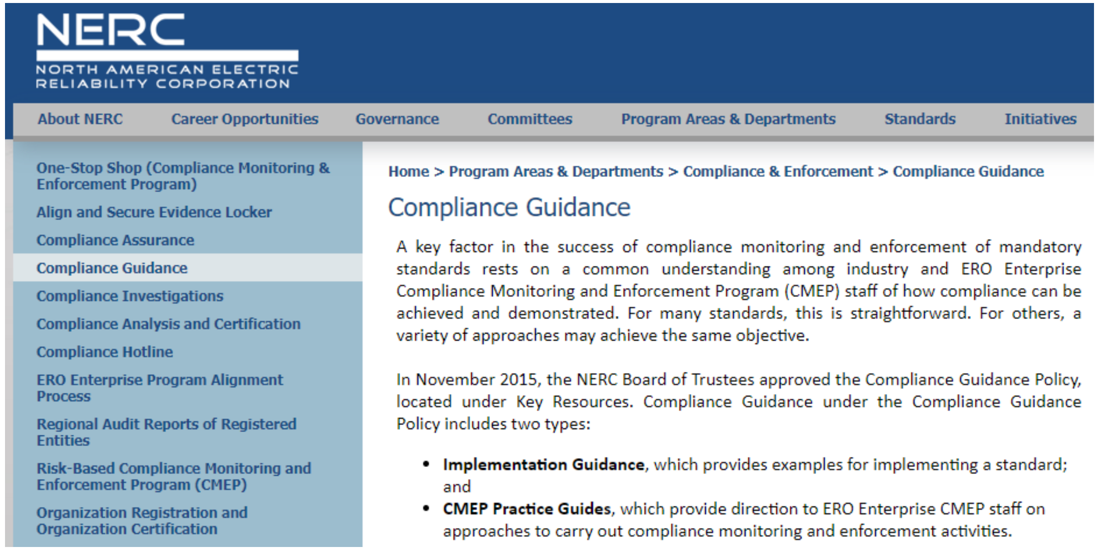
Cold Weather Preparedness Small Group Advisor Session General Session Webinar

Background

On March 7, 2023, the ERO Enterprise hosted a Cold Weather Preparedness Small Group Advisory Sessions General Session Webinar as well as one-on-one sessions for registered entities focused on frequently asked questions and compliance monitoring approaches related to EOP-011-2 R7 and R8, IRO-010-4 R1.3, and TOP-003-5 R1.3. The following are the questions and answers discussed during the general session as well as during the one-on-one sessions.

https://www.nerc.com/pa/comp/CAOneStopShop/Cold%20Weather%20Preparedness%20FAQ.pdf

Useful Documents



NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION
About NERC
Career Opportunities
Governance
Committees
Program Areas & Departments
Standards
Initiatives
One-Stop Shop (Compliance Monitoring & Enforcement Program)
Align and Secure Evidence Locker
Compliance Assurance
Compliance Guidance
Compliance Investigations
Compliance Analysis and Certification
Compliance Hotline
ERO Enterprise Program Alignment Process
Regional Audit Reports of Registered Entities
Risk-Based Compliance Monitoring and Enforcement Program (CMEP)
Organization Registration and Organization Certification
Home > Program Areas & Departments > Compliance & Enforcement > Compliance Guidance

Compliance Guidance

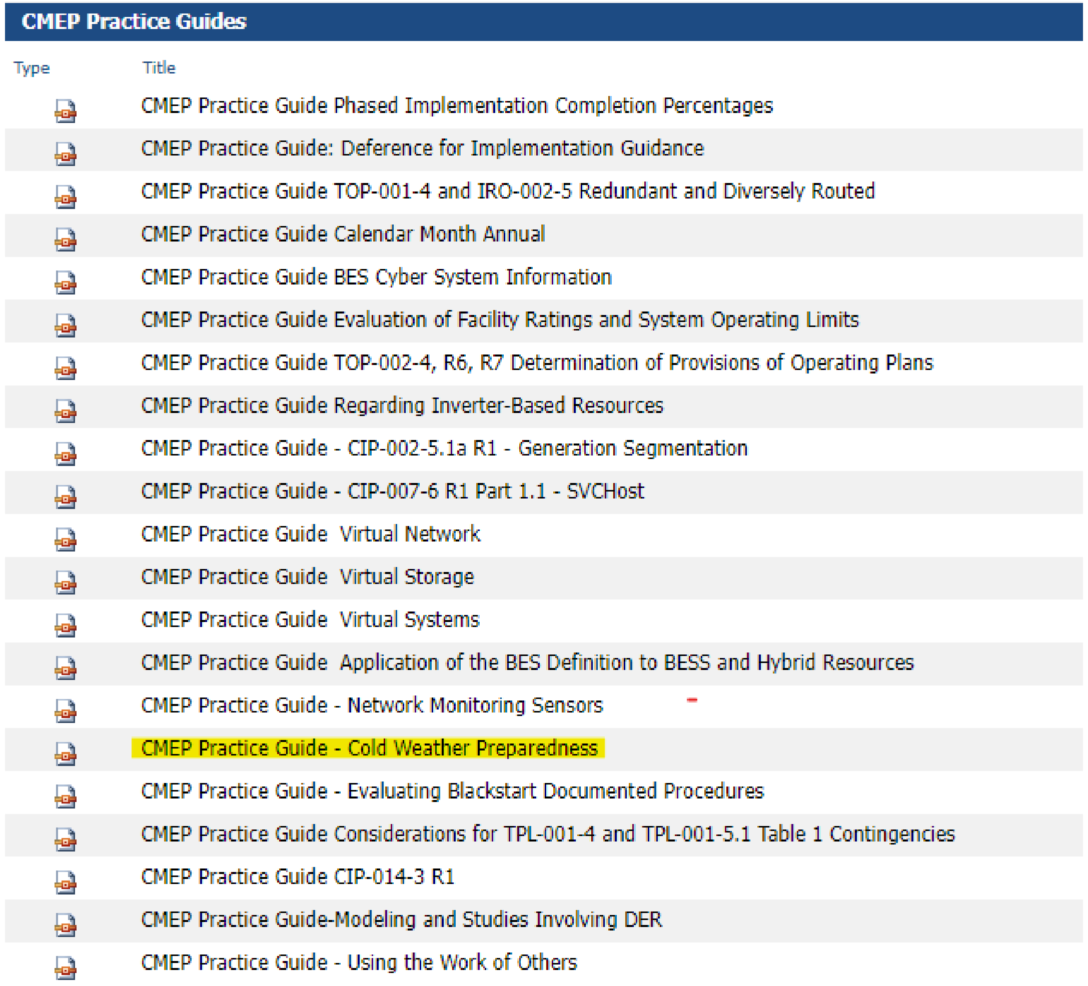
A key factor in the success of compliance monitoring and enforcement of mandatory standards rests on a common understanding among industry and ERO Enterprise Compliance Monitoring and Enforcement Program (CMEP) staff of how compliance can be achieved and demonstrated. For many standards, this is straightforward. For others, a variety of approaches may achieve the same objective.

In November 2015, the NERC Board of Trustees approved the Compliance Guidance Policy, located under Key Resources. Compliance Guidance under the Compliance Guidance Policy includes two types:

- **Implementation Guidance**, which provides examples for implementing a standard; and
- **CMEP Practice Guides**, which provide direction to ERO Enterprise CMEP staff on approaches to carry out compliance monitoring and enforcement activities.

[Compliance Guidance (nerc.com)](#)

[CMEP Practice Guide - Cold Weather Preparedness](#)



CMEP Practice Guides

Type	Title
📄	CMEP Practice Guide Phased Implementation Completion Percentages
📄	CMEP Practice Guide: Deference for Implementation Guidance
📄	CMEP Practice Guide TOP-001-4 and IRO-002-5 Redundant and Diversely Routed
📄	CMEP Practice Guide Calendar Month Annual
📄	CMEP Practice Guide BES Cyber System Information
📄	CMEP Practice Guide Evaluation of Facility Ratings and System Operating Limits
📄	CMEP Practice Guide TOP-002-4, R6, R7 Determination of Provisions of Operating Plans
📄	CMEP Practice Guide Regarding Inverter-Based Resources
📄	CMEP Practice Guide - CIP-002-5.1a R1 - Generation Segmentation
📄	CMEP Practice Guide - CIP-007-6 R1 Part 1.1 - SVCHost
📄	CMEP Practice Guide Virtual Network
📄	CMEP Practice Guide Virtual Storage
📄	CMEP Practice Guide Virtual Systems
📄	CMEP Practice Guide Application of the BES Definition to BESS and Hybrid Resources
📄	CMEP Practice Guide - Network Monitoring Sensors
📄	CMEP Practice Guide - Cold Weather Preparedness
📄	CMEP Practice Guide - Evaluating Blackstart Documented Procedures
📄	CMEP Practice Guide Considerations for TPL-001-4 and TPL-001-5.1 Table 1 Contingencies
📄	CMEP Practice Guide CIP-014-3 R1
📄	CMEP Practice Guide-Modeling and Studies Involving DER
📄	CMEP Practice Guide - Using the Work of Others

Useful Documents

Questions for Understanding Entity Cold Weather Preparedness Risk Mitigation and Practices

- CMEP staff shall consider the data points provided by the following questions to gain an understanding of how an entity mitigates risk relative to cold weather preparedness. The risk mitigation practices and controls identified through these questions can affect monitoring activities, including requests for information and adjustments to an entity’s compliance oversight plan and future monitoring activities.
  - Reliability Coordinator (RC): eight questions with sub parts.
  - Balancing Authority (BA): six questions with sub parts.
  - Transmission Operator (TOP): 10 questions with sub parts.
  - Generator Owner (GO)/Generator Operator (GOP): 17 questions with sub parts.
  - Planning Authority/Planning Coordinator (PA/PC): six questions with sub parts.
  - BA, TOP, GO, and GOP: seven questions with sub parts.

Useful Documents

NERC

- □Project 2019-06 Cold Weather (nerc.com)
- □EOP-011-2 Emergency Preparedness and Operations
- □ERO Enterprise CMEP Practice Guide Cold Weather Preparedness v1.0
- □Cold Weather Preparedness FAQ.pdf
- □Cold Weather Training Materials (nerc.com)
- □NERC Information Resources on Cold Weather Preparation and BPS Impacts

ERCOT/PUC

- □ERCOT Historical Weather Study Final Report Version 1.1
- □Interchange - Filings (texas.gov)

Change Management Controls

EOP-011-2 R7 and R8

- Eric Newnam, O&P Compliance Engineer III

CIP-003-8 and CIP-012-1

- Paul Hopson, CIP Compliance Team Lead

How Internal Controls are Viewed in Enforcement

- Kaitlin Van Zee, Director, Enforcement & Registration

Internal Controls

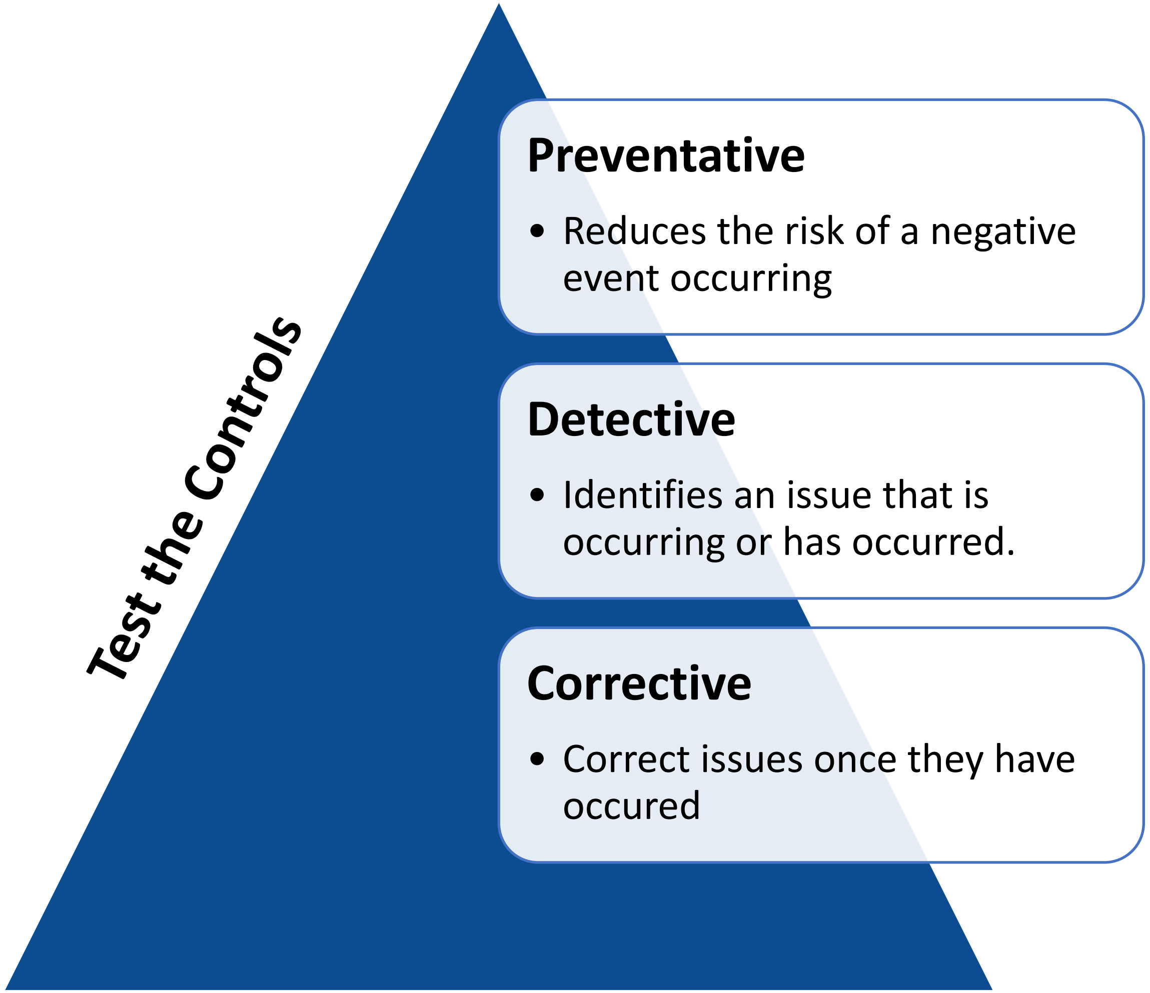
❑Internal Controls Overview

- **Internal controls help companies operate effectively and efficiently, reduce the risk of noncompliance, and improve the reliability of the Bulk Electric System (BES). As part of the Compliance Audit, Spot Check, and Self-Certification process, auditors will review subsets of an entity's internal controls. Auditors will then provide feedback to the Texas RE Risk Assessments Group for the entity's Compliance Oversight Plan (COP) and to inform future engagement scheduling and engagement scopes.**

Internal Controls

- Texas RE’s experience is that many entities have internal controls, but entities do not always recognize their existing internal controls as “internal controls.” Often, this is because the control is part of the company’s normal business process and is not specifically called out as an internal control.
- We want to help entities identify existing internal controls and provide a general overview for building out internal controls for applicable Requirements.

Internal Controls



Test the Controls

Preventative

- Reduces the risk of a negative event occurring

Detective

- Identifies an issue that is occurring or has occurred.

Corrective

- Correct issues once they have occured

NERC CIP-003-8 and CIP-012-1 Standards

Standard Requirement	Procedural Requirement
CIP-003-8 R1	Review and obtain CIP Senior Manager approval for one or more documented cyber security policies that collectively address the topics found in 1.1 (1.1.1 – 1.1.9) and 1.2 (1.2.1-1.2.6).
CIP-003-8 R2	Implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1 Sections 1-5. • Section 1 – Cyber Security Awareness • Section 2 – Physical Security Controls • Section 3 – Electronic Access Controls • Section 4 – Cyber Security Incident Response • Section 5 – Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation
CIP-003-8 R3	Identify a CIP Senior Manager by name.
CIP-003-8 R4	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. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator.
CIP-012-1 R1	Implement, except under CIP Exceptional Circumstances, one or more documented plan(s) to mitigate the risks posed by unauthorized disclosure and unauthorized modification of Real-time Assessment and Real-time monitoring data while being transmitted between any applicable Control Centers.

Change Management Internal Controls for CIP-003-8 R2

Standard Requirement	Control Considerations
CIP-003-8 R2 **Section 1** – Cyber Security Awareness	**Preventative Controls** • Train personnel on cyber security awareness reinforcement • Utilize multiple methods of reinforcement (direct and indirect communications, etc.) • Retain all evidence associated with reinforcement **Detective Controls** • Establish alerts or reminders to prevent missing due dates • Reminders for periodic cyber security awareness reinforcement before annual due date (every 15 calendar months) **Corrective Controls** • Actions required to remediate any late reinforcements.

Change Management Internal Controls for CIP-003-8 R2

Standard Requirement	Control Considerations
CIP-003-8 R2 **Section 2** – Physical Security Controls	**Preventative Controls** - Train personnel on physical access controls - Utilize layered (multiple) physical access controls - Utilize key management controls for locks, doors, etc. - Utilize a visitor access control program - Document physical security perimeter diagrams **Detective Controls** - Reminders for periodic review of physical access controls - Utilize alarms and alerting for unauthorized physical access **Corrective Controls** - Actions required to remediate any non-working physical access controls - Actions required to remediate any unauthorized physical access.

Change Management Internal Controls for CIP-003-8 R2

Standard Requirement	Control Considerations
CIP-003-8 R2 **Section 3** – Electronic Access Controls	**Preventative Controls** • Train personnel on electronic access controls • Utilize defense in depth electronic access controls applying the concept of least privilege • Evaluate and document all justifications for inbound and outbound electronic access • Utilize controls for malicious code and communications • Utilize controls for vendor remote access • Document network diagrams **Detective Controls** • Reminders for periodic review of electronic access controls • Utilize alarms and alerting for unauthorized electronic access and malicious code and communications **Corrective Controls** • Actions required to remediate any broadly defined electronic access controls • Actions required to remediate any unauthorized electronic access and malicious code communications

Change Management Internal Controls for CIP-003-8 R2

Standard Requirement	Control Considerations
CIP-003-8 R2 **Section 4** – Cyber Security Incident Response	**Preventative Controls** • Train personnel on Cyber Security Incident Response • Incorporate both the IT and OT personnel including O&P personnel when implementing or testing the Cyber Security Incident response plan(s) • Subscribe to DHS CISA industry alerts • Retain all evidence associated with testing or actual Reportable Cyber Security Incidents **Detective Controls** • Reminders for periodic testing of the Cyber Security Incident response plan(s) at least once every 36 calendar months • Reminders for updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after the test • Utilize security event logs, alarms, and alerting of detected Cyber Security Incidents **Corrective Controls** • Actions required to remediate any late testing • Actions required to contain, eradicate, or have recovery/incident resolution of Cyber Security Incidents

Change Management Internal Controls for CIP-003-8 R2

Standard Requirement	Control Considerations
CIP-003-8 R2 **Section 5** – Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation	**Preventative Controls** • Train personnel on Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation • Inventory all TCA and RM including the location where they will be utilized • Utilize the concept of least privilege and need to know for personnel who need TCA or RM access • Ensure malicious code detection methods are up to date and effective • Utilize controls for vendor owned TCA or RM • Block unauthorized TCA or RM • Retain all evidence associated with the utilization of any TCA or RM **Detective Controls** • Reminders for periodic review and evaluation of TCA, RM, and malicious code methods • Utilize security event logs, alarms, and alerting for unauthorized TCA or RM usage • Utilize security event logs, alarms, and alerting for out-of-date malicious code methods **Corrective Controls** • Actions required to remediate any unauthorized TCA or RM • Force malicious code method updates

Change Management Internal Controls for CIP-012-1 R1

Standard Requirement	Control Considerations
CIP-012-1 R1 – Implement, except under CIP Exceptional Circumstances, one or more documented plan(s) to mitigate the risks posed by unauthorized disclosure and unauthorized modification of Real-time Assessment and Real-time monitoring data while being transmitted between any applicable Control Centers.	**Preventative Controls** • Train personnel on the identification of Control Centers per the NERC Glossary of Terms • Train personnel on the identification of Real-time Assessment and Real-time monitoring data • Utilize controls to protect the confidentiality and integrity of Real-time Assessment and Real-time monitoring data (e.g., encryption) • Collaboration and implementation of controls with Control Centers that are owned or operated by different Responsible Entities • Document network diagrams, network configurations, and collaboration with Control Centers that are owned or operated by different Responsible Entities **Detective Controls** • Utilize alarms and alerting for unauthorized disclosure and unauthorized modification of Real-time Assessment and Real-time monitoring data • Utilize alarms and alerting for failures of controls implemented **Corrective Controls** • Actions required to remediate any failures of controls implemented

Top Five Internal Controls for CIP-003-8 R2

1

Access Control:
Implement access controls to regulate and monitor access to low impact BES Cyber Systems. This includes authentication and authorization, even for low impact assets, to prevent unauthorized access.

2

Change Management:
Establish a simplified change management process to track and control changes made to low impact BES Cyber Assets. This should include documenting changes and ensuring basic testing before implementation.

3

Security Patch Management:
Develop a process for identifying, evaluating, and applying security patches and updates to low impact BES Cyber Assets. Even low impact assets should receive security patches to address vulnerabilities.

4

Vulnerability Awareness:
Maintain a basic awareness of vulnerabilities in low impact assets. While the level of scrutiny may be lower, periodically assessing vulnerabilities and taking steps to mitigate them is essential.

5

Basic Logging and Monitoring:
Implement basic logging and monitoring of low impact Cyber Assets. While not as extensive as for high and medium assets, some level of monitoring should be in place to detect potential unauthorized access or activities.

Top Five Internal Controls for CIP-012-1 R1

1

Risk Assessment:
Conduct a comprehensive risk assessment to identify and evaluate the potential threats and vulnerabilities that could impact the operation of the BES. This should include a systematic analysis of risks to help prioritize security measures.

2

BES Cyber Asset Identification:
Identify and classify BES Cyber Assets. These are assets that are crucial for the reliable operation an of the electric grid and require enhanced protection and monitoring.

3

Security Management:
Develop and implement a comprehensive security management program that includes policies, procedures, and controls to protect BES Cyber Assets. This program should address both physical and cybersecurity aspects of security.

4

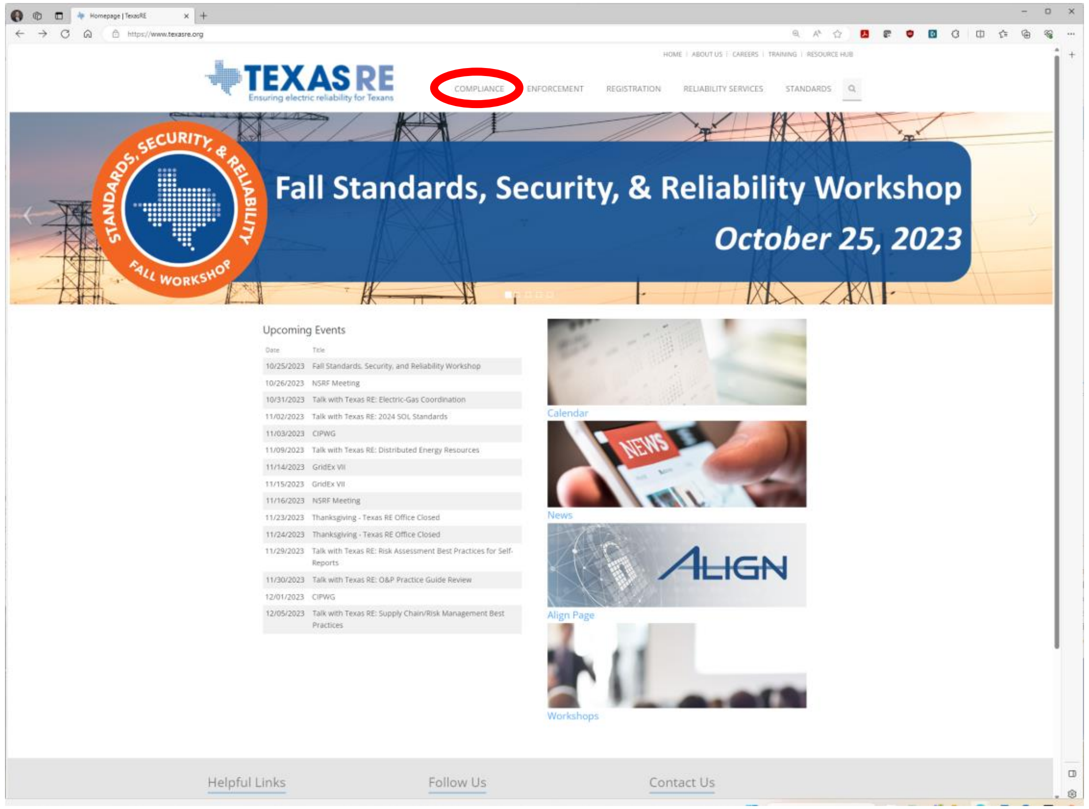
Access Control:
Implement access controls for BES Cyber Assets. This involves managing and monitoring access, both physical and electronic, to ensure that only authorized personnel have access to these vital components.

5

Incident Response Plan:
Develop and maintain a well-defined incident response plan tailored specifically to address security incidents related to BES Cyber Assets. The plan should include procedures for detection, response, and recovery.

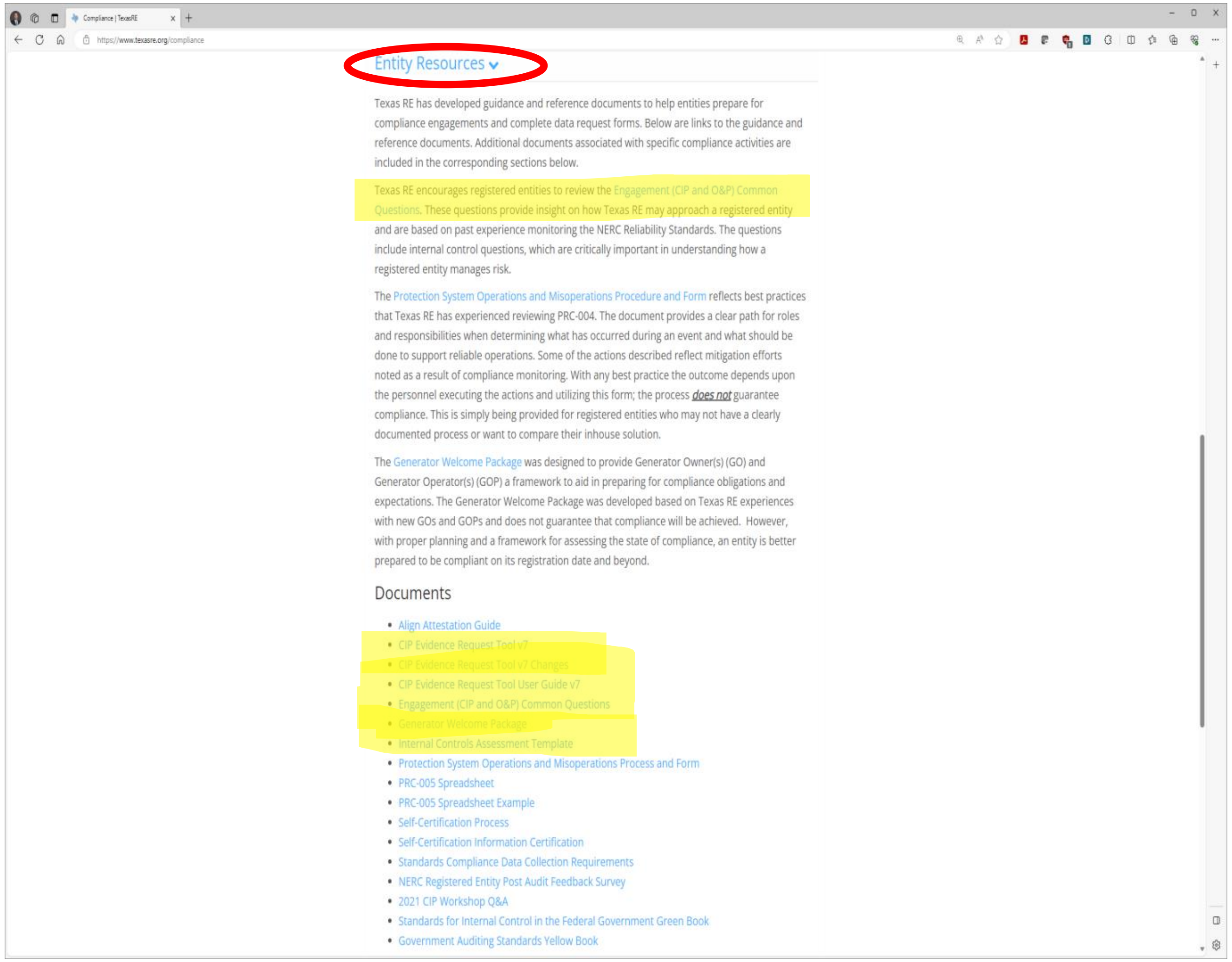
Public

Texas RE’s Website - Entity Resources



Upcoming Events

Date	Title
10/25/2023	Fall Standards, Security, and Reliability Workshop
10/26/2023	NSRF Meeting
10/31/2023	Talk with Texas RE: Electric-Gas Coordination
11/02/2023	Talk with Texas RE: 2024 SOL Standards
11/03/2023	CIPWG
11/09/2023	Talk with Texas RE: Distributed Energy Resources
11/14/2023	GridEx VII
11/15/2023	GridEx VII
11/16/2023	NSRF Meeting
11/23/2023	Thanksgiving - Texas RE Office Closed
11/24/2023	Thanksgiving - Texas RE Office Closed
11/29/2023	Talk with Texas RE: Risk Assessment Best Practices for Self-Reports
11/30/2023	Talk with Texas RE: O&P Practice Guide Review
12/01/2023	CIPWG
12/05/2023	Talk with Texas RE: Supply Chain/Risk Management Best Practices



Entity Resources

Texas RE has developed guidance and reference documents to help entities prepare for compliance engagements and complete data request forms. Below are links to the guidance and reference documents. Additional documents associated with specific compliance activities are included in the corresponding sections below.

Texas RE encourages registered entities to review the Engagement (CIP and O&P) Common Questions. These questions provide insight on how Texas RE may approach a registered entity and are based on past experience monitoring the NERC Reliability Standards. The questions include internal control questions, which are critically important in understanding how a registered entity manages risk.

The Protection System Operations and Misoperations Procedure and Form reflects best practices that Texas RE has experienced reviewing PRC-004. The document provides a clear path for roles and responsibilities when determining what has occurred during an event and what should be done to support reliable operations. Some of the actions described reflect mitigation efforts noted as a result of compliance monitoring. With any best practice the outcome depends upon the personnel executing the actions and utilizing this form; the process ***does not*** guarantee compliance. This is simply being provided for registered entities who may not have a clearly documented process or want to compare their inhouse solution.

The Generator Welcome Package was designed to provide Generator Owner(s) (GO) and Generator Operator(s) (GOP) a framework to aid in preparing for compliance obligations and expectations. The Generator Welcome Package was developed based on Texas RE experiences with new GOs and GOPs and does not guarantee that compliance will be achieved. However, with proper planning and a framework for assessing the state of compliance, an entity is better prepared to be compliant on its registration date and beyond.

Documents

- Align Attestation Guide
- CIP Evidence Request Tool v7
- CIP Evidence Request Tool v7 Changes
- CIP Evidence Request Tool User Guide v7
- Engagement (CIP and O&P) Common Questions
- Generator Welcome Package
- Internal Controls Assessment Template
- Protection System Operations and Misoperations Process and Form
- PRC-005 Spreadsheet
- PRC-005 Spreadsheet Example
- Self-Certification Process
- Self-Certification Information Certification
- Standards Compliance Data Collection Requirements
- NERC Registered Entity Post Audit Feedback Survey
- 2021 CIP Workshop Q&A
- Standards for Internal Control in the Federal Government Green Book
- Government Auditing Standards Yellow Book

Change Management Controls

EOP-011-2 R7 and R8

- Eric Newnam, O&P Compliance Engineer III

CIP-003-8 and CIP-012-1

- Paul Hopson, CIP Compliance Team Lead

How Internal Controls are Viewed in Enforcement

- Kaitlin Van Zee, Director, Enforcement & Registration

Change Management Controls and Enforcement

Risk Assessment

Efficiency in Enforcement Processing

Streamlined Dispositions

Risk Assessment

Risk Can Be…

- Minimal
- Moderate
- Serious

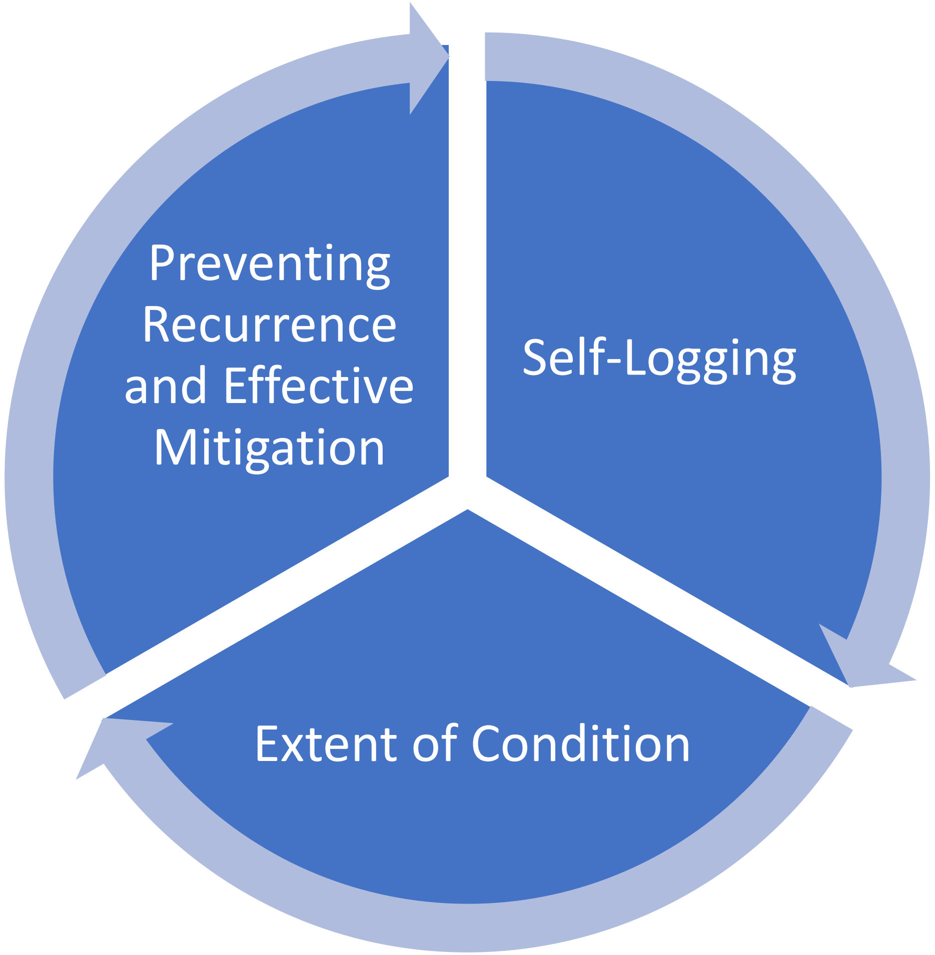
***Appendix 4B § 3.2.3, NERC Rules of Procedure

Factors Reducing the Risk

- Internal controls
- Early detection
- Redundancies

"The registered entity should include details on any internal controls that were in place that quickened the discovery of the noncompliance, shortened the duration of the noncompliance, or reduced the severity of the impact of the noncompliance." *ERO Registered Entity Self-Report and Mitigation User Guide*, June 2018, at p. 12.

Efficiency in Enforcement Processing



Self-Logging

Alternative to Self-Reporting for Minimal Risk Potential Noncompliance (PNC)

All Registered Entities may apply

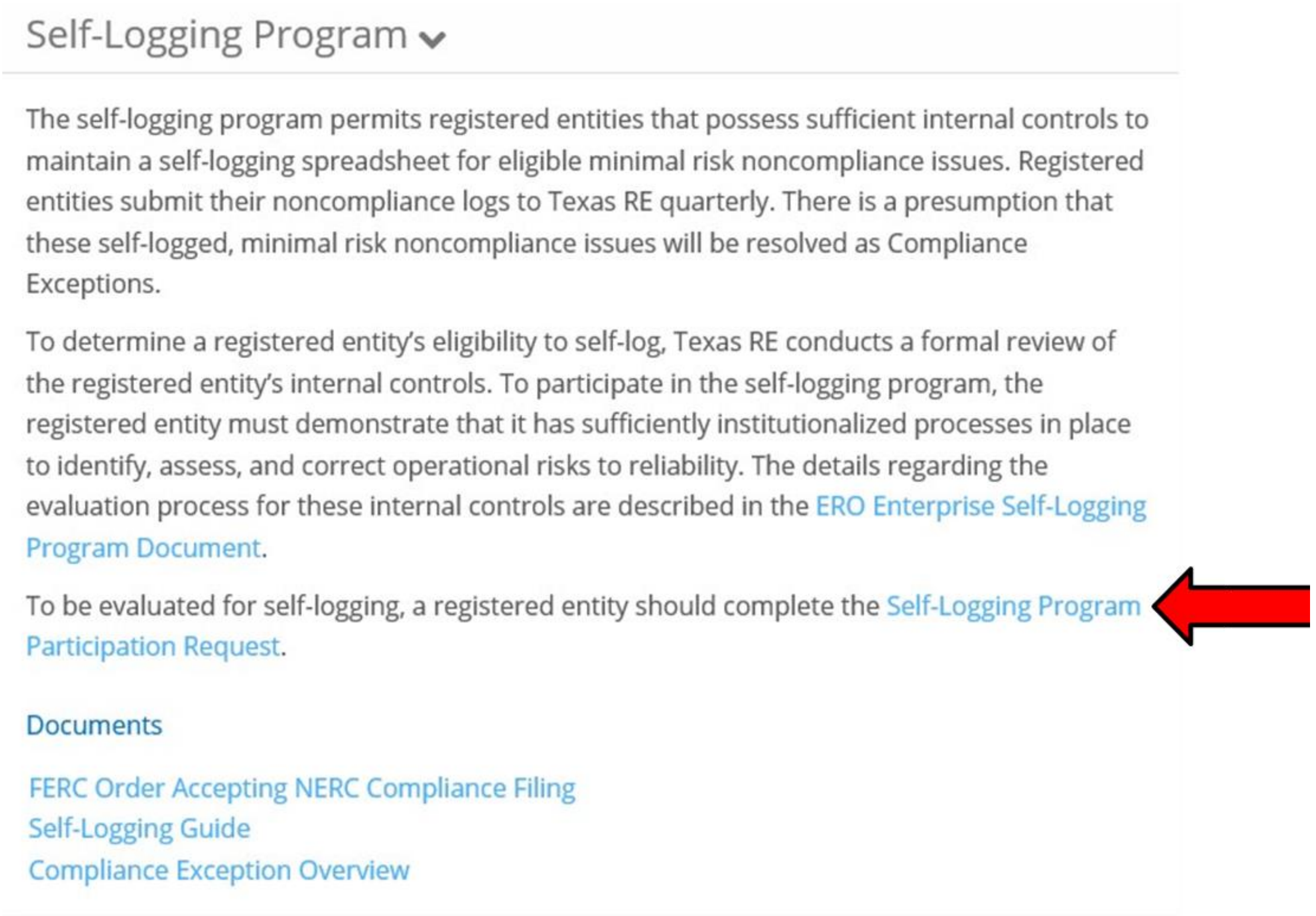
Eligibility Criteria

- Compliance history
- Texas RE’s experience with your entity
- Evidence of effective processes for identifying possible noncompliance
- Timing and quality of self-reports
- Risk Assessment ability/quality
- Mitigation Performance
- Internal Compliance Program
- Inherent Risk Assessment
- Proposed Self-Logging procedure (optional)

NERC Self-Logging User Guide

Benefits of Self-Logging

- Presumption of compliance exemption (CE) treatment
- Fewer (if any) requests for information (RFIs)
- No evidence submission required
- Faster processing



Self-Logging Program

The self-logging program permits registered entities that possess sufficient internal controls to maintain a self-logging spreadsheet for eligible minimal risk noncompliance issues. Registered entities submit their noncompliance logs to Texas RE quarterly. There is a presumption that these self-logged, minimal risk noncompliance issues will be resolved as Compliance Exceptions.

To determine a registered entity's eligibility to self-log, Texas RE conducts a formal review of the registered entity's internal controls. To participate in the self-logging program, the registered entity must demonstrate that it has sufficiently institutionalized processes in place to identify, assess, and correct operational risks to reliability. The details regarding the evaluation process for these internal controls are described in the ERO Enterprise Self-Logging Program Document.

To be evaluated for self-logging, a registered entity should complete the Self-Logging Program Participation Request.

Documents

FERC Order Accepting NERC Compliance Filing
Self-Logging Guide
Compliance Exception Overview

Public

Extent of Condition (EOC)

Needed for Description of PNC

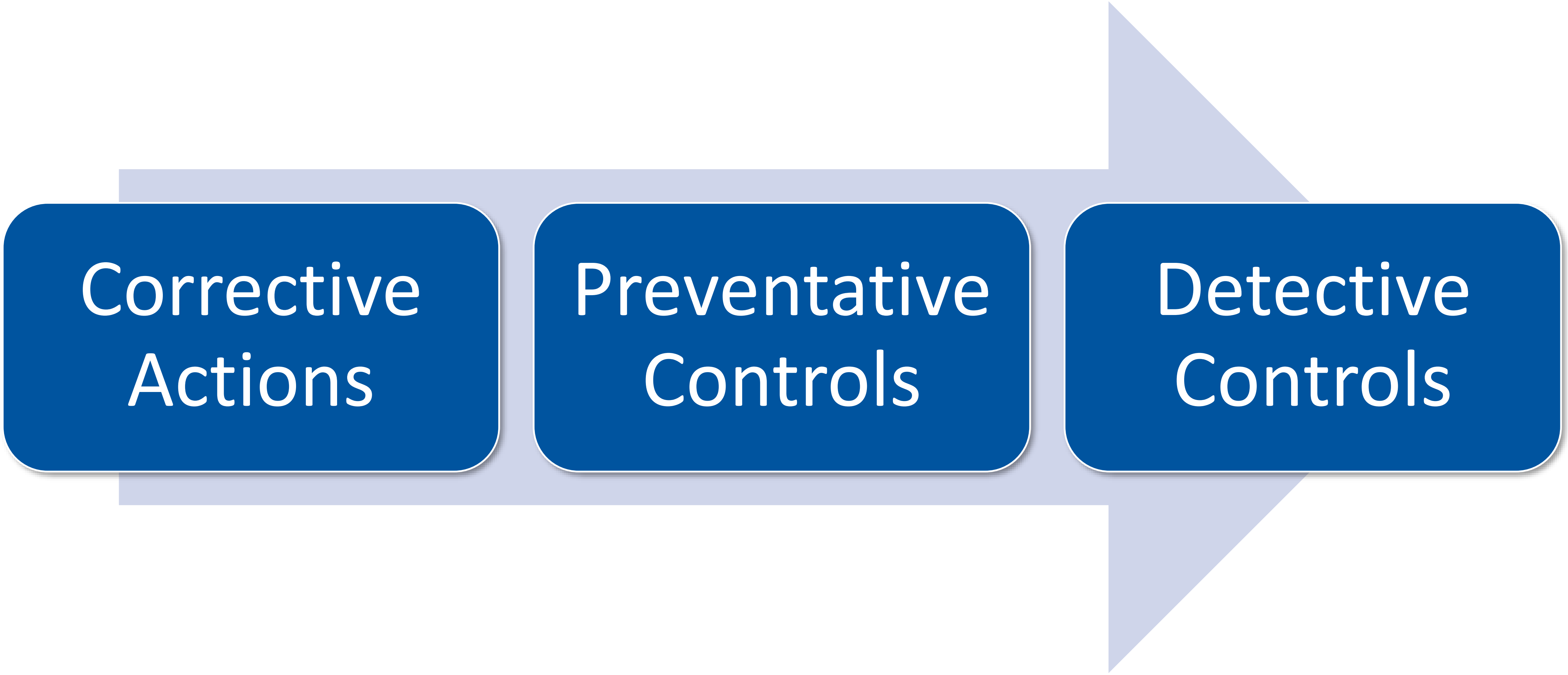
- Facts and Circumstances of the PNC
- Risk Assessment
- Root Cause

“Integral to successful mitigation”

- ERO Registered Entity Self-Report and Mitigation User Guide, June 2018 a p. 9.

Robust Internal Controls may suffice for EOC

Preventing Recurrence and Effective Mitigation



Corrective Actions

Preventative Controls

Detective Controls

Streamlined Dispositions

CE and Find, Fix, Track and Report (FFT)

- Appendix 4C § 4A.0 Enforcement Discretion, NERC Rules of Procedure

CEs are not included in a registered entity’s compliance history for penalty purposes

Faster processing times

Questions?

TEXAS RE

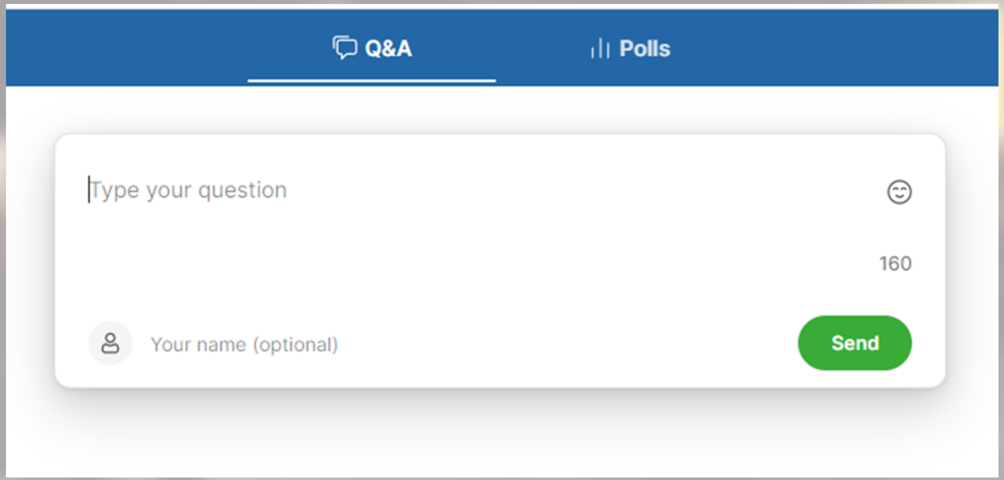
Ensuring electric reliability for Texans

Fall Standards, Security, & Reliability Workshop

Return at: 2:05 p.m.

- New BCSI in the Cloud Standards
- FERC Vulnerability and Physical Security Assessment Program
- New Weatherization Requirements
- Emerging Cyber and Physical Risks
- Entity Ownership Change Considerations
- Cyber Informed Transmission Planning
- Change Management Controls
- **Emerging Issues with Distributed Energy Resources**
- Grid Forming Inverter Technology: Opportunities for a Changing Grid

To submit questions during the workshop, please visit **slido.com** and enter today's participant code: **TXRE**



ADER Pilot Project Status Update

Jason M. Ryan

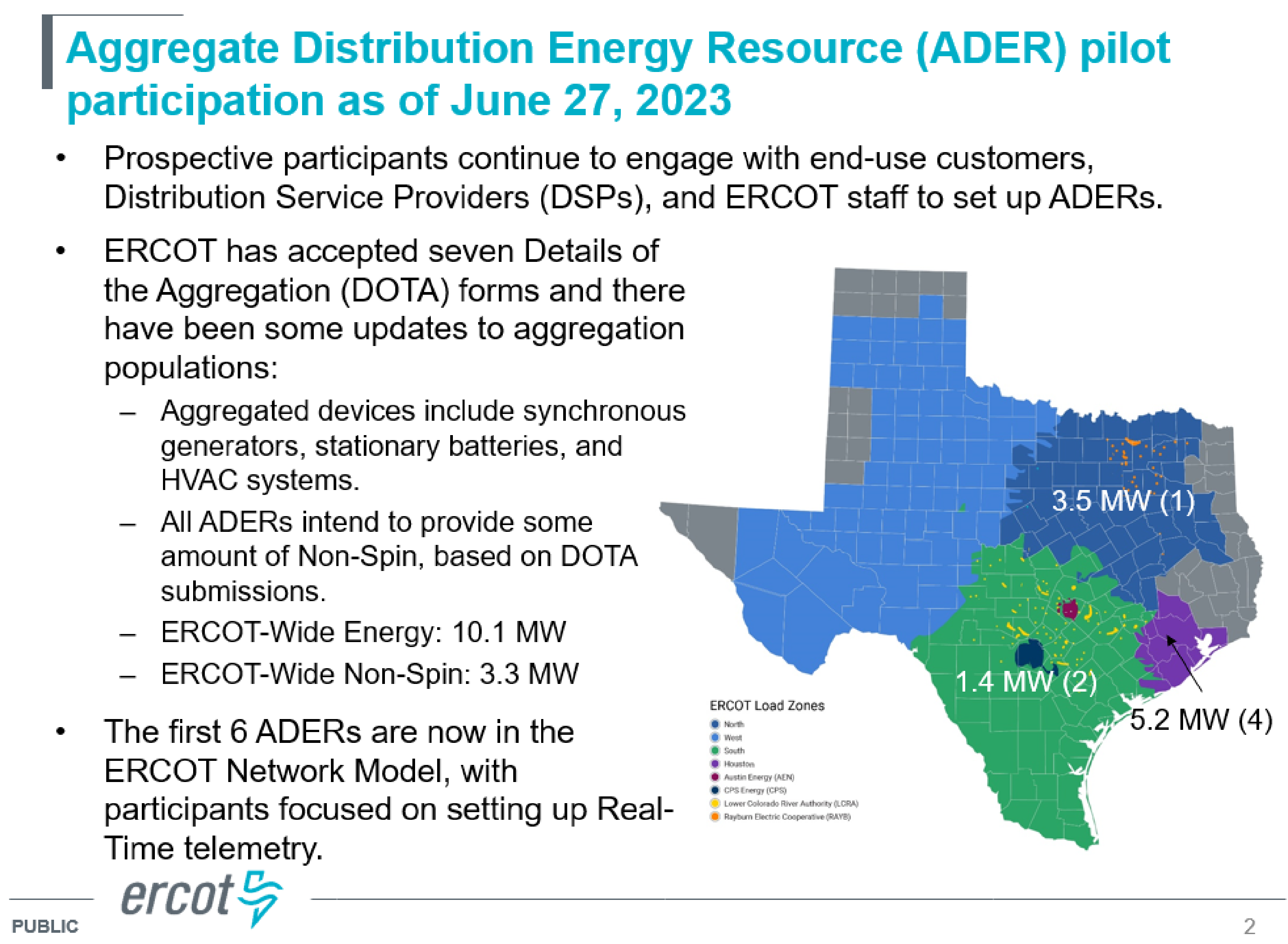
Texas RE Fall Workshop
25 October 2023

CenterPoint Energy

ADER Pilot Project Overview

- Task Force began its work AUG22
  - Completed governing document SEP22
    - Contemplates pilot project in phases, over 3 years
  - ERCOT approved pilot project governing document OCT22
  - PUC approved governing document NOV22
- Phase 1 pilot project began JAN23
  - 80MW limit across ERCOT
  - 40MW limit on non-spin
- Both the Task Force and ERCOT must study and report once ADERs become operational during Phase 1
- Task Force Year 1 overview presentation at the PUC’s 24AUG23 open meeting

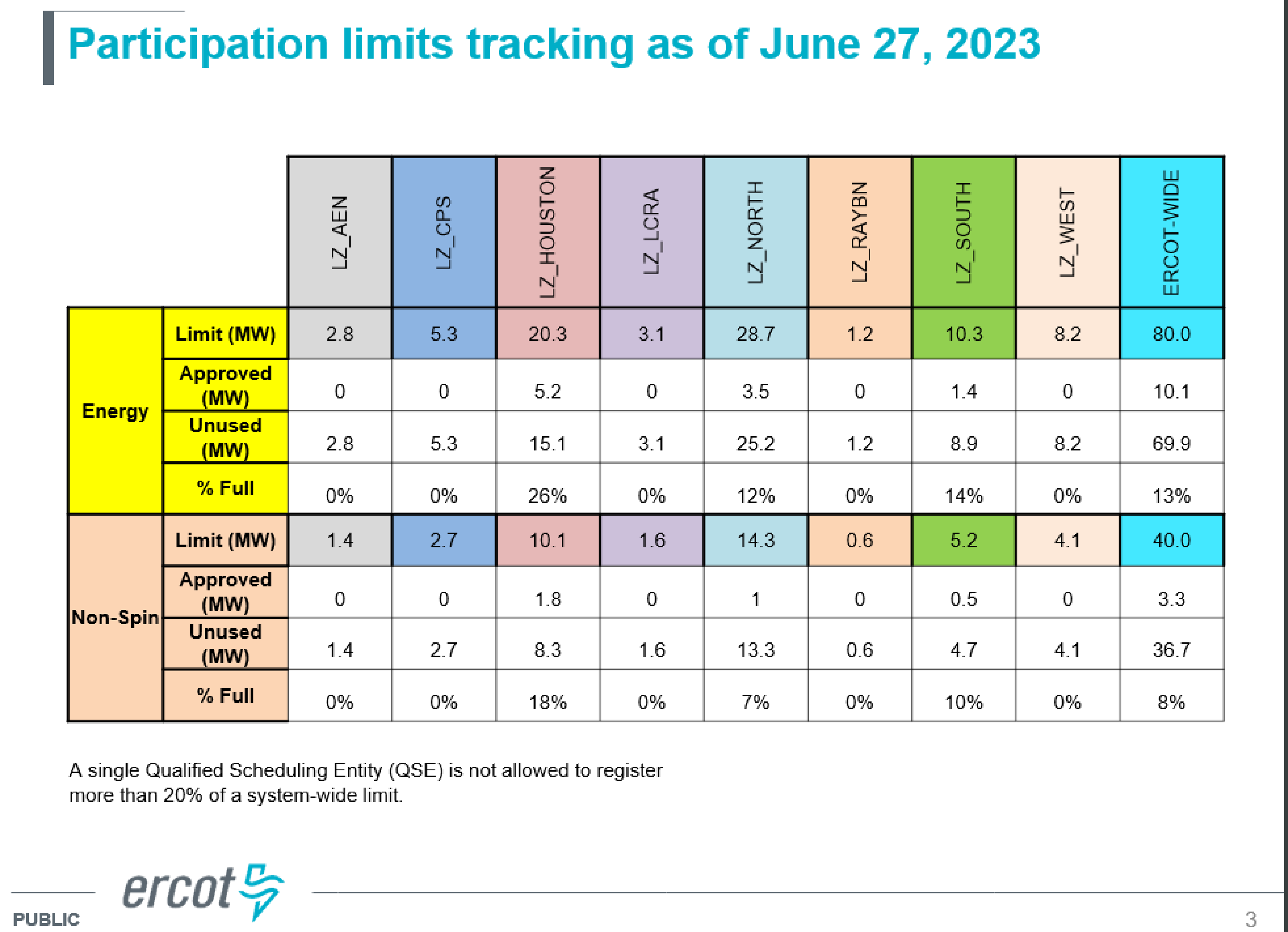
ERCOT Status Update



Aggregate Distribution Energy Resource (ADER) pilot participation as of June 27, 2023

- Prospective participants continue to engage with end-use customers, Distribution Service Providers (DSPs), and ERCOT staff to set up ADERs.
- ERCOT has accepted seven Details of the Aggregation (DOTA) forms and there have been some updates to aggregation populations:
  - Aggregated devices include synchronous generators, stationary batteries, and HVAC systems.
  - All ADERs intend to provide some amount of Non-Spin, based on DOTA submissions.
  - ERCOT-Wide Energy: 10.1 MW
  - ERCOT-Wide Non-Spin: 3.3 MW
- The first 6 ADERs are now in the ERCOT Network Model, with participants focused on setting up Real-Time telemetry.

ERCOT Status Update (continued)



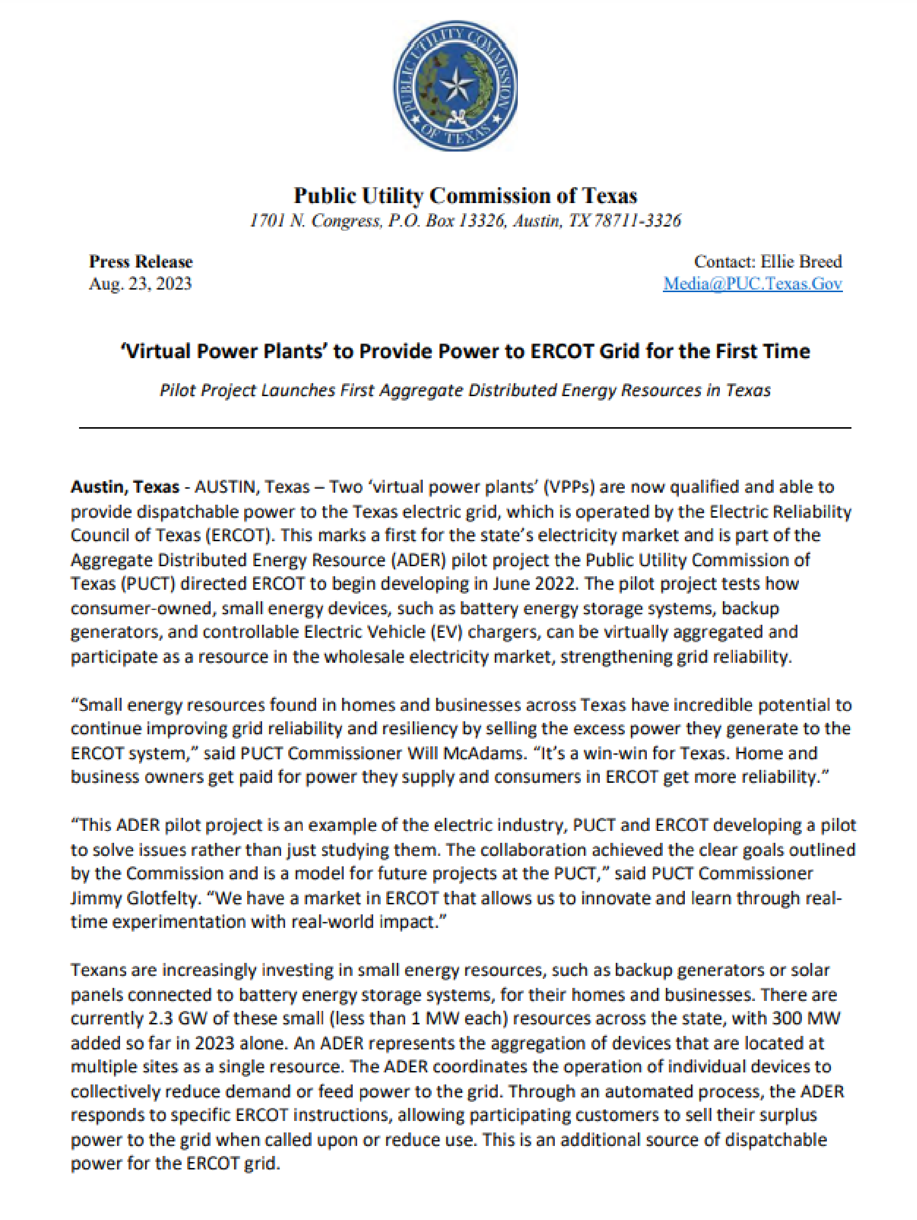
Participation limits tracking as of June 27, 2023

		LZ_AEN	LZ_CPS	LZ_HOUSTON	LZ_LCRA	LZ_NORTH	LZ_RAYBN	LZ_SOUTH	LZ_WEST	ERCOT-WIDE
Energy	Limit (MW)	2.8	5.3	20.3	3.1	28.7	1.2	10.3	8.2	80.0
	Approved (MW)	0	0	5.2	0	3.5	0	1.4	0	10.1
	Unused (MW)	2.8	5.3	15.1	3.1	25.2	1.2	8.9	8.2	69.9
	% Full	0%	0%	26%	0%	12%	0%	14%	0%	13%
Non-Spin	Limit (MW)	1.4	2.7	10.1	1.6	14.3	0.6	5.2	4.1	40.0
	Approved (MW)	0	0	1.8	0	1	0	0.5	0	3.3
	Unused (MW)	1.4	2.7	8.3	1.6	13.3	0.6	4.7	4.1	36.7
	% Full	0%	0%	18%	0%	7%	0%	10%	0%	8%

A single Qualified Scheduling Entity (QSE) is not allowed to register more than 20% of a system-wide limit.

ERCOT Status Update (continued)

- ADERs go live in AUG23
  - Houston
  - Dallas



Public Utility Commission of Texas
1701 N. Congress, P.O. Box 13326, Austin, TX 78711-3326

Press Release
Aug. 23, 2023

Contact: Ellie Breed
Media@PUC.Texas.Gov

'Virtual Power Plants' to Provide Power to ERCOT Grid for the First Time

Pilot Project Launches First Aggregate Distributed Energy Resources in Texas

Austin, Texas - AUSTIN, Texas – Two 'virtual power plants' (VPPs) are now qualified and able to provide dispatchable power to the Texas electric grid, which is operated by the Electric Reliability Council of Texas (ERCOT). This marks a first for the state's electricity market and is part of the Aggregate Distributed Energy Resource (ADER) pilot project the Public Utility Commission of Texas (PUCT) directed ERCOT to begin developing in June 2022. The pilot project tests how consumer-owned, small energy devices, such as battery energy storage systems, backup generators, and controllable Electric Vehicle (EV) chargers, can be virtually aggregated and participate as a resource in the wholesale electricity market, strengthening grid reliability.

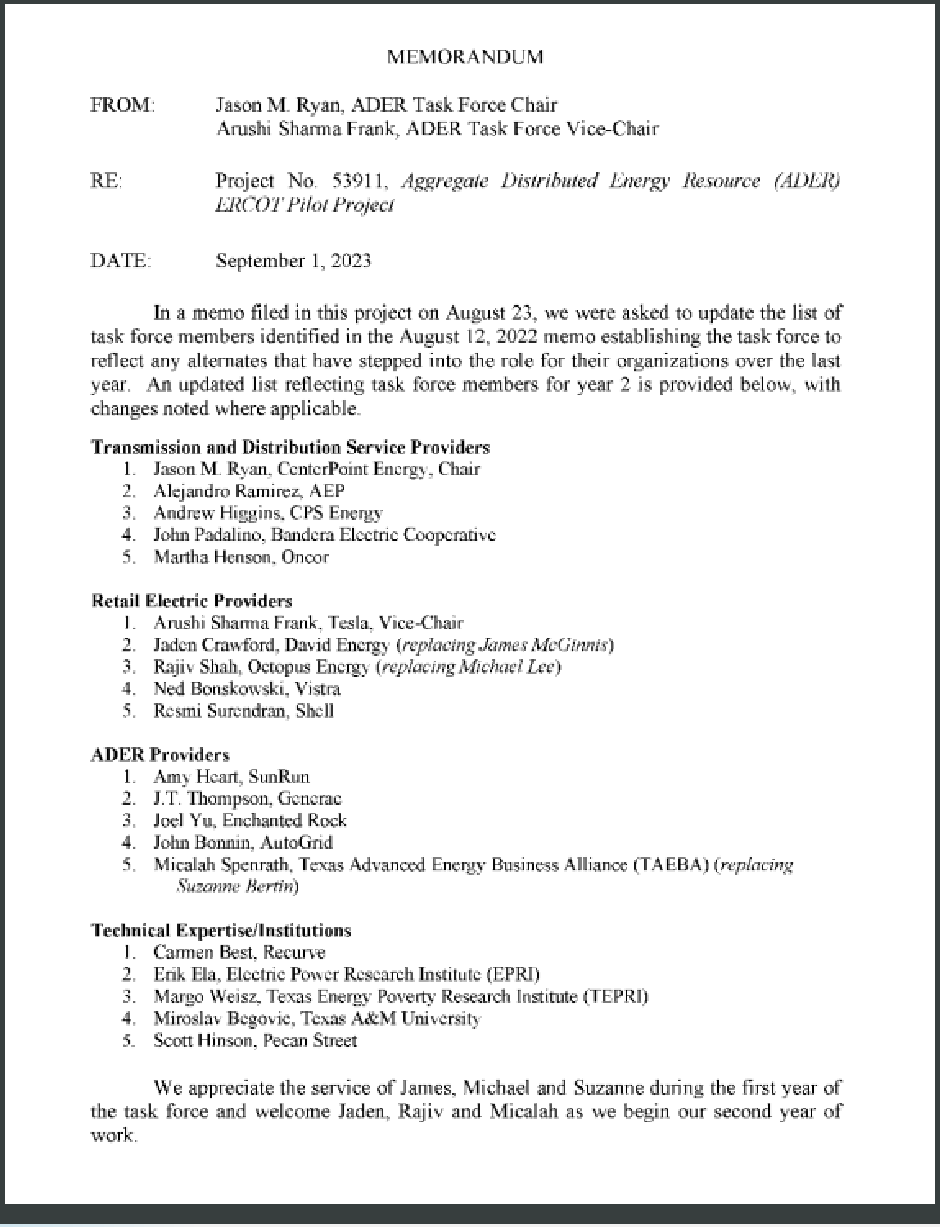
"Small energy resources found in homes and businesses across Texas have incredible potential to continue improving grid reliability and resiliency by selling the excess power they generate to the ERCOT system," said PUCT Commissioner Will McAdams. "It's a win-win for Texas. Home and business owners get paid for power they supply and consumers in ERCOT get more reliability."

"This ADER pilot project is an example of the electric industry, PUCT and ERCOT developing a pilot to solve issues rather than just studying them. The collaboration achieved the clear goals outlined by the Commission and is a model for future projects at the PUCT," said PUCT Commissioner Jimmy Glotfelty. "We have a market in ERCOT that allows us to innovate and learn through real-time experimentation with real-world impact."

Texans are increasingly investing in small energy resources, such as backup generators or solar panels connected to battery energy storage systems, for their homes and businesses. There are currently 2.3 GW of these small (less than 1 MW each) resources across the state, with 300 MW added so far in 2023 alone. An ADER represents the aggregation of devices that are located at multiple sites as a single resource. The ADER coordinates the operation of individual devices to collectively reduce demand or feed power to the grid. Through an automated process, the ADER responds to specific ERCOT instructions, allowing participating customers to sell their surplus power to the grid when called upon or reduce use. This is an additional source of dispatchable power for the ERCOT grid.

Task Force Status Update

- Task Force member refresh 01SEP23
- Year 2 of the Task Force began AUG23
- Year 2 of the Pilot will begin JAN24



MEMORANDUM

FROM: Jason M. Ryan, ADER Task Force Chair
Arushi Sharma Frank, ADER Task Force Vice-Chair

RE: Project No. 53911, *Aggregate Distributed Energy Resource (ADER) ERCOT Pilot Project*

DATE: September 1, 2023

In a memo filed in this project on August 23, we were asked to update the list of task force members identified in the August 12, 2022 memo establishing the task force to reflect any alternates that have stepped into the role for their organizations over the last year. An updated list reflecting task force members for year 2 is provided below, with changes noted where applicable.

Transmission and Distribution Service Providers

1. Jason M. Ryan, CenterPoint Energy, Chair
2. Alejandro Ramirez, AEP
3. Andrew Higgins, CPS Energy
4. John Padalino, Bandera Electric Cooperative
5. Martha Henson, Oncor

Retail Electric Providers

1. Arushi Sharma Frank, Tesla, Vice-Chair
2. Jaden Crawford, David Energy (*replacing James McGinnis*)
3. Rajiv Shah, Octopus Energy (*replacing Michael Lee*)
4. Ned Bonskowski, Vistra
5. Resmi Surendran, Shell

ADER Providers

1. Amy Heart, SunRun
2. J.T. Thompson, Generac
3. Joel Yu, Enchanted Rock
4. John Bonnin, AutoGrid
5. Micalah Spenrath, Texas Advanced Energy Business Alliance (TAEBA) (*replacing Suzanne Bertin*)

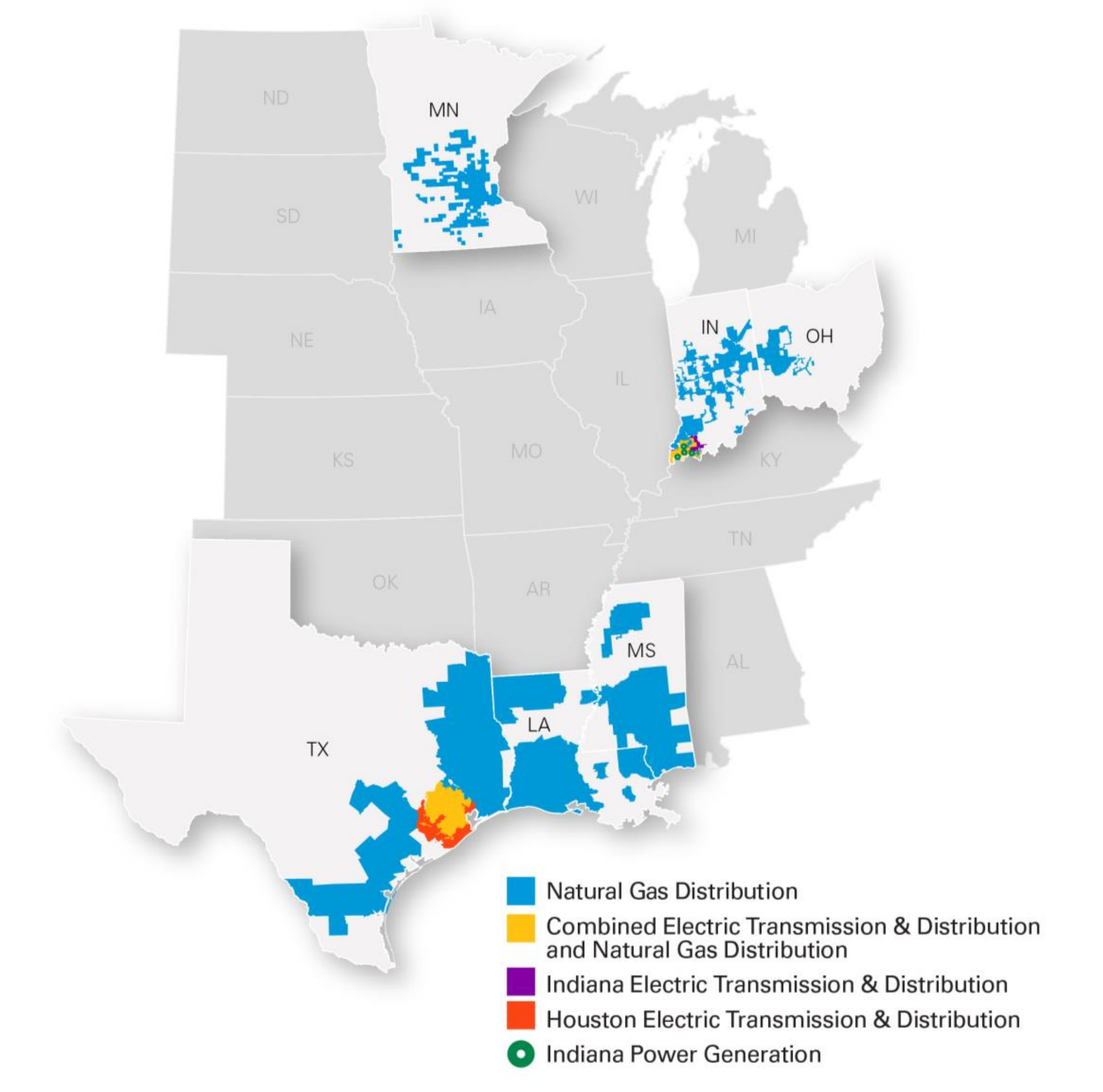
Technical Expertise/Institutions

1. Carmen Best, Recurve
2. Erik Ela, Electric Power Research Institute (EPRI)
3. Margo Weisz, Texas Energy Poverty Research Institute (TEPRI)
4. Miroslav Begovic, Texas A&M University
5. Scott Hinson, Pecan Street

We appreciate the service of James, Michael and Suzanne during the first year of the task force and welcome Jaden, Rajiv and Micalah as we begin our second year of work.

Public

Houston: <3% of the state; ~25% of ERCOT load



ND
MN
SD
WI
MI
IA
NE
IN
OH
IL
KS
MO
KY
TN
OK
AR
MS
AL
LA
TX
🟦 Natural Gas Distribution
🟨 Combined Electric Transmission & Distribution and Natural Gas Distribution
🟪 Indiana Electric Transmission & Distribution
🟥 Houston Electric Transmission & Distribution
● Indiana Power Generation

All of the above

1

Traditional Power Plants

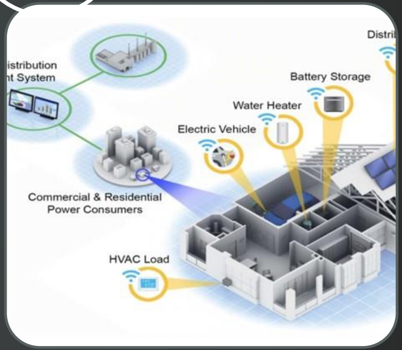
2

Transmission Lines

3

Energy Efficiency

4



Virtual Power Plants

Where to get more information?

- ➢ Texas PUC Project No. 53911
- ➢ Task Force Members
- ➢ ERCOT: ercot.com/mktrules/pilots/ader

CenterPoint®
Energy

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

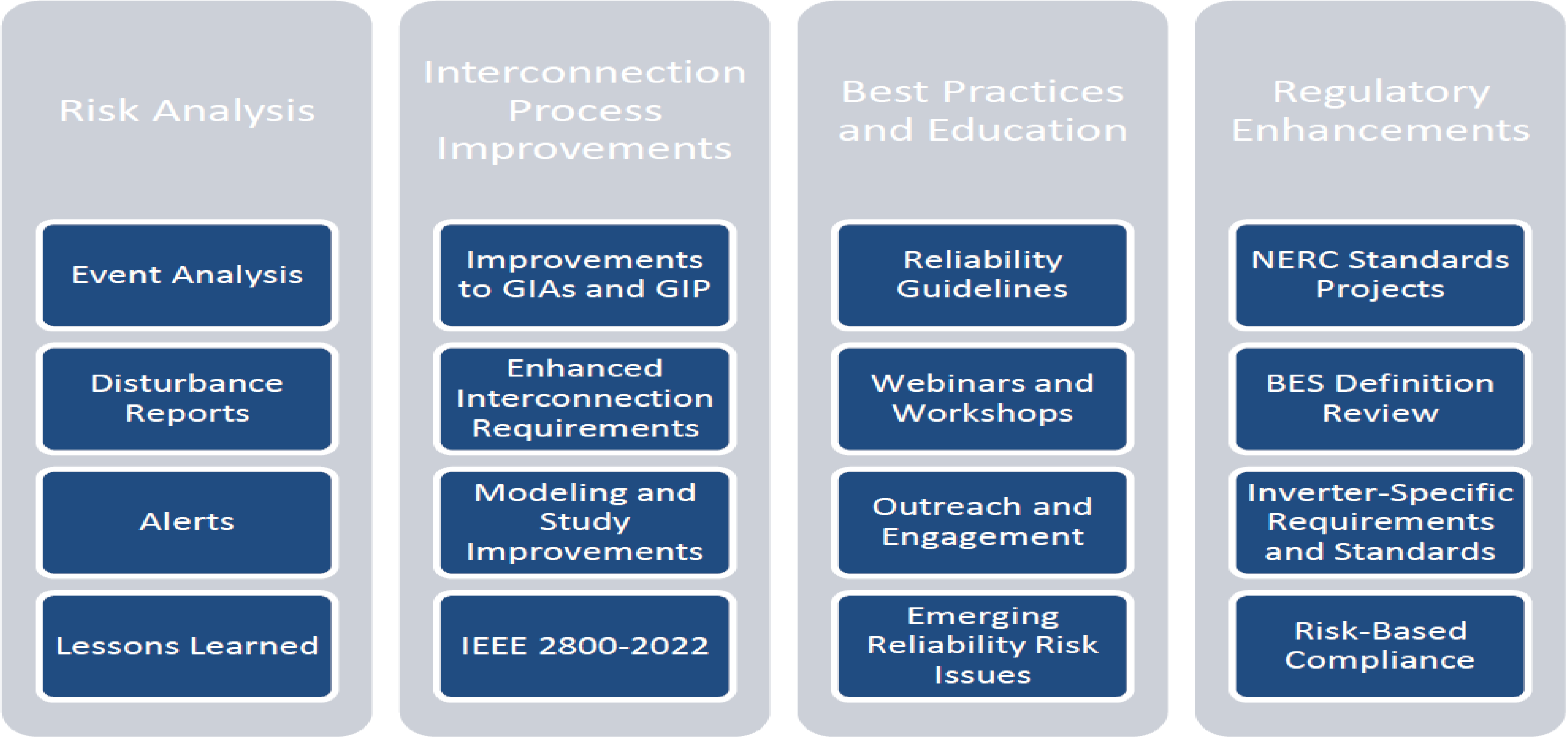
Grid Forming Inverter Technology

Opportunities for a Changing Grid

Alex Shattuck, Senior Engineer, Engineering & Security Integration
Texas RE 2023 Fall Workshop
October 25, 2023

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

NERC IBR Strategy



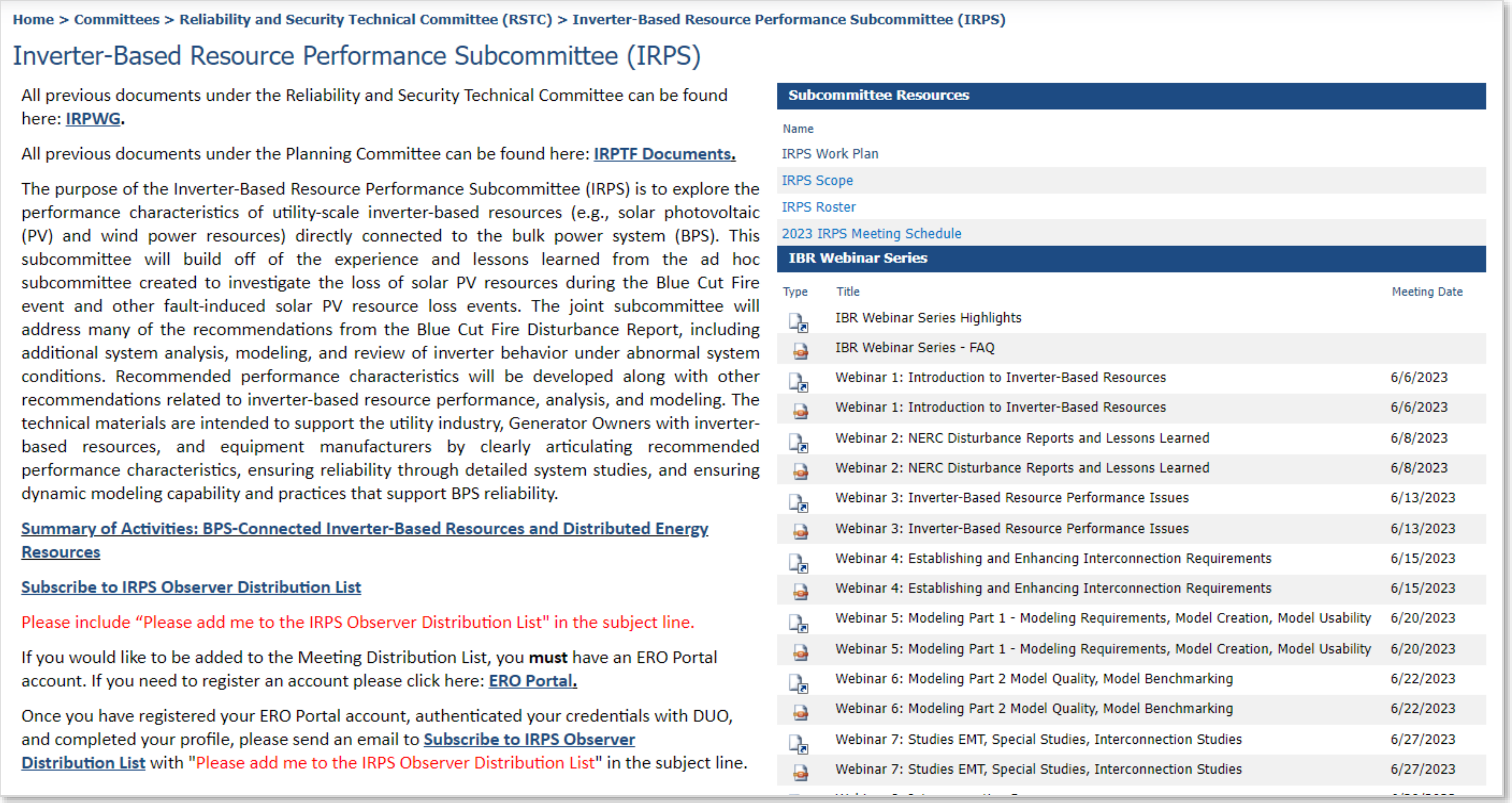
Risk Analysis	Interconnection Process Improvements	Best Practices and Education	Regulatory Enhancements
Event Analysis	Improvements to GIAs and GIP	Reliability Guidelines	NERC Standards Projects
Disturbance Reports	Enhanced Interconnection Requirements	Webinars and Workshops	BES Definition Review
Alerts	Modeling and Study Improvements	Outreach and Engagement	Inverter-Specific Requirements and Standards
Lessons Learned	IEEE 2800-2022	Emerging Reliability Risk Issues	Risk-Based Compliance

NERC IBR Strategy

IBR Webinar Series

Best Practices and Education

- Reliability Guidelines
- Webinars and Workshops
- Outreach and Engagement
- Emerging Reliability Risk Issues



Home > Committees > Reliability and Security Technical Committee (RSTC) > Inverter-Based Resource Performance Subcommittee (IRPS)

Inverter-Based Resource Performance Subcommittee (IRPS)

All previous documents under the Reliability and Security Technical Committee can be found here: IRPWG.

All previous documents under the Planning Committee can be found here: IRPTF Documents.

The purpose of the Inverter-Based Resource Performance Subcommittee (IRPS) is to explore the performance characteristics of utility-scale inverter-based resources (e.g., solar photovoltaic (PV) and wind power resources) directly connected to the bulk power system (BPS). This subcommittee will build off of the experience and lessons learned from the ad hoc subcommittee created to investigate the loss of solar PV resources during the Blue Cut Fire event and other fault-induced solar PV resource loss events. The joint subcommittee will address many of the recommendations from the Blue Cut Fire Disturbance Report, including additional system analysis, modeling, and review of inverter behavior under abnormal system conditions. Recommended performance characteristics will be developed along with other recommendations related to inverter-based resource performance, analysis, and modeling. The technical materials are intended to support the utility industry, Generator Owners with inverter-based resources, and equipment manufacturers by clearly articulating recommended performance characteristics, ensuring reliability through detailed system studies, and ensuring dynamic modeling capability and practices that support BPS reliability.

Summary of Activities: BPS-Connected Inverter-Based Resources and Distributed Energy Resources

Subscribe to IRPS Observer Distribution List

Please include “Please add me to the IRPS Observer Distribution List" in the subject line.

If you would like to be added to the Meeting Distribution List, you **must** have an ERO Portal account. If you need to register an account please click here: ERO Portal.

Once you have registered your ERO Portal account, authenticated your credentials with DUO, and completed your profile, please send an email to Subscribe to IRPS Observer Distribution List with "Please add me to the IRPS Observer Distribution List" in the subject line.

Subcommittee Resources

Name
IRPS Work Plan
IRPS Scope
IRPS Roster
2023 IRPS Meeting Schedule

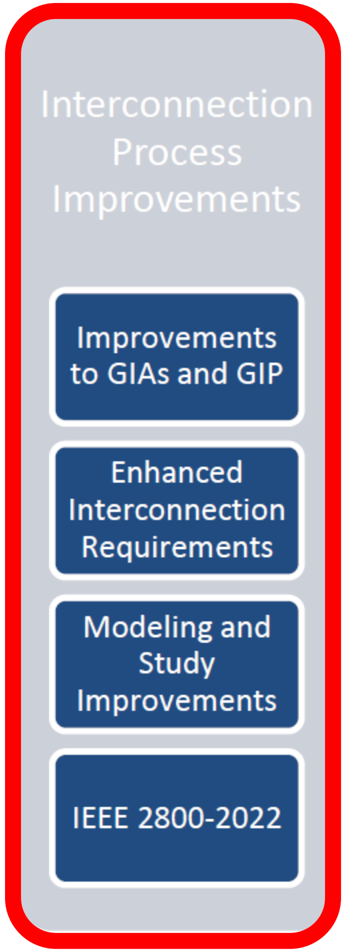
IBR Webinar Series

Type	Title	Meeting Date
	IBR Webinar Series Highlights	
	IBR Webinar Series - FAQ	
	Webinar 1: Introduction to Inverter-Based Resources	6/6/2023
	Webinar 1: Introduction to Inverter-Based Resources	6/6/2023
	Webinar 2: NERC Disturbance Reports and Lessons Learned	6/8/2023
	Webinar 2: NERC Disturbance Reports and Lessons Learned	6/8/2023
	Webinar 3: Inverter-Based Resource Performance Issues	6/13/2023
	Webinar 3: Inverter-Based Resource Performance Issues	6/13/2023
	Webinar 4: Establishing and Enhancing Interconnection Requirements	6/15/2023
	Webinar 4: Establishing and Enhancing Interconnection Requirements	6/15/2023
	Webinar 5: Modeling Part 1 - Modeling Requirements, Model Creation, Model Usability	6/20/2023
	Webinar 5: Modeling Part 1 - Modeling Requirements, Model Creation, Model Usability	6/20/2023
	Webinar 6: Modeling Part 2 Model Quality, Model Benchmarking	6/22/2023
	Webinar 6: Modeling Part 2 Model Quality, Model Benchmarking	6/22/2023
	Webinar 7: Studies EMT, Special Studies, Interconnection Studies	6/27/2023
	Webinar 7: Studies EMT, Special Studies, Interconnection Studies	6/27/2023

NERC IRPS - Webinar Series

https://www.nerc.com/pa/Documents/IBR_Quick%20Reference%20Guide.pdf

Interconnection Process Enhancements Needed



Interconnection Process Improvements

Improvements to GIAs and GIP

Enhanced Interconnection Requirements

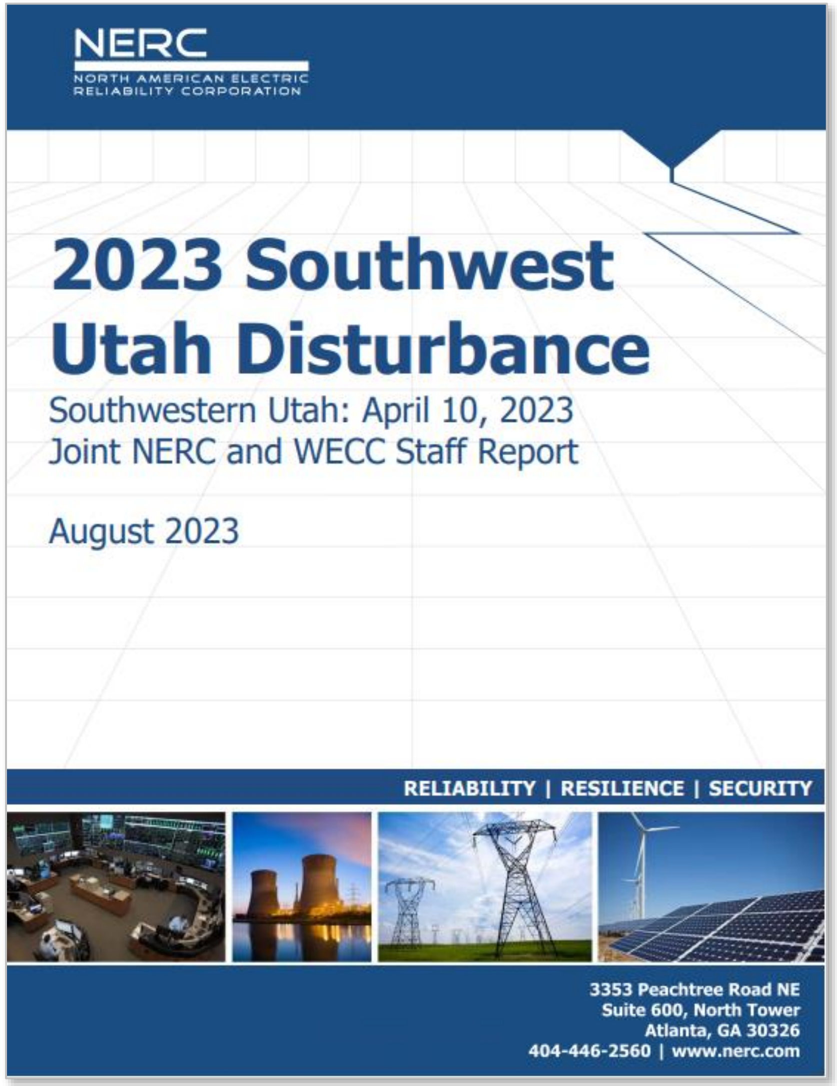
Modeling and Study Improvements

IEEE 2800-2022

- Interconnection speed versus grid reliability
- Clear, consistent, and detailed interconnection requirements are necessary
  - Implementation and enforcement (verification) of requirements is necessary
- Accurate (correct) modeling and studies is critical throughout the interconnection process
  - Model quality checks
  - Detailed positive sequence and EMT modeling
  - Verification of as-built vs. modeled ***at commissioning***
- Adoption of IEEE 2800-2022 is vital – requires significant work by industry; not a “point and done”

Public

Recent Disturbance Reports: Southwest Utah Solar



NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

2023 Southwest Utah Disturbance

Southwestern Utah: April 10, 2023
Joint NERC and WECC Staff Report

August 2023

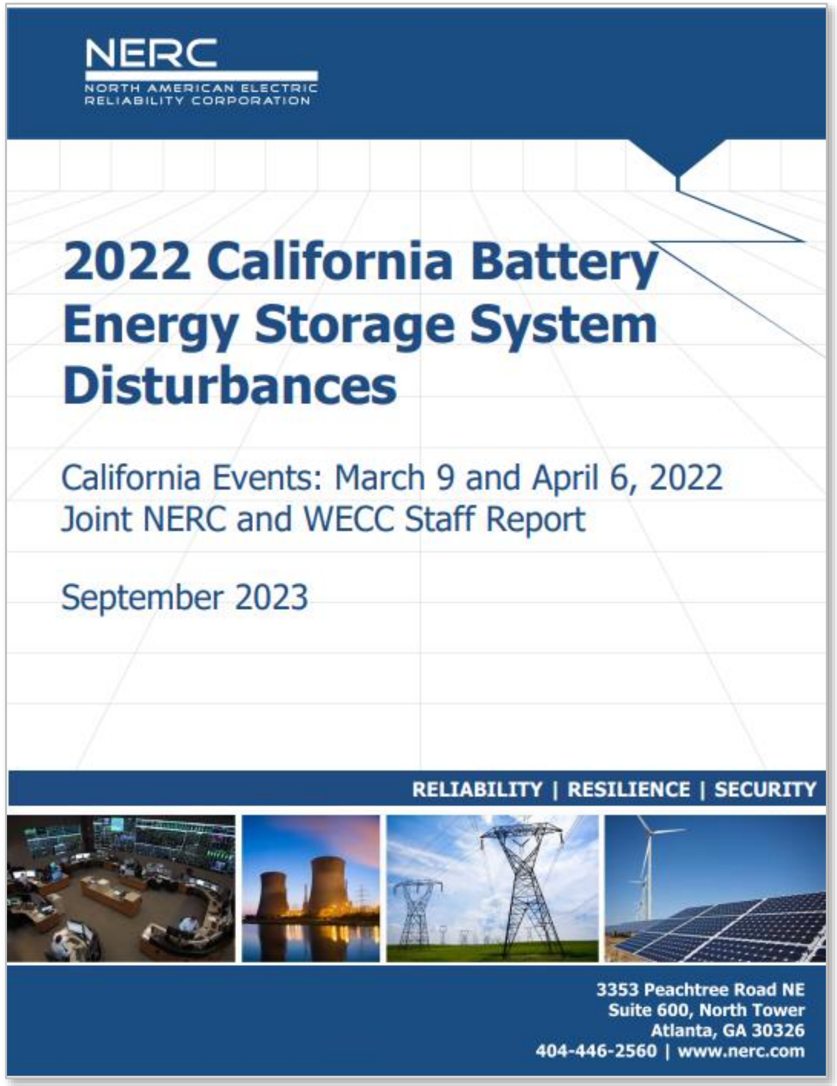
RELIABILITY | RESILIENCE | SECURITY

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

- Older “legacy” resources
- 920 MW loss across 9 facilities
- Systemic inverter tripping issues
- No action taken by industry based on guidelines and reports published by NERC
- Latent BPS risks that threaten BPS reliability
- Inadequate modeling and studies (older plants)

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Recent Disturbance Reports: California BESS



NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

2022 California Battery Energy Storage System Disturbances

California Events: March 9 and April 6, 2022
Joint NERC and WECC Staff Report

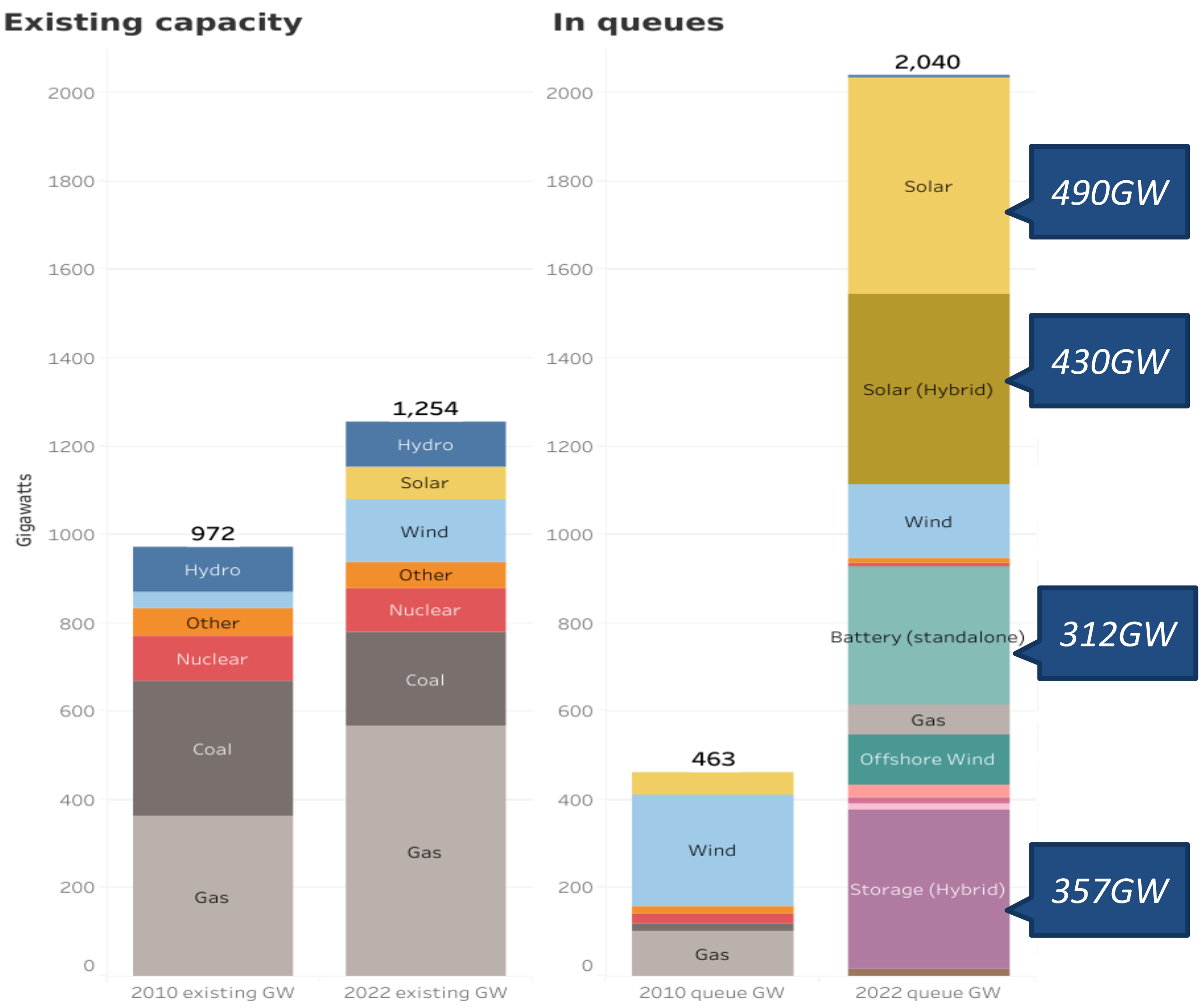
September 2023

RELIABILITY | RESILIENCE | SECURITY

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

- Same story, different resource type
- Systemic inverter tripping issues
- Inadequate ride-through assessments conducted
- Poor commissioning practices
- Bad data, lost data, etc.
- Questionable modeling practices
- Relatively new facilities

Motivation for GFM Work



490GW

430GW

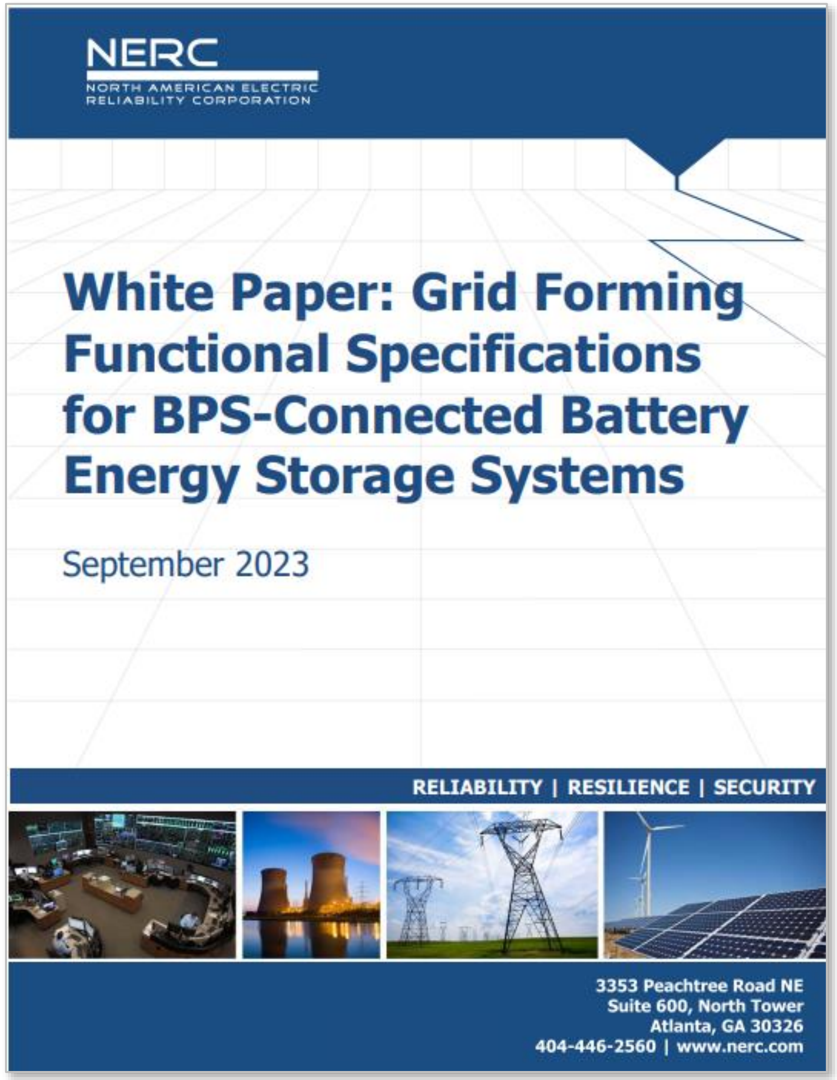
312GW

357GW

Source: LBL.GOV

Generation, Storage, and Hybrid Capacity in Interconnection Queues

RSTC Approved IRPS GFM White Paper



NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

White Paper: Grid Forming Functional Specifications for BPS-Connected Battery Energy Storage Systems

September 2023

RELIABILITY | RESILIENCE | SECURITY

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

- GFM is commercially available for BPS-connected BESS
  - Standalone and hybrid element
  - Very small incremental project cost
- All new BESS should be designed, commissioned, and operated in GFM mode
  - Additional grid-stabilizing characteristics
- Requires studies, like any plant
- Also requires testing against a GFM functional spec
- Requires EMT studies

Why do GFM BESS Make Sense – As a Start

- Enabling GFM controls at BESS facilities (after the effects have been studied by TP) could be cost-effective, and easy step towards BPS stability under high IBR penetrations
- Why newly-interconnecting BESS?
  - Stored energy on dc bus
  - Available in newer BESS equipment today
  - Typically requires only software/firmware changes to enable controls on new BESS
  - Growing industry experience with GFM and successes
  - Significant cost of inaction
  - Retrofit possible but additional hardware costs and complexity are large roadblocks
- GFM BESS facilities are **not the only solution** but can be a good source of low cost GFM capabilities

Functional Specifications for BESS

Capability	Grid Forming	Grid Following
Sub-cycle Voltage and Frequency Support	✓	
Phase Jump Resistance	✓	
System Strength Support	✓	
Ability to Stably Operate with Loss of Last Synchronous Machine	✓	
Dispatchability	✓	✓
Steady-state Voltage Control	✓	✓
Dynamic Reactive Power Support	✓	✓
Active-Power Frequency Control	✓	✓
Disturbance Ride-Through Performance	✓	✓
Fault Current and Negative Sequence Current Contribution	✓	✓
Cyber and Physical Security	✓	✓

Overview of BESS Functional Specifications

Functional Specifications for BESS

Capability	Grid Forming	Grid Following
Sub-cycle Voltage and Frequency Support	✓	
Phase Jump Resistance	✓	
System Strength Support	✓	
Ability to Stably Operate with Loss of Last Synchronous Machine	✓	

- **GFM-Specific Voltage and Frequency Support**: GFM shall provide autonomous, near-instantaneous frequency and voltage support by maintaining a nearly-constant internal voltage phasor in the sub-transient time frame
- **Phase Jump Performance:** GFM shall resist near-instantaneous voltage magnitude and phase angle changes by providing appropriate levels of active and reactive power output in the sub-transient timeframe

Functional Specifications for BESS

Capability	Grid Forming	Grid Following
Sub-cycle Voltage and Frequency Support	✓	
Phase Jump Resistance	✓	
System Strength Support	✓	
Ability to Stably Operate with Loss of Last Synchronous Machine	✓	

- **System Strength Support:** GFM shall help reduce the sensitivity of voltage change for a given change in current in the sub-transient time scale
- **Ability to Stably Operate with Loss of Last Synchronous Machine**: GFM shall be able to stably operate through and following the disconnection of the last synchronous machine in its portion of the power grid

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

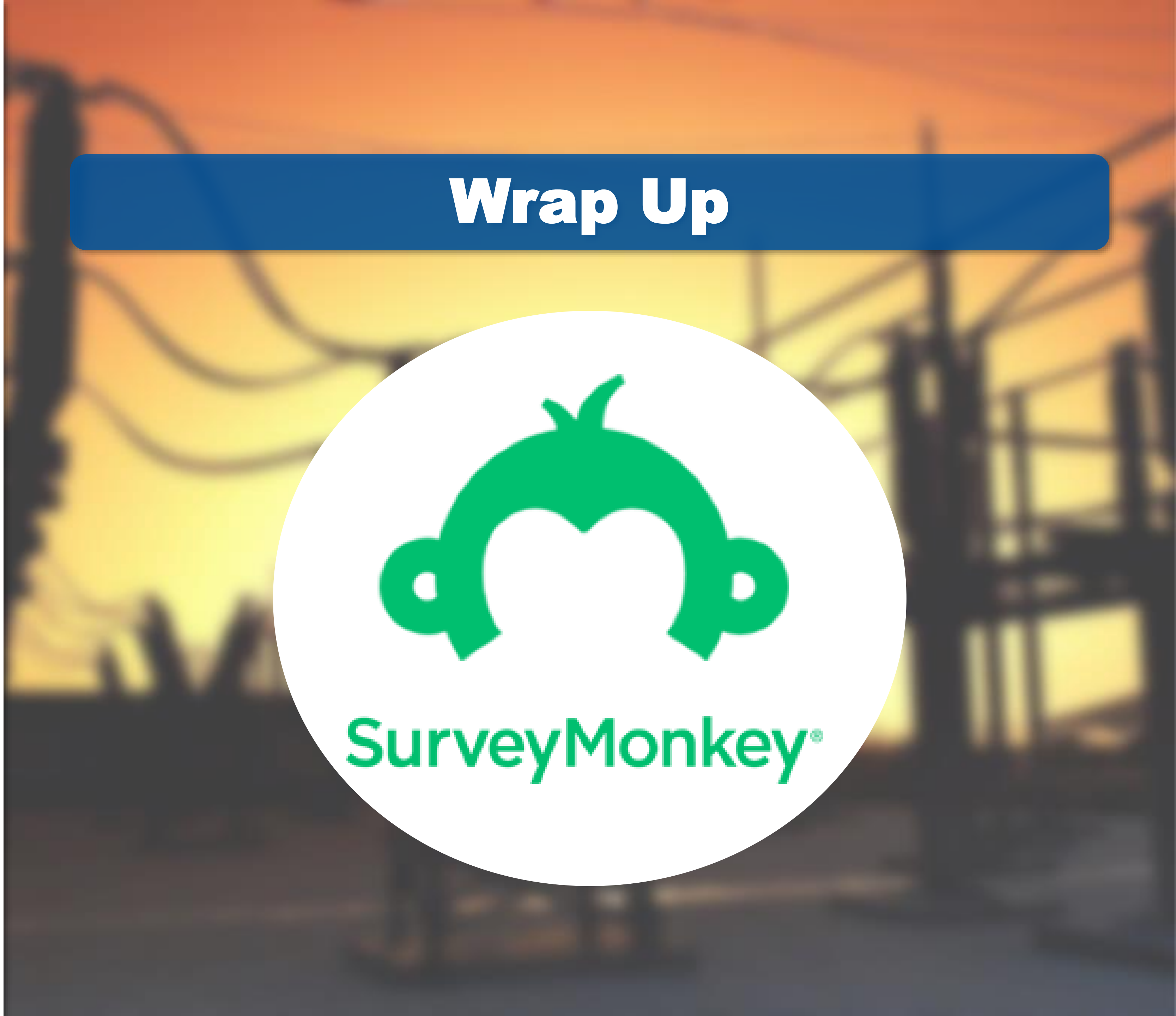
GFM BESS Key Takeaways and Recommendations

- GFM technology is commercially available and field-proven for transmission-connected applications, particularly BESS
    - GFM technology has been shown to operate reliably in transmission systems with high IBR penetration outside of the BPS and provide grid stabilizing characteristics
- All newly interconnecting BPS-connected BESS should be designed, carefully studied, and commissioned with GFM controls enabled
- The IRPS *White Paper: Grid Forming Functional Specifications for BPS-Connected Battery Energy Storage Systems* should be leveraged by TOs, TPs, and PCs to begin the process of establishing GFM functional specifications

Questions and Answers

STANDARDS, SECURITY, & RELIABILITY
FALL WORKSHOP

Wrap Up



SurveyMonkey®

Talk with Texas RE
Electric-Gas Coordination

October 31, 2023

Talk with Texas RE
2024 SOL Standards

November 2, 2023