NPCC

NPCC 2026 Spring Compliance and Reliability Webinar

Jacqueline Jimenez
Vice President, Compliance

May 20, 2026

Public

NPCC Outreach, Training, Events Disclaimer

Northeast Power Coordinating Council, Inc. (NPCC) is committed to providing outreach, training, and nonbinding guidance to industry stakeholders on important industry topics. Subject Matter Experts (SMEs) from NPCC's organizational groups and the industry may develop materials, including presentations, provided as part of the event. The views expressed in the event materials are those of the SMEs and do not necessarily express the opinions and views of NPCC.

Antitrust Compliance Guidelines

Because this event brings together market participants who may be viewed as actual or potential competitors, we must be mindful to conduct it in a manner that is consistent with the antitrust and competition laws. Participants should not disclose non-public, proprietary, or competitively sensitive information.

Attendees should exercise independent judgment and avoid even the appearance of discussions of agreements or concerted actions that may be viewed as restraining competition. Any company decisions that are informed by your discussions today must be made independently.

This guidance is not intended as legal advice, and each attendee is responsible for seeking their own legal advice with respect compliance with applicable antitrust and competition laws. However, any questions on NPCC's Antitrust Policy may be directed to NPCC's General Counsel.

Webinar Housekeeping

Recording: This webinar is being recorded. A link to the recording will be shared with all registrants after the session, so you can revisit the content or share it with colleagues.

Audio: All participants are muted by default to minimize background noise. If you experience any audio issues, try refreshing your browser or checking your device settings.

Q&A: We encourage your questions! Please use the Q&A box at the top of your screen. We'll address as many as we can during the Q&A portion at the end.

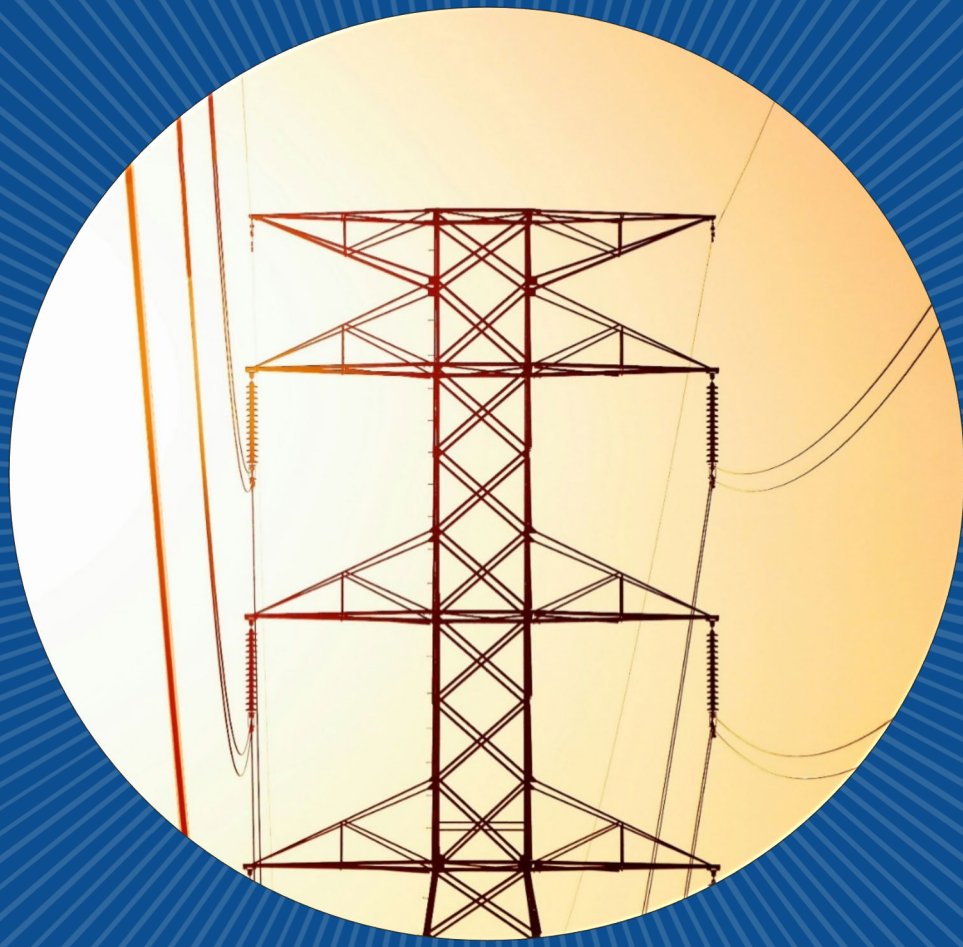
Agenda

AGENDA	
9:00 AM	**WELCOME** Jacqueline Jimenez – NPCC – Vice President, Compliance
9:10 AM	**INSIDER THREAT** Harrison Crow – FBI – Special Agent
9:35 AM	**ENFORCEMENT INTAKE REQUEST FOR INFORMATION (EIR)** Cory Boughton – NPCC – Senior O&P Enforcement Analyst
9:45 AM	**UPDATED ERO CMEP IP - COMMUNICATION PROTOCOLS & OPERATING INSTRUCTIONS** Daniel Kidney – NPCC – Senior Compliance Engineer
10:00 AM	**CIP ERT v10 UPDATES** Chase Cameron – NPCC – Senior CIP Compliance Analyst
10:15 AM	**POLAND CYBER SHIELD: NAVIGATING ATTACKS AND CYBER HYGIENE** Michael Bilheimer – NPCC – Senior CIP Analyst
10:35 AM	**BREAK**

AGENDA	
10:45 AM	**MODERNIZATION OF STANDARDS PROCESSES AND PROCEDURES (MSPP) UPDATE** **PROJECT 2026-02 RELIABILITY STANDARDS TO ADDRESS COMPUTATIONAL LOAD – PHASE I** Soo Jin Kim – NERC – Vice President, Standards and Registration
11:05 AM	**NEW CONTROL CENTER CONSTRUCTION: BEST PRACTICES AND LESSONS LEARNED** Damian Interrante – Central Hudson Gas & Electric – Manager, Reliability Compliance
11:30 AM	**NPCC'S SECURITY OUTREACH** Doug Vitale – NPCC - Security Outreach Manager
11:45 AM	**PNC ABEYANCE PROCESS** Arthur Brown – NPCC – Associate General Counsel
11:55 AM	**NERC LARGE LOAD WORKING GROUP UPDATE** Diana Barsotti – NPCC – Senior Reliability Assessment Engineer
12:05 PM	**CLOSING** Jacqueline Jimenez – NPCC – Vice President, Compliance

NPCC

Enforcement Intake Request For Information (EIR)



Cory Boughton
Senior O&P Enforcement Analyst

NPCC Spring Compliance and Reliability Webinar | May 20, 2026

EIR Overview

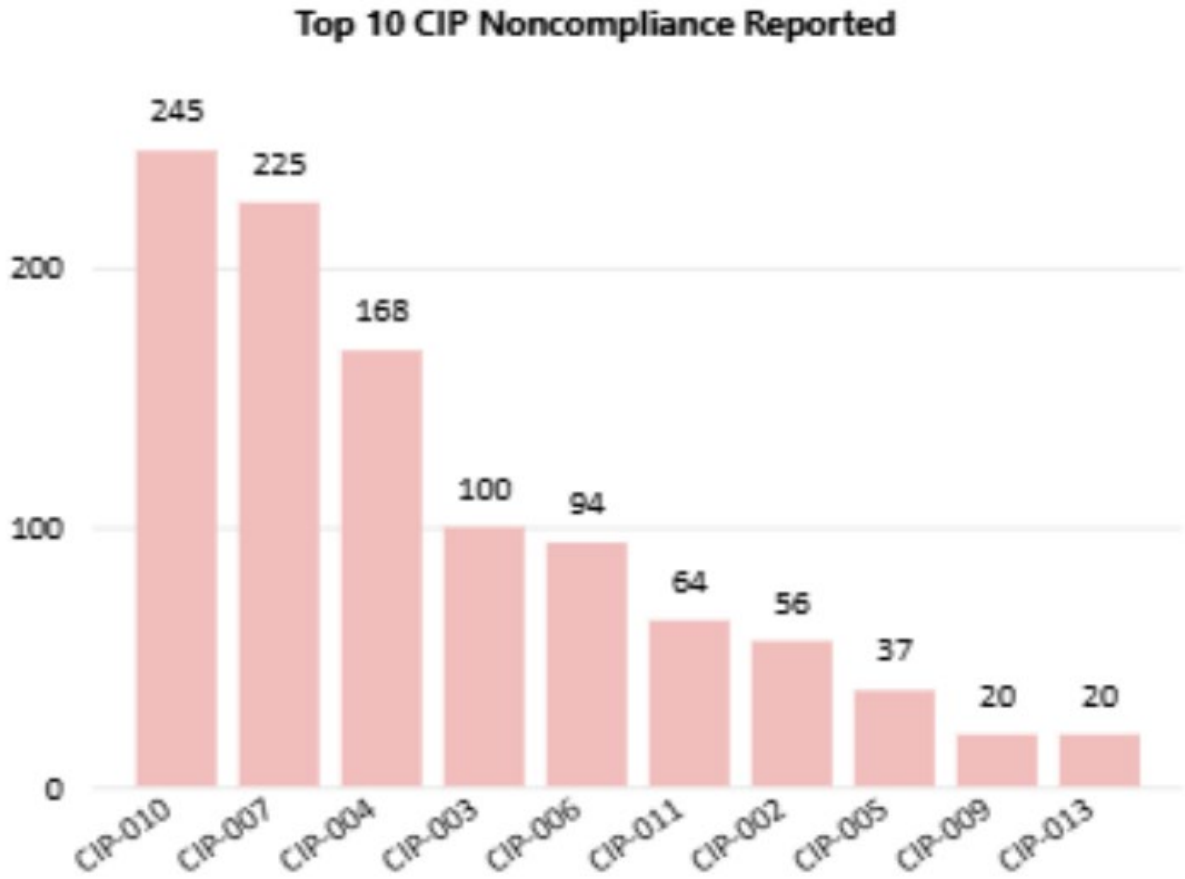
- NPCC identified an improvement opportunity to the Align Self Report/Self Log Template.
- Provide a structured format for submitting information related to a potential noncompliance.
- Specific to the applicable NERC Reliability Standard.
- The information requested reflects the details NPCC typically considers when assessing the scope, risk, and disposition of a potential noncompliance.
- The worksheet may be used when preparing information related to a potential noncompliance, or it may be issued by NPCC as a Request for Information (RFI).

EIR Development

- EIRs are developed by the NPCC Enforcement Team.
- NPCC will prioritize the most violated CIP/O&P standards.
- Published EIRs can be found on the NPCC Website.
- Published EIRs will be updated as needed for standard revisions.
- Member entities will be notified of new and updated EIRs through the NPCC Compliance and Reliability Bulletin

Most Violated Standards
CIP

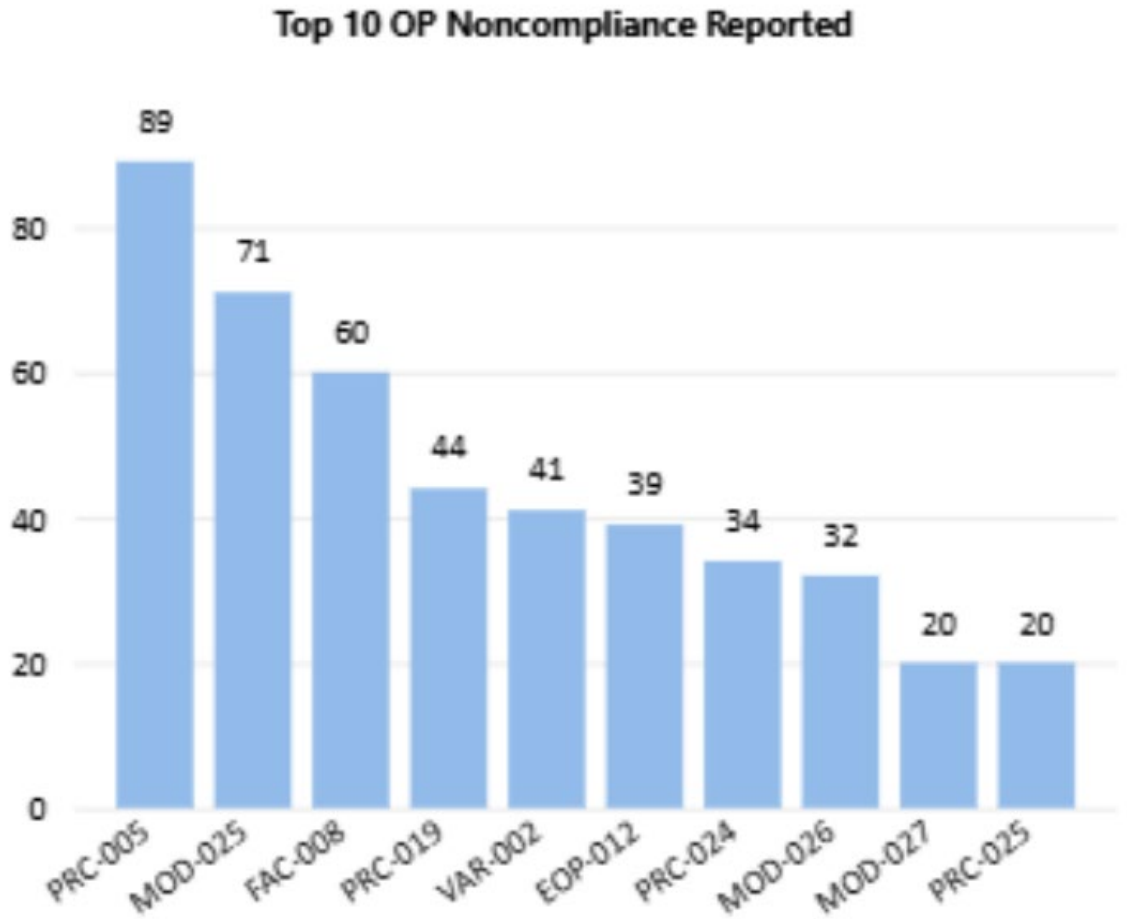
- In 2025, the most frequently reported noncompliance involving CIP standards included CIP-010, CIP-007, and CIP-004.



Source: NERC ORCP and CMEP Annual Report – February 11, 2026
https://www.nerc.com/globalassets/programs/enforcement/cmep-and-vegetation-reports/2025-orcp-and-cmep-annual-report.pdf -

Most Violated Standards
O&P

- In 2025, the most frequently reported noncompliance involving O&P standards included PRC-005, MOD-025, and FAC-008.



Source: NERC ORCP and CMEP Annual Report – February 11, 2026
https://www.nerc.com/globalassets/programs/enforcement/cmep-and-vegetation-reports/2025-orcp-and-cmep-annual-report.pdf -

How to Access EIRs?

EIRs can be found on the NPCC Website

NPCC Website > Enforcement > View all Enforcement Documents

- MOD-025-2 Enforcement Intake RFI
- PRC-005-6 Enforcement Intake RFI
- CIP-004-6 Enforcement Intake RFI **Coming Soon!**

Questions?

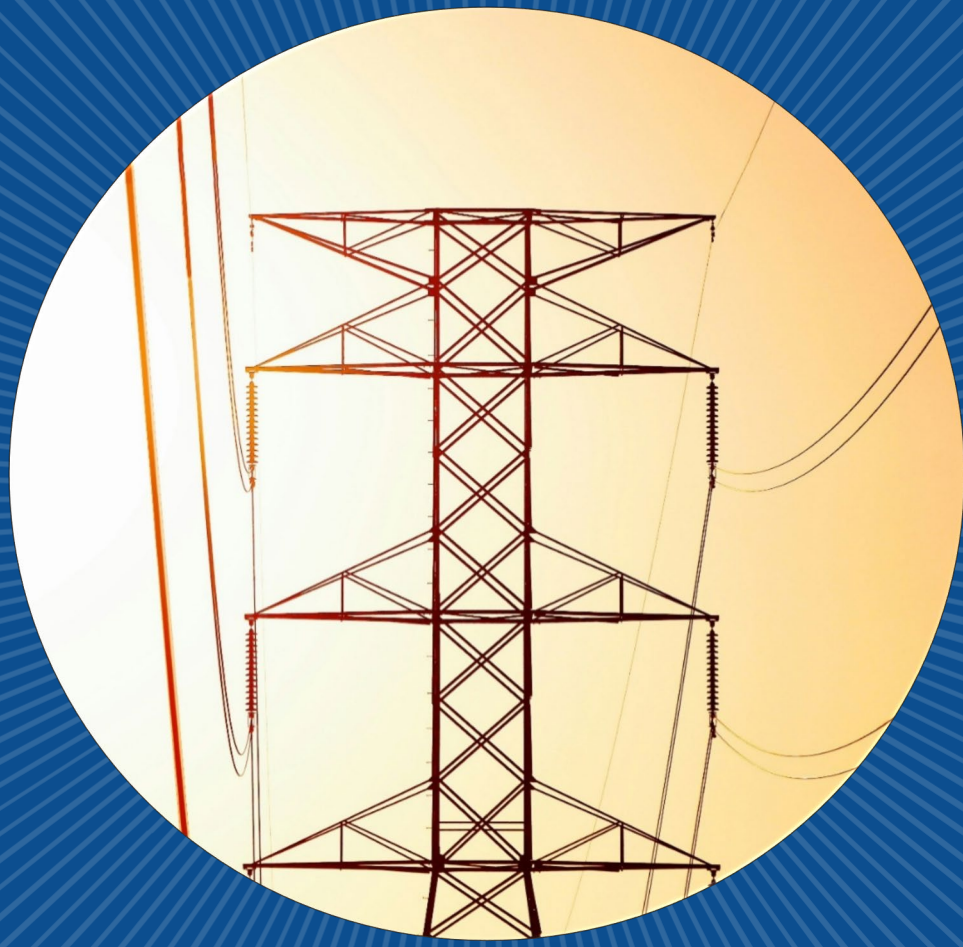
Contact Us: npcc.org/contact

NPCC Enforcement

Cory Boughton

NPCC

Updated ERO CMEP IP – Communication Protocols & Operating Instructions



Daniel Kidney
Senior Compliance Engineer

NPCC Spring Compliance and Reliability Webinar | May 20, 2026

Agenda

- 2026 CMEP IP Update
- Why?
- What is the Risk?
- Operating Instructions
- Areas of Focus
- Best Practices
- Additional Resources
- Questions

2026 CMEP IP Update

- Risk-based compliance monitoring approach
- Risk Elements reviewed and assessed annually by ERO Enterprise
  - Compliance findings, event analysis, etc.
  - Risks are prioritized for CMEP activities
- Communication Protocols & Operating Instructions Risk Element added to 2026 Risk Elements list in February

Risk Elements	
2025	**2026**
Remote Connectivity	Remote Connectivity
Supply Chain	Supply Chain
Physical Security	Physical Security
Incident Response	Grid Transformation
Transmission Planning and Modeling	Facility Ratings
Inverter-Based Resources	Extreme Weather Response
Facility Ratings	Communication Protocols & Operating Instructions
Extreme Weather Response	

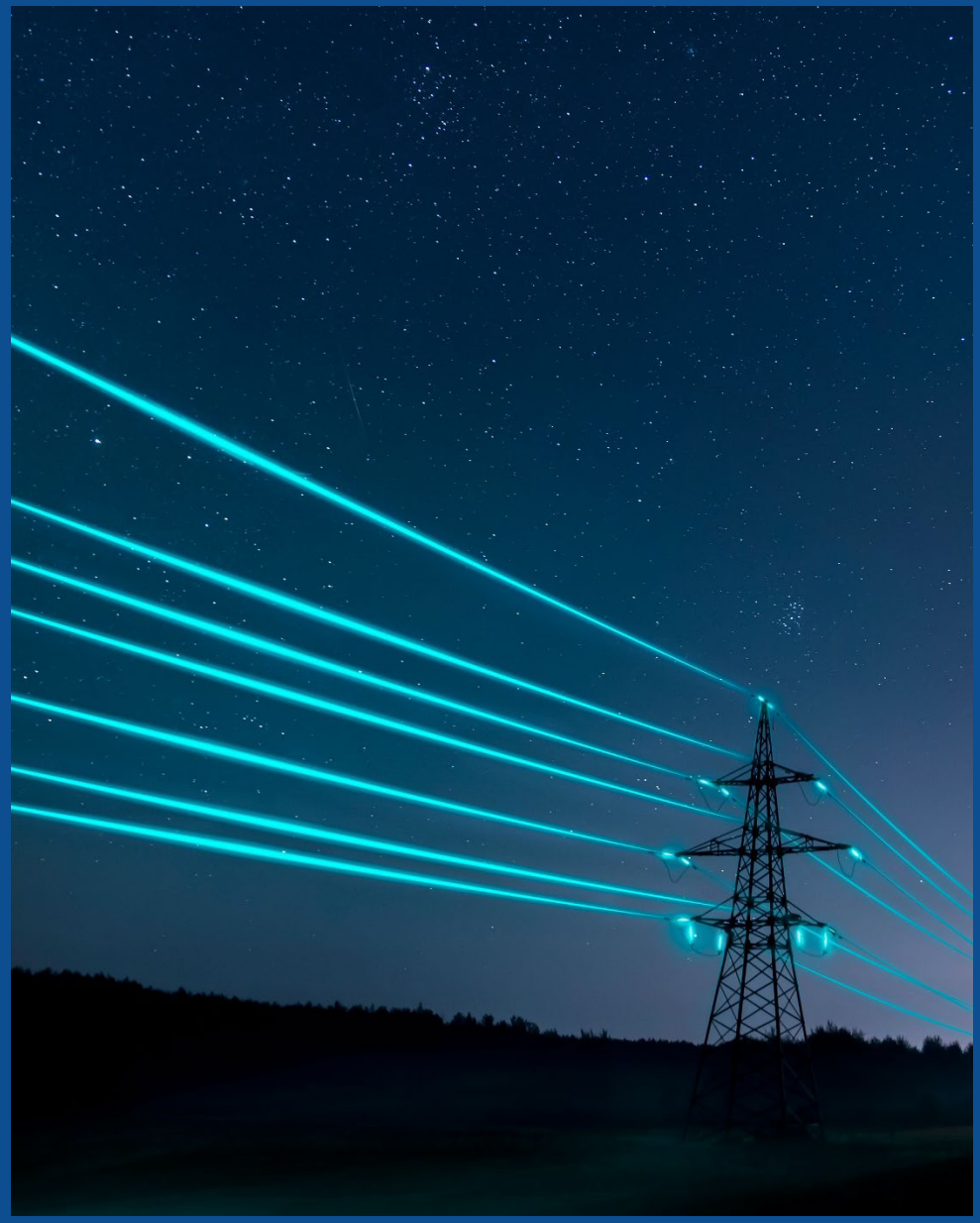
Source: 2026 ERO Enterprise CMEP Implementation Plan

Why?

- Heightened consequences of ineffective communication
  - Growing system complexity
  - Tighter operating margins
  - Increasing interdependence
- Instances where Operating Instructions were treated as informal guidance rather than authoritative commands
- Risk being introduced due to poor communications protocol adherence

What is the Risk?

- Misunderstanding leading to incorrect actions being taken
  - Can impede Reliability Coordinator (RC) actions during an Emergency
  - Impairs Operators' ability to maintain safety and reliability of the BES
- Delayed execution of Operating Instructions
  - Can affect ability to respond to Emergencies in a timely manner
- Cascading outages
- Risk exacerbated by evolving BES



Operating Instructions

- Defined in NERC Glossary of Terms
- Insufficient or ineffective use of Operating Instructions creates critical vulnerability in grid stability
- All parties that are involved in an Operating Instruction have responsibilities to ensure effective communication
- Operating Instructions are not suggestions
- Operating Instructions must be clear, concise, technically accurate, timely, and definitive to maintain safety and reliability

Areas of Focus

COM-002-4	IRO-001-4
- **R1 – <u>Ensure</u>** adherence to documented communication protocols for operating personnel that issue and receive Operating Instructions - **R4 – <u>Assess</u>** adherence to documented communication protocols and evaluate their effectiveness; providing feedback and/or corrective action to address deviations from documented protocols. - **R5, R7 –** Ensure Operating Instructions are correctly **<u>understood and repeated</u>** back as required, or; that Operating Instruction was reissued as required/requested, or alternative action was taken.	- **R1 –** Ensure Reliability Coordinators act to address reliability of its RC Area via direct actions or by issuing Operating Instructions.

Best Practices

Communication Training

- Stress the importance of Operating Instructions
- Explain possible consequences of poor communication
- Refresher communication training

Communication Protocols “Audits”

- Ensure that Operating Instructions are specifically reviewed, where possible
- More frequent communication “audits”
- Provide examples of excellent communications to all Operations staff

Identify issues that may cause confusion

Additional Resources

- 2026 ERO Enterprise CMEP IP
- COM-002-4
- IRO-001-4

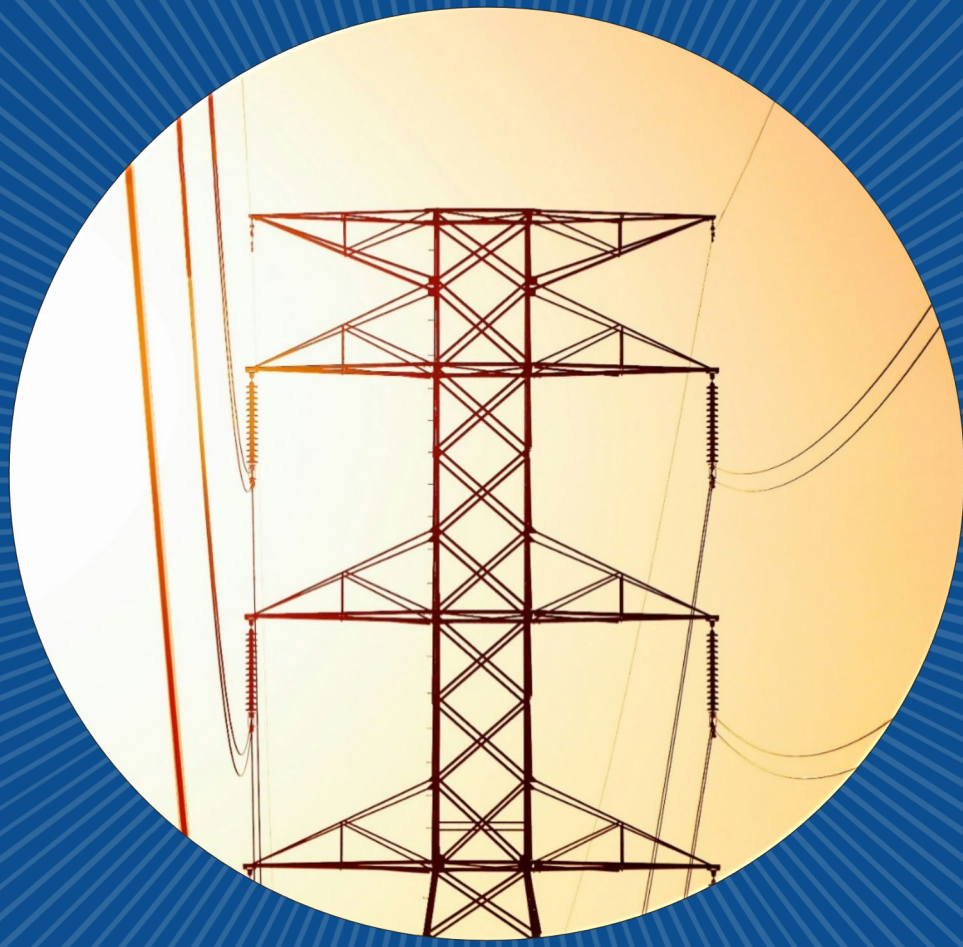
Questions?

Contact Us: npcc.org/contact

Compliance Monitoring & Enforcement
Daniel Kidney

NPCC

CIP ERT v10 Updates

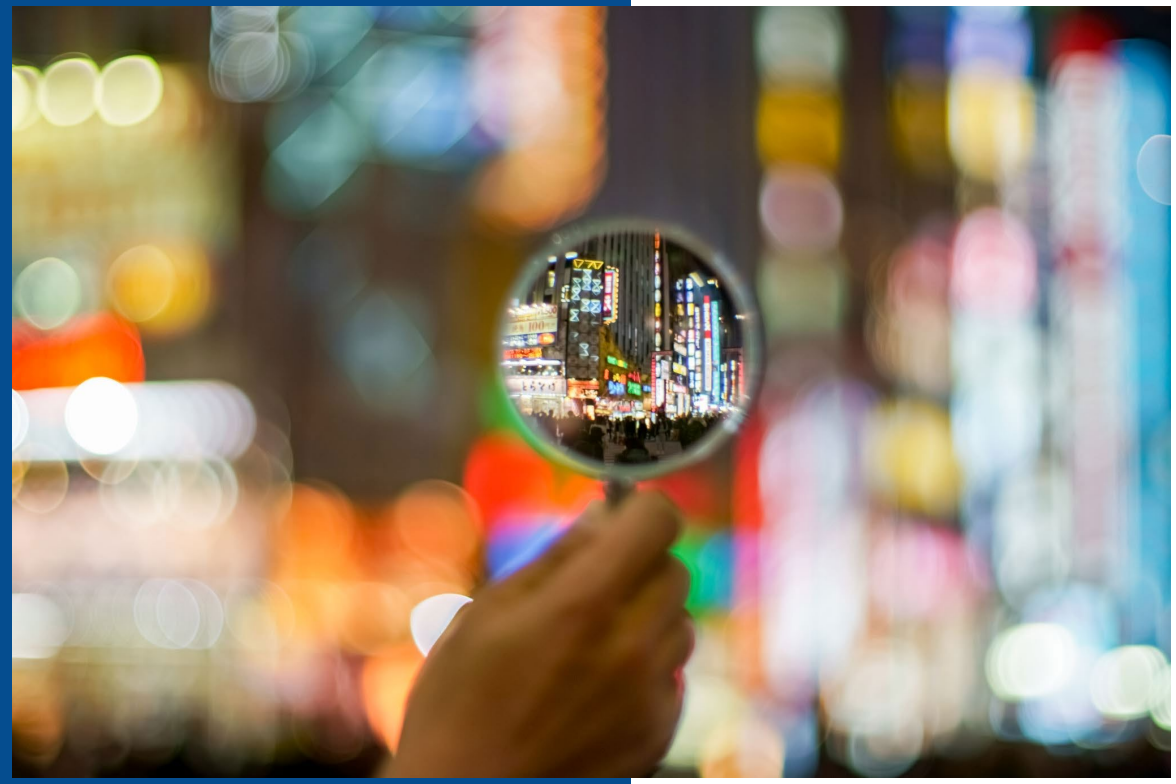


Chase Cameron
Senior CIP Analyst

NPCC 2026 Spring Compliance and Reliability Webinar | May 20, 2026

Overview

- Instructions Tab Updates
- Level 1 Tab Updates
- Sample Sets L2 Tab Updates
- Level 2 Tab Updates
- CA Tab Updates
- Tabs with Identical Updates



Instructions Tab - Updates

Changed Version v9.0 to v10.0

Level 1 Tab - Updates

- Updated SEL Reference ID formula to replace periods from the tags section to hyphens
- Updated CIP-005-7-R1-L1-02 request language
- Updated CIP-006-6-R1-L1-02 request language
- Updated CIP-007-6-R2-L1-01 to be consistent with the rest of the Level 1 “-01” requests
- Added CIP-007-6-R2-L1-02, which contains the second request previously from CIP-007-6-R2-L1-01

Level 1 Tab Updates Cont'd

Requests added for Reliability Standards from Standard Drafting Project 2016-02 pending FERC approval at time of ERT v10 publication:

- CIP-002-7
- CIP-003-10
- CIP-004-8
- CIP-005-8
- CIP-006-7
- CIP-007-7
- CIP-008-7
- CIP-009-7
- CIP-010-5
- CIP-011-4
- CIP-013-3

Sample Sets L2 Tab - Updates

Added new Sample Sets needed for Level 2 requests related to Reliability Standards from Standard Drafting Project 2016-02 pending FERC approval at time of ERTv10 publication.

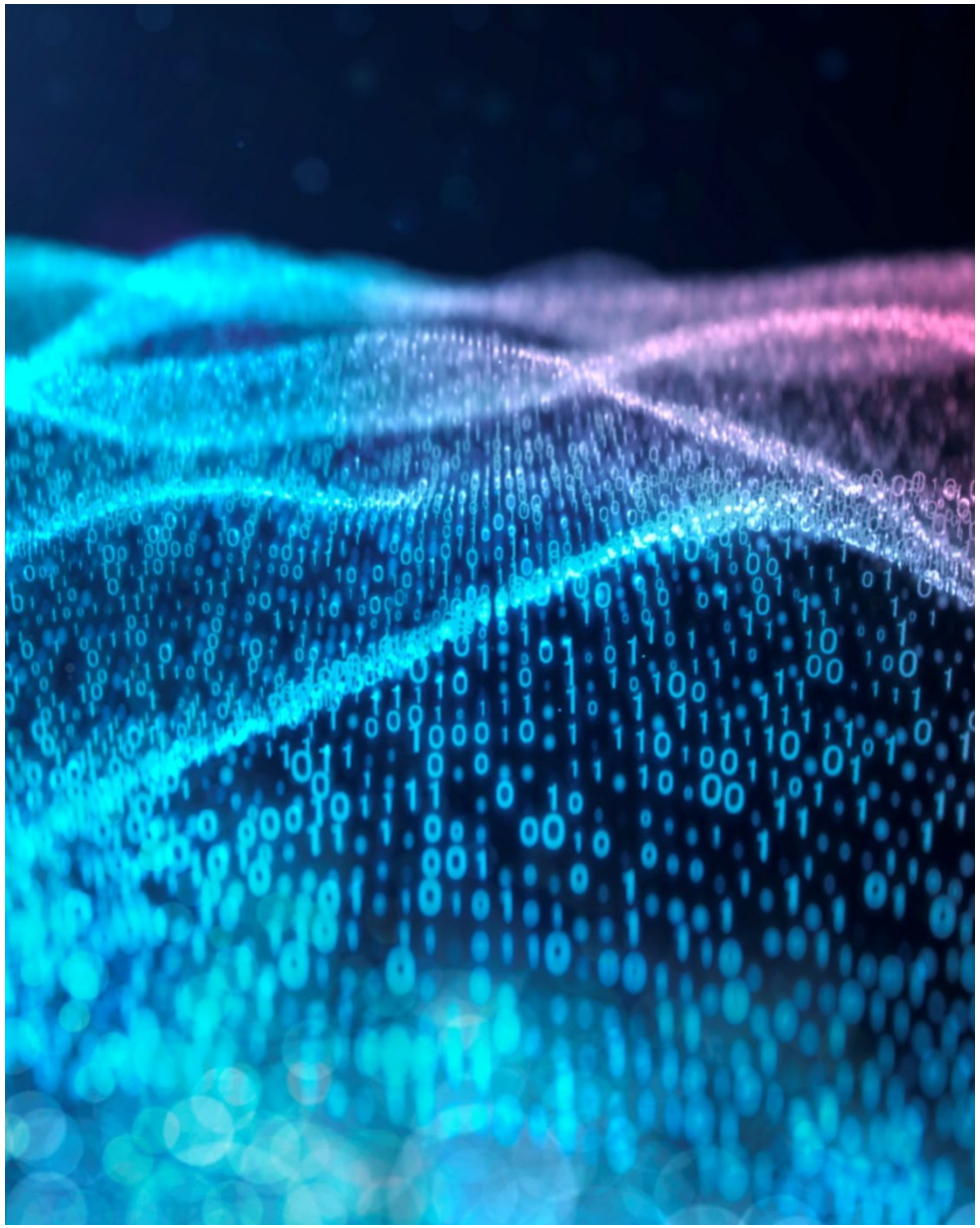
Level 2 Tab - Updates

Separated “Sample Set” field into “Index Sample Set” and “Date Sample Set” columns:

- Index Sample Set field contains the sample set for the assets/personnel
- Date Sample Set field contains the sampled date range for a given request, if applicable

Requests added for Reliability Standards from Standard Drafting Project 2016-02 pending FERC approval at time of ERTv10 publication:

- CIP-002-7
- CIP-003-10
- CIP-004-8
- CIP-005-8
- CIP-006-7
- CIP-007-7
- CIP-008-7
- CIP-009-7
- CIP-010-5
- CIP-011-4
- CIP-013-3



Level 2 Tab – Updates Cont'd

- Updated CIP-003-9-R2-L2-05 and CIP-003-9-R2-L2-06 Sample Set Index Numbers and Sampled Dates field to reference the correct cells
- Updated CIP-004-7-R6-L2-01 request language to request evidence from the correct sample set
- Updated CIP-005-7-R2-L2-01 and CIP-005-7-R2-L2-02 to sample from Electronic Security Perimeters rather than from Cyber Assets
- Updated CIP-010-4-R1-L2-01 request language
- Requests that previously requested both PSP-L2-01 and PSP-L2-02 now request PSP-L2-03

CA Tab - Updates

- Updated “TRUE/ ” validation fields to “TRUE/FALSE”
- Some field names have been updated to be more concise and consistent with other worksheets. See the ERT User Guide for details

- Added columns for Reliability Standards from Standard Drafting Project 2016-02 pending FERC approval at time of ERTv10 publication. See the User Guide for details
  - Virtual
  - SCI ID
  - VCA Classifications
  - EACMS Controls ESP

Tabs with Identical Changes

BES Assets	Low CA	ESP
EAP	PSP	TCA
RM	BCSI	Personnel
Reuse_ Disposal	CSI	Procurement

- Updated “TRUE/ ” validation fields to “TRUE/FALSE”
- Some field names have been updated to be more concise and consistent with other worksheets. See the User Guide for details on what is requested in each field

Questions?

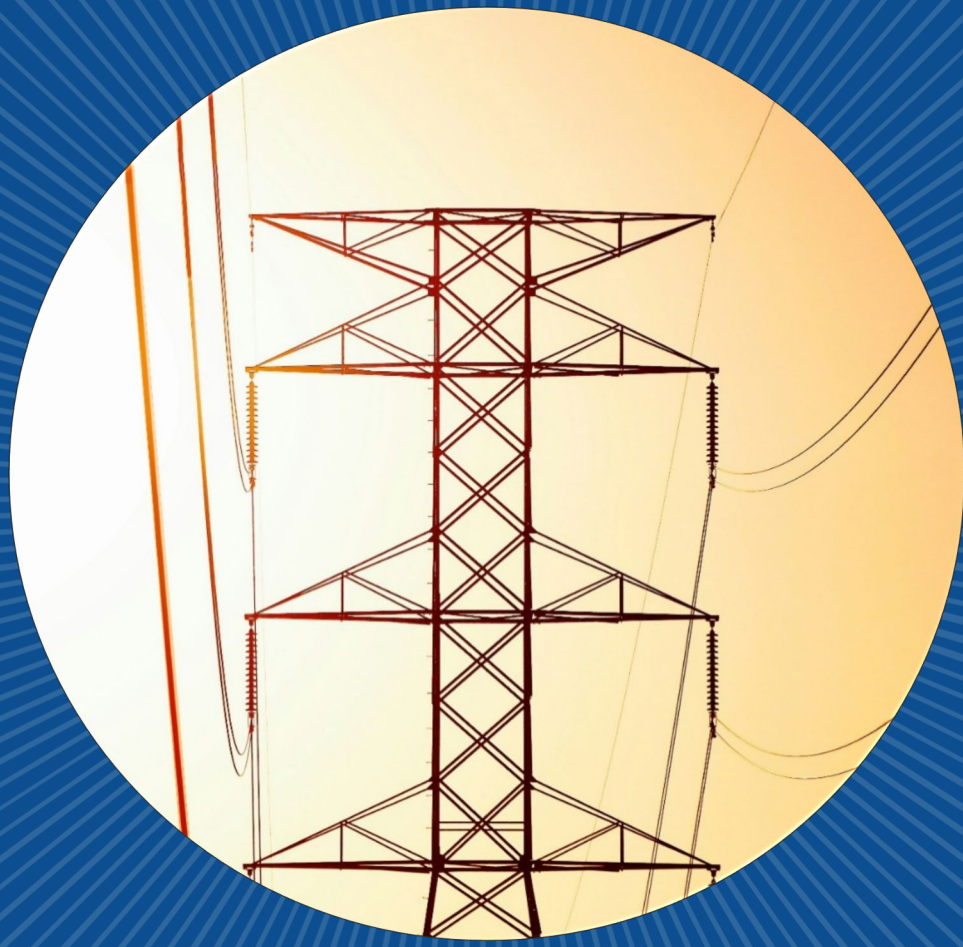
Contact Us: npcc.org/contact

Compliance Monitoring & Enforcement

Chase Cameron

NPCC

Poland Cyber Shield: Navigating Attacks And Cyber Hygiene

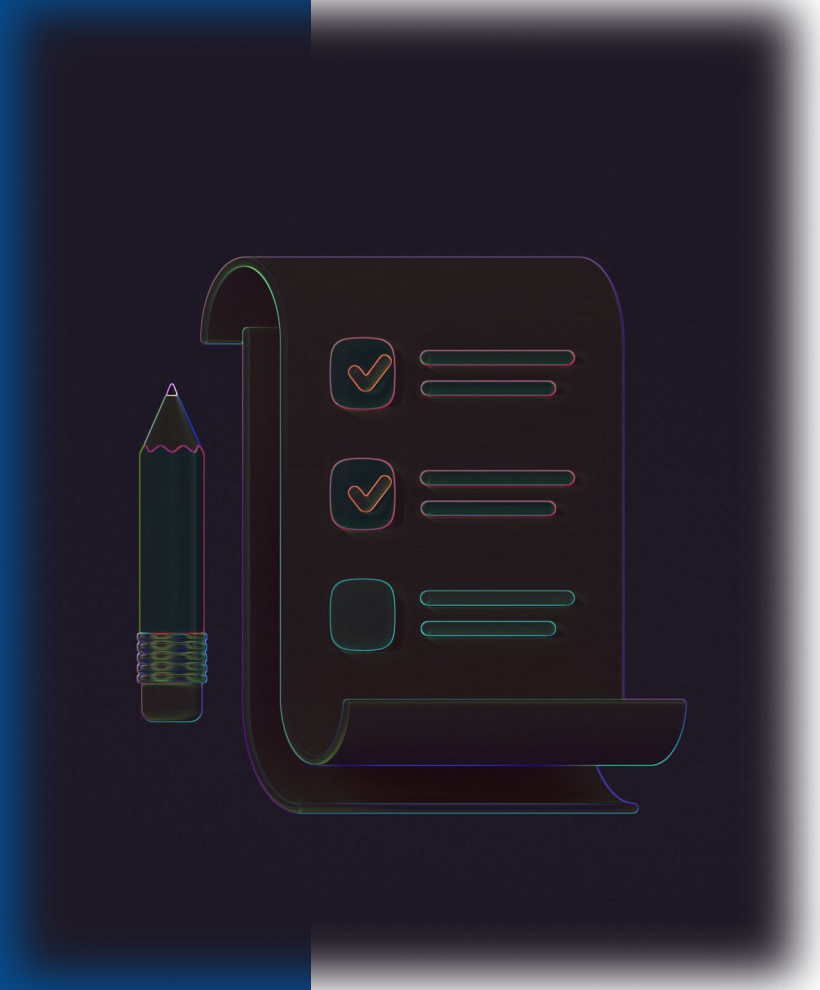


Michael Bilheimer
Senior CIP Auditor

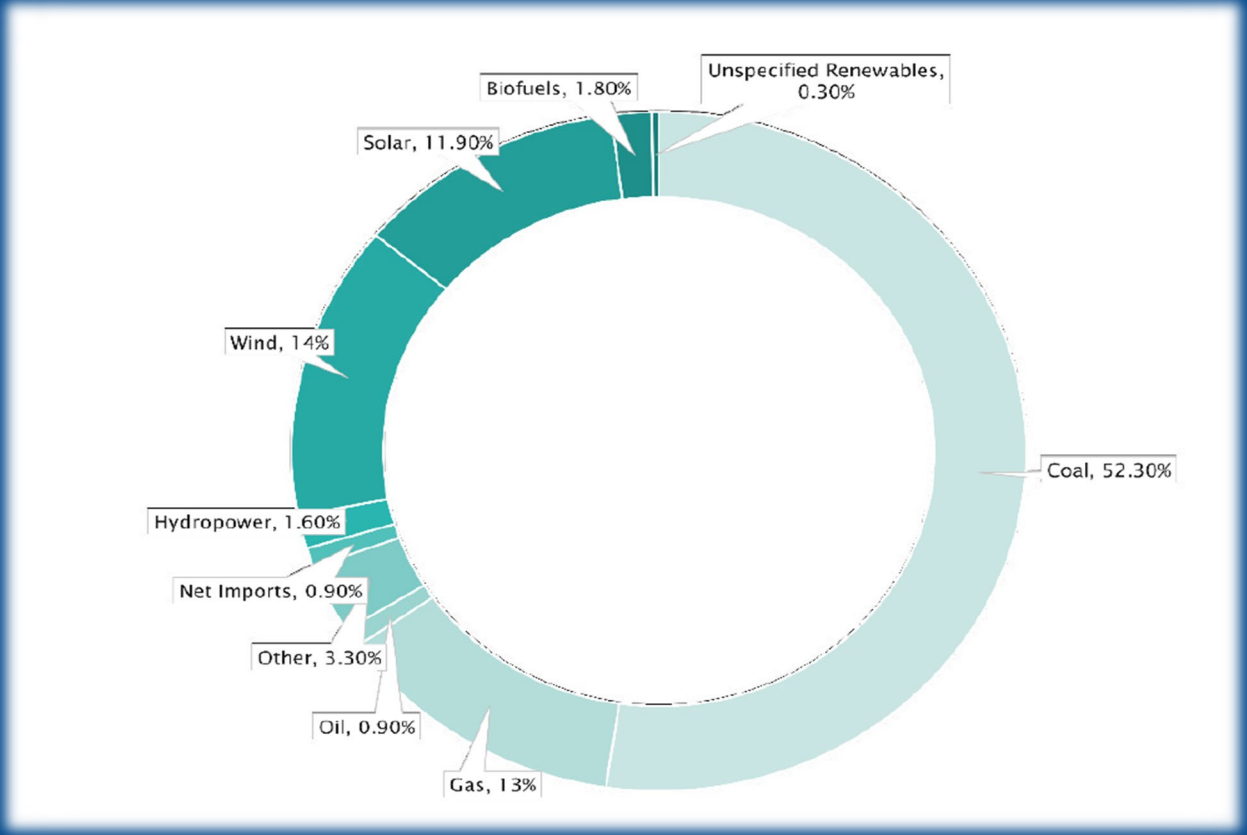
NPCC 2026 Spring Compliance & Reliability Webinar | May 20, 2026

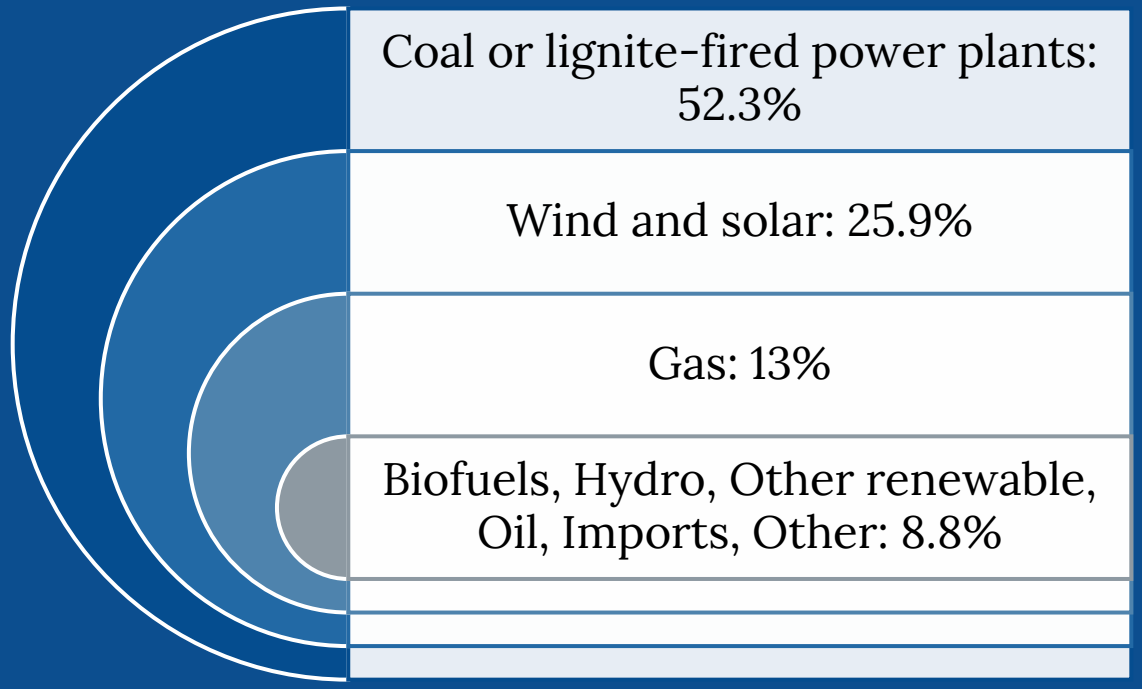
Agenda

- Poland Energy Make-up
- Event Summary
- Cyber Attack Timeline and Vectors
- CISA Actions
- Good Cyber Security Hygiene
- CISA Cyber Hygiene Tools
- Sources



Poland Energy Makeup





Source: Dragos: ELECTRUM: Cyber Attack on Poland's Electric System 2025 INTELLIGENCE BRIEF

Event Summary

On December 29, 2025, a coordinated cyberattack targeted multiple sites across the Polish power grid, specifically those connected to distributed energy generation. The attack affected communication and control systems at combined heat and power (CHP) facilities and systems managing the dispatch of renewable energy systems from wind and solar sites.

The attacks targeted numerous wind and solar farms, a private company in the manufacturing sector, and a combined heat and power (CHP) plant supplying heat to nearly half a million customers in Poland.

The Cyber Attack affected both information systems (IT) and physical industrial equipment (OT)

Effect: No power outages but loss of remote control and visibility at the affected sites.

Sites Attacked

- Attack targeted at least **30** wind and solar farms GCP (grid interconnection point) substation
- A Combined Heat and Power (CHP) plant
- Manufacturing sector company (opportunistic in nature and not linked to the other affected organizations.)
- Cloud Services (M365 service, Exchange, Teams, and SharePoint)

Image Source: Green and grey transmission tower during nighttime photo – Free Dark Image on Unsplash

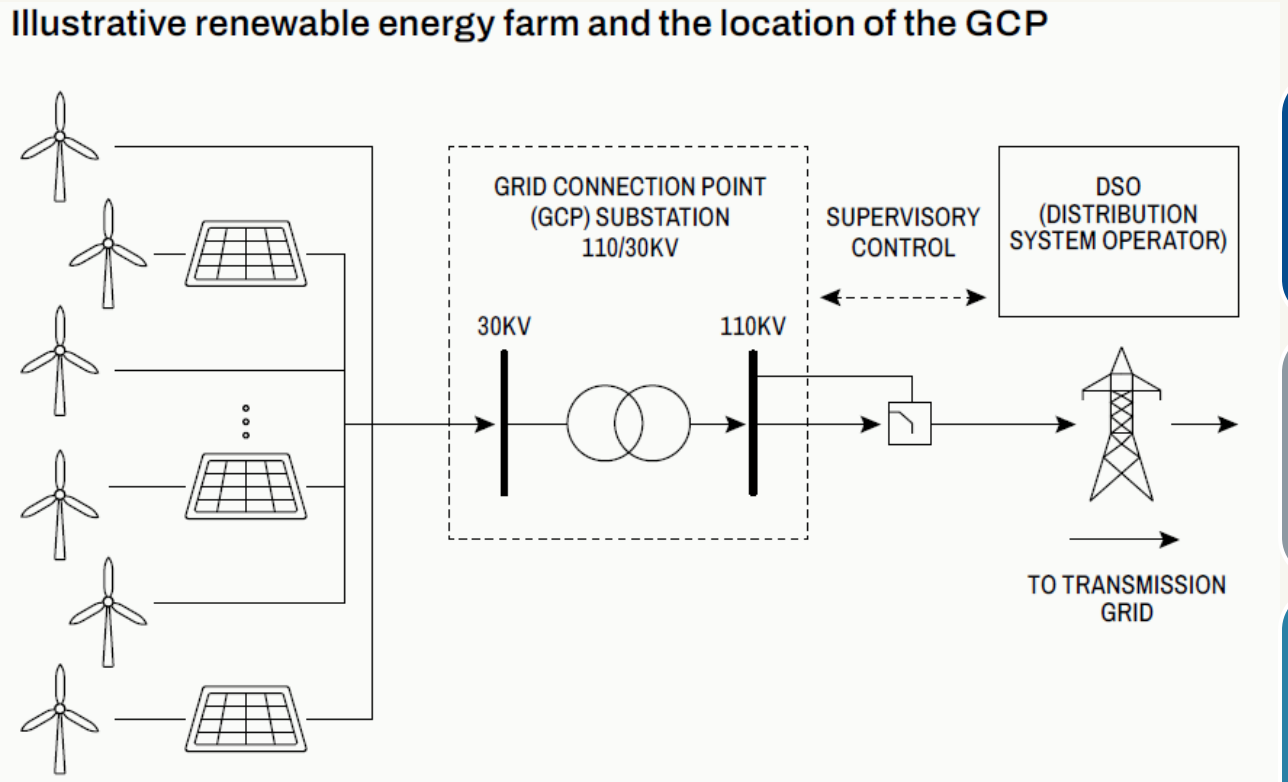
Attack Timeline

10 Month Attack Time Period from Initial Attack to Executed Attack

Exploited:

- VPN Perimeter Devices
- RDP
- Weak Passwords or Unchanged Default password
- Lack of East West Monitoring
- Known Device Vulnerabilities

Wind Farm and Solar



Source: ELECTRUM: Cyber Attack on Poland's Electric System 2025 INTELLIGENCE BRIEF

Many Remote unstaffed locations

Standardized Design using the same or similar RTU, HMI, Protection Relays, Serial devices, Primary and backup communication links (a cellular router), and Integrated VPN concentrator and firewall.

Operator's SCADA system and the GCP is required to pass through serial links.

Solar and Wind Attack Vector

- Firewall Device served as both a VPN concentrator and a firewall and exposed to the Internet
- VPN authentication to accounts defined in the configuration without multi-factor authentication
- VPN Logs Destroyed during the attack
- Firewall Device:
  - Past Vulnerably
  - Common practice in the industry to reuse the same accounts and passwords across multiple facilities
  - Threat actor gained administrative privileges on the device to access segregated VLAN Subnets

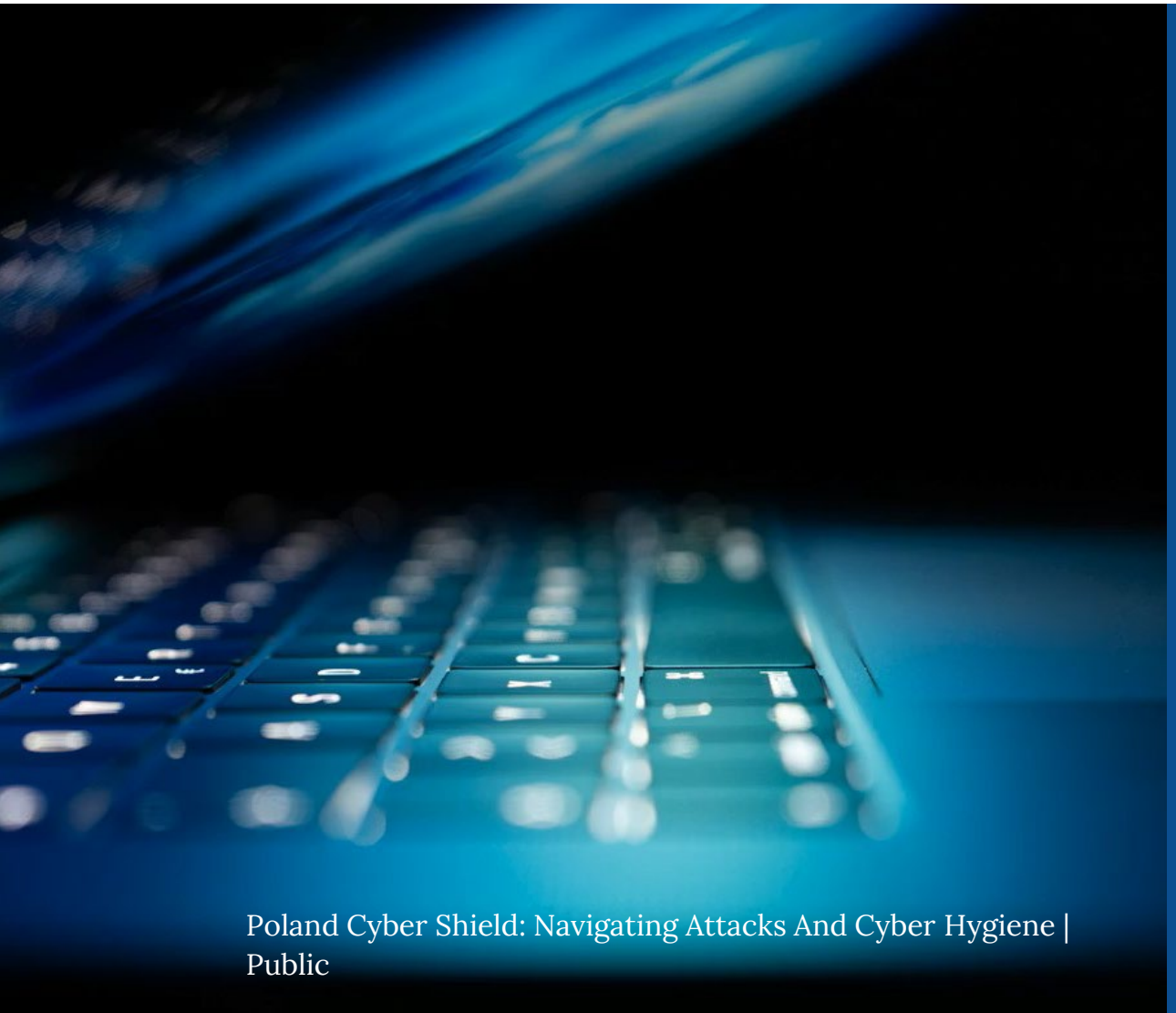
Solar and Wind Destructive Activities Part 1

Type 1 RTUs - configured with default credentials, including an account named “Default.” the attackers uploaded corrupt firmware which resulted in device reboot loop.

Type 2 RTUs - used default credentials to log in via the SSH console to an account with root privileges. The attacker then executed a command intended to delete all files from the system, which resulted in device failure

IEDs - used default credentials to log in via the SSH console to an account with root privileges. The attacker then executed a command intended to delete all files from the system, which resulted in device failure

Solar and Wind Destructive Activities Part 2



- **HMI -** machines were configured with a default password set during deployment for an account with local administrator privileges. Used PowerShell to conduct reconnaissance activities and damage data.
- **Serial Device Servers -** had the web interface enabled and were configured with default login credentials. Attackers restored the devices to factory settings, change the login password, and set the device IP address to an unreachable value

Attack on the Large CHP Plant

- Objective of the sabotage was the irreversible destruction of data stored on devices within the organization's internal network, achieved through the execution of the wiper malware.
- Long-term infiltration of the infrastructure and the theft of sensitive information.
- Attacker gained access to privileged accounts in the Active Directory domain, which enabled unrestricted lateral movement across the organization's systems.
    - Wiper used on Group Policy Object (GPO) but was detected by Endpoint Detection and Response (EDR) solution.

Image Source: unsplash/ Bird eye view photography of lighted building photo – Free Dark Image on Unsplash

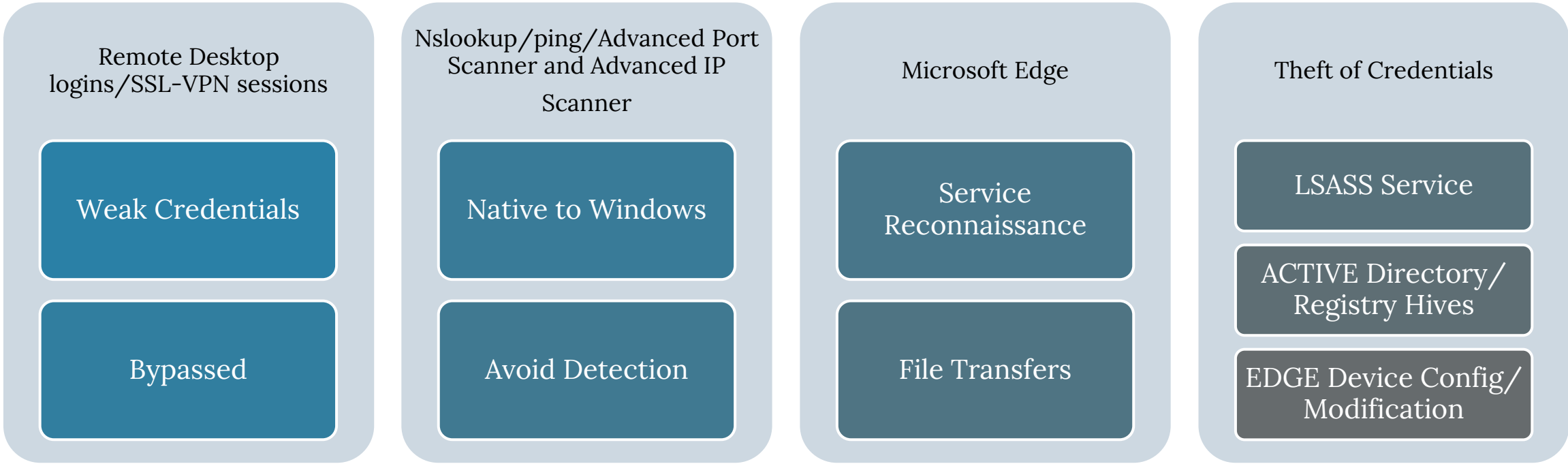
CHP Attack Process

- Between March and July 2025 – suspicious activity observed.
- **Initial Indicators**
  - Jump Host access, and RDP to perimeter devices and domain controllers.
  - Attacker focused on industrial automation systems and other systems on the network and taking screenshots.
  - Attacker initiated remote execution of a command that wrote information to a file named outlog.txt.
  - Attacker also interacted with the file systems of other systems, gaining access to them via the SMB protocol.
  - Attacker looked for the word “SCADA”.
  - Within a month Attacker initiated Privilege Escalation within the Infrastructure.
  - After gaining access to the SSL-VPN portal service, the attacker used bookmarks defined in the configuration file that allowed authorized users to access jump hosts via RDP.
  - Perimeter device had statically configured target user credentials, which enabled connections to the jump host from the SSL-VPN portal without the need to provide additional local or domain user credentials.

Image Source: Bing images Free to Share and Use/cyber skull - Search Images

Infrastructure Reconnaissance Traces

Analysis of the forensics data revealed that during the incident the attacker repeatedly established connections



Manufacturing Sector Company

Attacker gained access via a perimeter device.

- The device had been vulnerable in the past, and its configuration had been stolen and publicly disclosed
- Attacker introduced changes aimed at maintaining persistent access, even if user passwords were changed

Execution of the File-Destruction Script - PowerShell

Activities Against Cloud Services

M365 service, the attacker downloaded selected data from services such as Exchange, Teams, and SharePoint.

Focused on files and email messages related to OT network modernization, SCADA systems, and technical work carried out within the organizations.

Attacker also attempted to expand privileges by exploiting misconfigured permissions

Malware Used

DynoWiper - A native Windows binary.

LazyWiper - PowerShell-based script.

Detailed Analysis and indicators of compromise in **RT Polska** Energy Sector Incident Report – 29 December. This includes Detection rules.

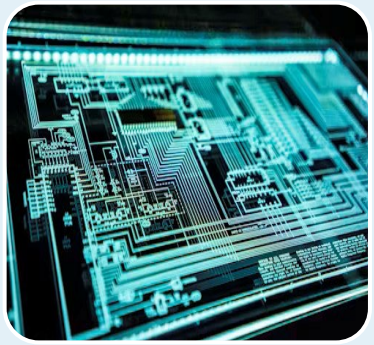
CISA Alert EOS

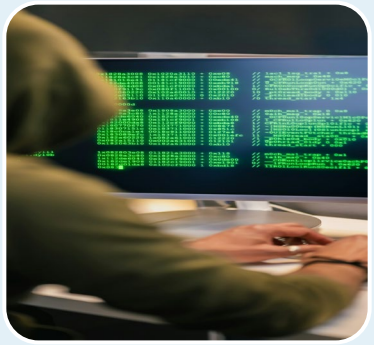
Poland Energy Sector Cyber Incident Highlights OT and ICS Security Gaps

- Binding Operational Directive (BOD) 26-02: Mitigating Risk From End-of-Support Edge Devices, end-of-support edge devices pose significant risks.
- CISA Fact Sheet: Primary Mitigations to Reduce Cyber Threats to Operational Technology
  - Multifactor authentication (MFA),
  - Asset management and identification,
  - Isolation of critical workloads and strong access policy, and
  - Encryption of data in transit.
- OT devices without firmware verification can be permanently damaged
- Threat actors leveraged default credentials, a vulnerability not limited to specific vendors, to pivot onto the HMI and RTUs

Sources: Home Page | CISA

Good Cyber Security Hygiene



Edge System Harding

- Remove OT connections to the public internet.
- Secure remote access to OT networks
- Elimination of default credentials
- Patching
- Monitoring

RTUs and Communications Infrastructure

- Monitoring of communication
- Change default/or generic passwords

Distributed energy networks require continuous, OT-native visibility

- Network Monitoring
- North/South and East/West

Defensible Architecture

- Avoid common configurations across multiple sites.
- Segment IT and OT networks (VLANS)
- Restrict access
- Script Management
- Monitor for Living off the land attacks

Secure Remote Access

- MFA
- Restricted Device access
- Restrict User Access
- Restrict Unauthorized Software Installations
- Monitor User Access
- Prevent Split-tunneling

Risk-based Vulnerability Management

- Patch Management
- Replace End of Support (EOS) devices
- Zero–Trust Security
- Incident Response Plan
- Recovery Plan
- Employee Cyber Security Training

CISA Cyber Hygiene Tools

For Organizations

Ford Foundation | Cybersecurity Assessment Tool

Assess your organization's cyber maturity, strength, and resilience and take actionable steps to improve elements of your cybersecurity program.

Global Cyber Alliance | Cybersecurity Toolkit for Mission-Based Organizations

Select no-cost tools and services to assess and enhance your cybersecurity posture through a guided process.

NetHope | Data Governance Toolkit

Develop or improve your data governance plan using these templates.

NTEN | Tech Accelerate

Use this no-cost assessment tool to evaluate your organization's technology adoption, practices, and policies.

[Link: Cybersecurity Resources for High-Risk Communities]

[Link: CISA: Cybersecurity Best Practices]

[Link: CCCS Cyber Security Guidance]

Cybersecurity is mission critical for individuals and organizations that belong to high-risk communities.

Disruption of Mission

A ransomware attack could disrupt your organization's operations by denying you access to your own data, devices, and network, halting your humanitarian efforts.

Data Leaks

Data leaks of your organization's sensitive information could enable cyber threat actors to target the vulnerable communities you serve.

Surveillance

Malware exploits could allow cyber threat actors to monitor and track your staff's activities, communications, and location.

[Source All Screenshots: Cybersecurity Resources for High-Risk Communities | CISA]

GCA Cybersecurity Toolkit™ For Mission-Based Orgs

TOOLBOXES

1 Know What You Have

2 Update Your Defenses

3 Beyond Simple Passwords

4 Prevent Phishing and Malware

5 Backup and Recover

6 Communicate Securely

7 Protect Your Email and Reputation

Sources

Dragos: ELECTRUM: Cyber Attack on Poland's Electric System 2025 INTELLIGENCE BRIEF

CERT Polska Energy Sector Incident Report (December 29, 2025)

CISA: Poland Energy Sector Cyber Incident Highlights OT and ICS Security Gaps (February 10, 2026)

CISA Fact Sheet: Primary Mitigations to Reduce Cyber Threats to Operational Technology

Summary

Cyber Hygiene: Apply cyber security measure on all company devices and systems.

Security Awareness Training: Educating staff to recognize phishing, pretexting, and social engineering attempts.

Multi-Factor Authentication (MFA): Implementing strong, phishing-resistant MFA (like FIDO2 keys) to prevent the use of stolen credentials.

Email Security Solutions: Utilizing AI-driven email filtering to detect phishing, business email compromise, and malicious attachments.

Questions?

Contact Us: npcc.org/contact

Michael Bilheimer
Compliance Monitoring & Enforcement

Break

RELIABILITY | RESILIENCE | SECURITY

POWERING TODAY. PROTECTING TOMORROW.

NERC

Modernization of Standards Processes and Procedures (MSPP) Implementation

NPCC

Soo Jin Kim
VP Standards and Registration

May 20, 2026

Guiding Principles

Transform and Modernize the Process

Re-envision a modernized standard development process to address evolving risks

Create Efficiencies

Identify areas of opportunity and recommendations to save time and remove redundant steps in the current process

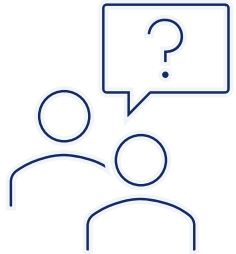
Develop a Trusted Process

Provide clear opportunities for stakeholder input, due process, openness, and balance of interests, remaining consistent with the requirements in Section 215 of the Federal Power Act

Stakeholder Engagement by the Numbers

50+ Presentations
during standalone meetings or as agenda items

5,800+ Attendees
at presentations since May 2025



5 Interactive Sessions with 1,100+ Attendees
to provide stakeholder access to Task Force members

10+ U.S. and Canadian Trades & Forums
engaged by MSPPTF members

11 Regional Entity-Hosted Events
Including webinars and in-person presentations

Recommendations

Standard Initiation

Semi-annual review and prioritization process

RSTC technically vets all requests for standard development projects

New RISC subcommittee determines path forward and oversees term sheet development

Standard Drafting

New Stakeholder SME Pool as expert bench to help develop standards

RISC subcommittee oversees drafting standards leveraging SME Pool, NERC staff, and technology tools

Emphasis on public comment process with straw polls, rather than multiple ballots, to drive consensus

Balloting

Individual entity balloting process to confirm consensus

Improved Registered Ballot Body voting rules

Refined Registered Ballot Body segment structure

Key Roles

RSTC

Centralized review of all Standard Initiation Requests

Provides technical vetting and recommended prioritization

RISC

Oversight of RISC Subcommittee

Ultimate approval of path forward for SIRs (based on RISC subcommittee determination)

Visibility and accountability

RISC Subcommittee

Strategic oversight and management of standard development process

Elected sector representatives, appointed at-large seats, and two RISC members as Chair and Vice Chair

Stakeholder SME Pool

Large dedicated technical pool of subject matter experts

Called upon by RISC subcommittee as needed to assist with reviewing and refining draft standards

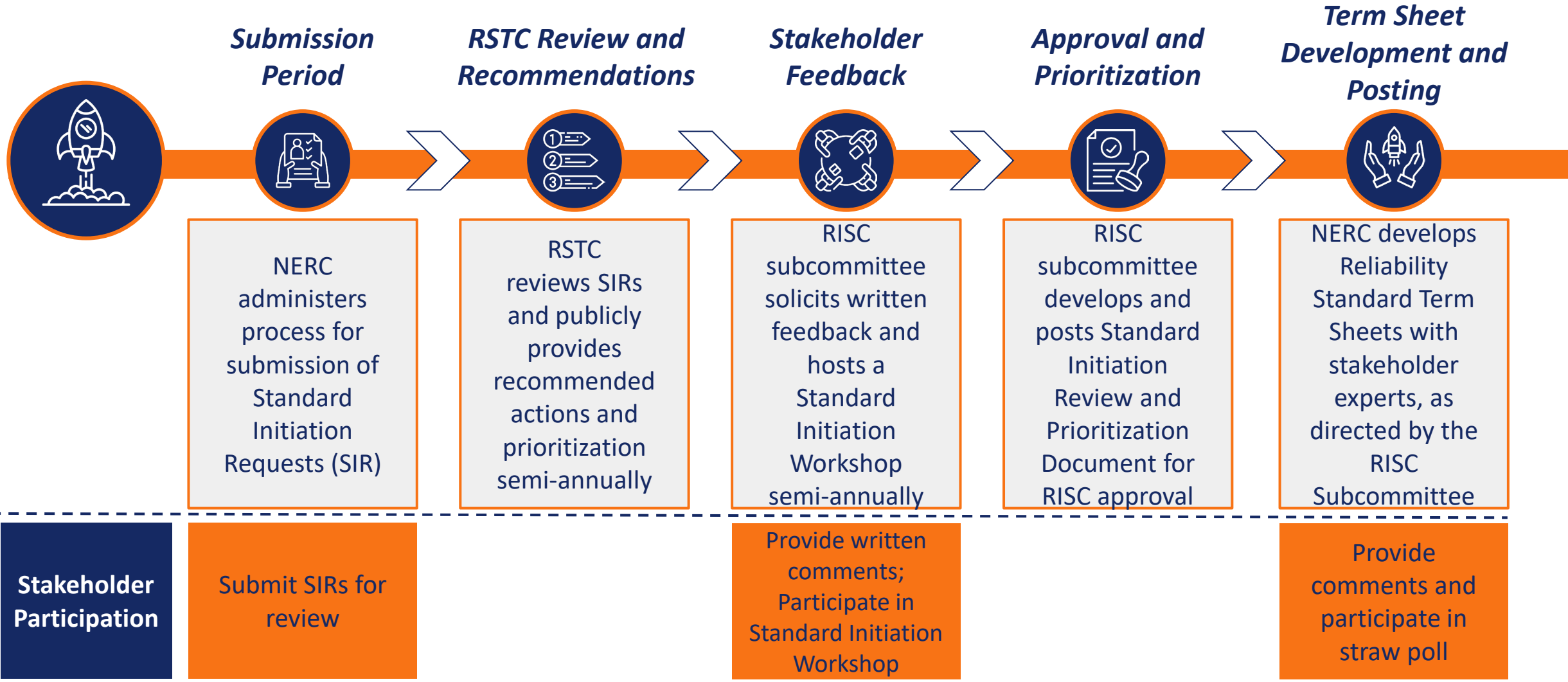
Project Teams

Formed by RISC Subcommittee with a subset from the Stakeholder SME Pool as needed

May be formally appointed or an informal ad hoc team led by NERC staff depending on project complexity

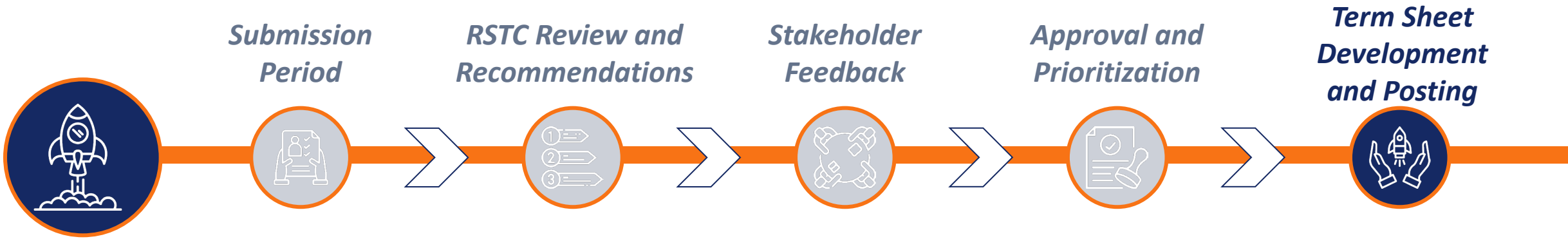
★ New Role

Standard Initiation Process Overview



Standard Initiation "Fast Track" Process

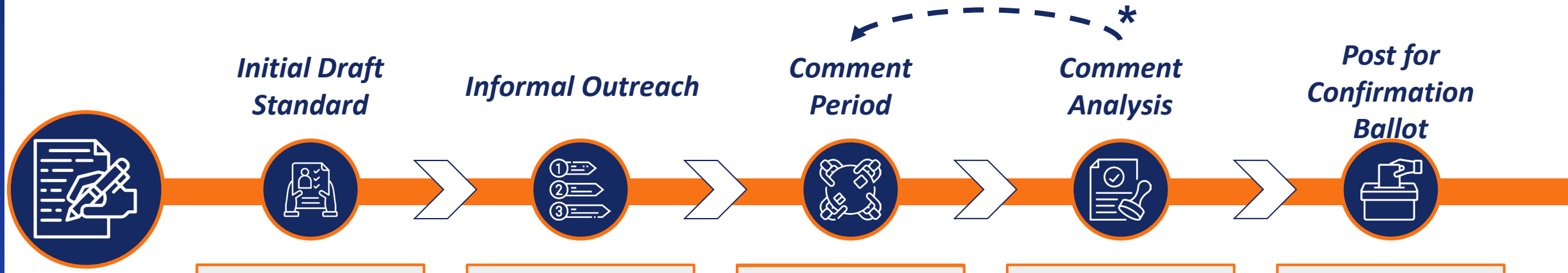
What	When	How
Expedited track for regulatory directives or urgent NERC Board directives	Following issuance of a regulatory or NERC Board directive to develop a standard	Begin with Term Sheet development, bypassing general intake and review process



Stakeholder Participation

Provide comments and participate in straw poll

Standard Drafting Process Overview



NERC develops "version zero" draft standard w/ Stakeholder SME Pool experts, as directed by the RISC Subcommittee

Project team conducts informal outreach and revises draft standard

Post draft standard for stakeholder comment period with straw poll (timing may be compressed for "Fast Track" projects)

Project team updates draft standard based on comments and outreach

* Revisions and additional comment period if needed

Standard posted for Confirmation Ballot

Stakeholder Participation

Participate in feedback process (possible technical conferences)

Provide comments and participate in straw poll

Standard Balloting Process Overview (with Passing Ballot)

Confirmation Ballot

Entities cast their ballots during the posting period (may be compressed for "Fast Track")

Ballot Approval

Ballot confirms stakeholder consensus; project team can make non-substantial edits if needed

Board Adoption

Standard presented to NERC Board for adoption

Stakeholder Participation

Cast ballot
(must be in RBB and have participated in a comment period)

Confirmation Ballot Does Not Pass

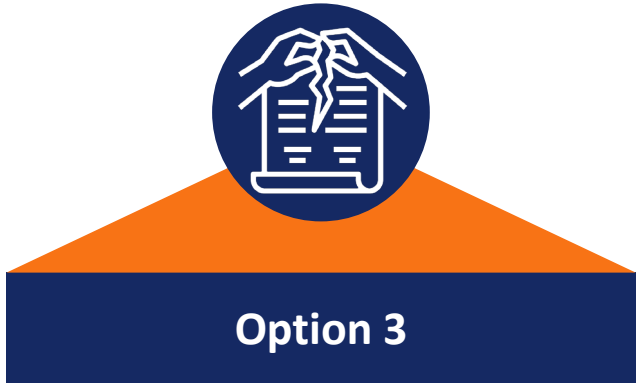
If the confirmation ballot does not pass, the project team shall review the ballot statements and present recommendations to the RISC Subcommittee, which will choose one of the following actions:

Option 1

Ask project team to revise the standard and post for extraordinary ballot

Option 2

Determine alternative action (e.g., refer back to RSTC, refer to Board for consideration of further action)



Option 3

End work on the standard

Registered Ballot Body Voting Rules

1 Relax Ballot Pool Rules

Entity is eligible to cast a ballot if they have participated in a comment period

2 Ease Participation Burdens

One voter could represent multiple segments, rather than requiring a distinct voter for each segment

3 Flexibility for Voting Representatives

Corporate entities would have improved flexibility to replace ballot body voters

Registered Ballot Body Structure

1	2	3	4	5
Segment 2 Weighting*	**Combine Segments 7 and 8***	**Consolidate Segments 5 and 6**	**Revisit Segment 9 Criteria***	**Retire Segment 10***
Ensure ISO/RTOs (including FRCC) have full and proportional segment weight to reflect their critical role in BPS reliability	Combine large electricity end users and small electricity users into one segment and remove participation thresholds to improve representation and engagement	Eliminate Segment 6 (Electricity Brokers, Aggregators, and Marketers) and consolidate members into Segment 5 (Electric Generators) to streamline participation while preserving all distinct voting interests	Update the government segment criteria to clarify eligibility, exclude oversight authorities, and include NYSRC and other qualified public-interest organizations	Remove Regional Reliability Organizations and remove Regional Entities from the RBB

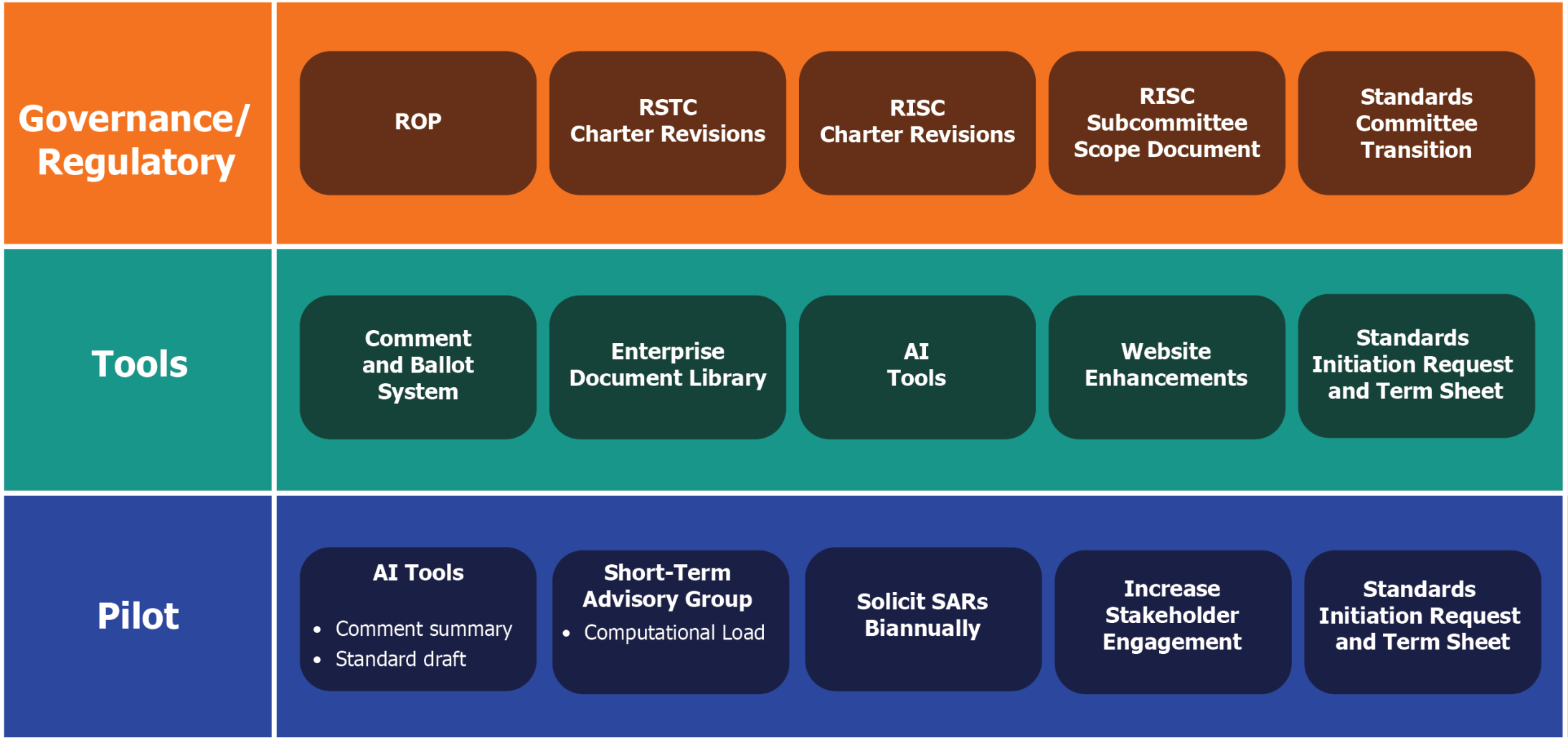
*Recommendations adopted (all or in part) from 2024 RBB Task Force Report

Registered Ballot Body Other Recommendations

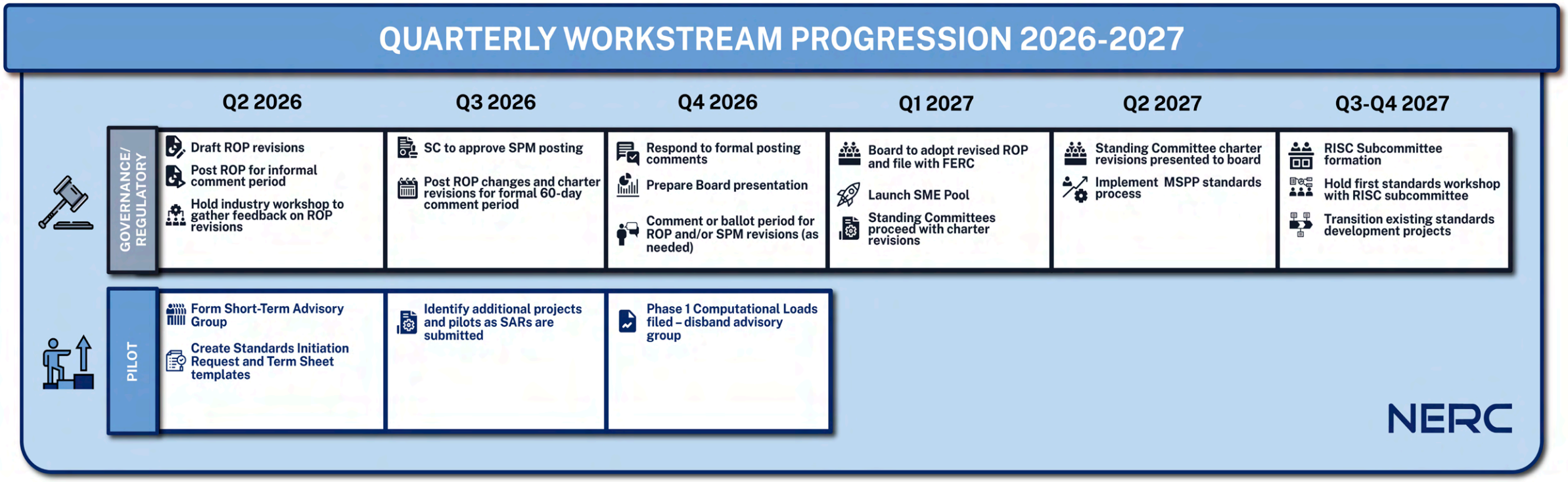
1	2	3	4
NCR Number Requirement*	**Stakeholder Outreach and Training***	**Review Segment Definitions**	**Two-Year Review**
Require the NCR number in the RBB for members who are NERC registered entities	Expand stakeholder outreach and training	Review segment definitions to improve clarity of qualifications	Review segment criteria after two years of implementation (consider new development in regulatory framework, changes in voter participation patterns, potential for mutually exclusive segment representation)

*Recommendations adopted (all or in part) from 2024 RBB Task Force Report

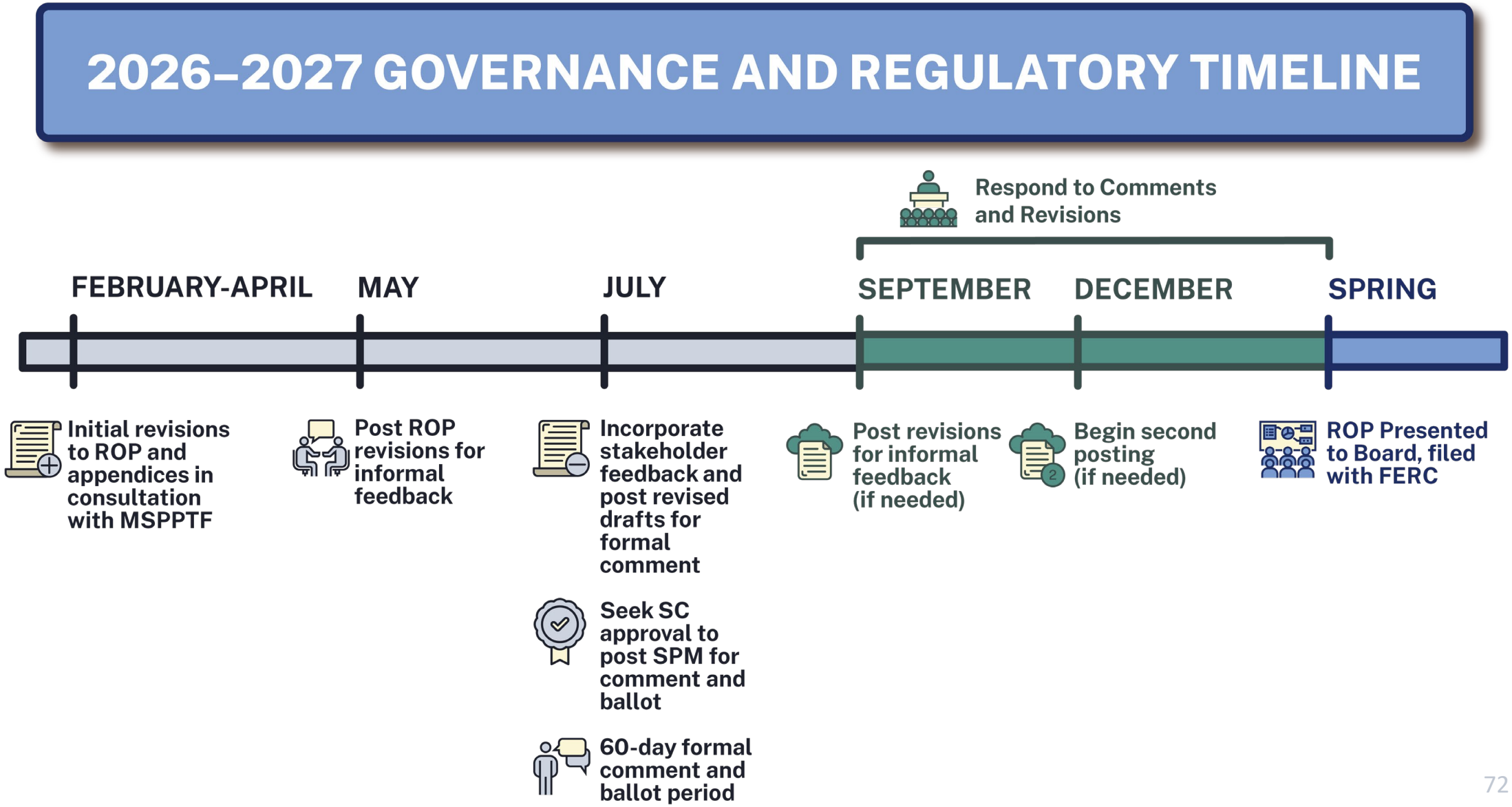
Areas of Focus



Implementation Timeline



Governance


2026–2027 GOVERNANCE AND REGULATORY TIMELINE
Respond to Comments and Revisions
FEBRUARY-APRIL
MAY
JULY
SEPTEMBER
DECEMBER
SPRING
Initial revisions to ROP and appendices in consultation with MSPPTF
Post ROP revisions for informal feedback
Incorporate stakeholder feedback and post revised drafts for formal comment
Seek SC approval to post SPM for comment and ballot
60-day formal comment and ballot period
Post revisions for informal feedback (if needed)
Begin second posting (if needed)
ROP Presented to Board, filed with FERC

What is Changing and Why

Standard Processes Manual (SPM): ROP Appendix 3A

- **To implement most MSPPTF recommendations, including standards development mechanics and responsibilities:**
  - SIR intake process and review coordination; term sheets
  - Standard development responsibilities of the new Reliability Standard Development Subcommittee
  - SME Pool, project teams, and drafting process
  - Comment and balloting processes

Other ROP Sections & Appendices

- **To conform with SPM changes and to address certain high-level MSPPTF recommendations related to standard development mechanics and responsibilities**:
  - Section 300, Reliability Standards Development
  - Removal of SC election procedures (Appendix 3B)
  - RBB segment updates (Appendix 3D)

Standing Committee Charters

- **Issues specifically pertaining to committee governance and authorities**:
  - Provide committees with the new authorities required by the MSPPTF recommendations
  - Outline the creation and governance of the new subcommittee

Certain recommendations will be addressed in committee process documents, not the charters

Revision Processes

Standard Processes Manual (SPM): ROP Appendix 3a	• Overseen by Standards Committee • Revised and posted at least once • Must be balloted and approved by Registered Ballot Body
Other ROP Sections & Appendices	• At least one 45-day public comment period • Board-approved changes submitted to FERC • FERC considers changes through open process (includes public comment opportunity)
Standing Committee Charters	• Oversight by the Board (through the Corporate Governance and Human Resources Committee (CGRHC)) • Presented to Board/CGHRC for approval in open sessions

Standing Committee Charters

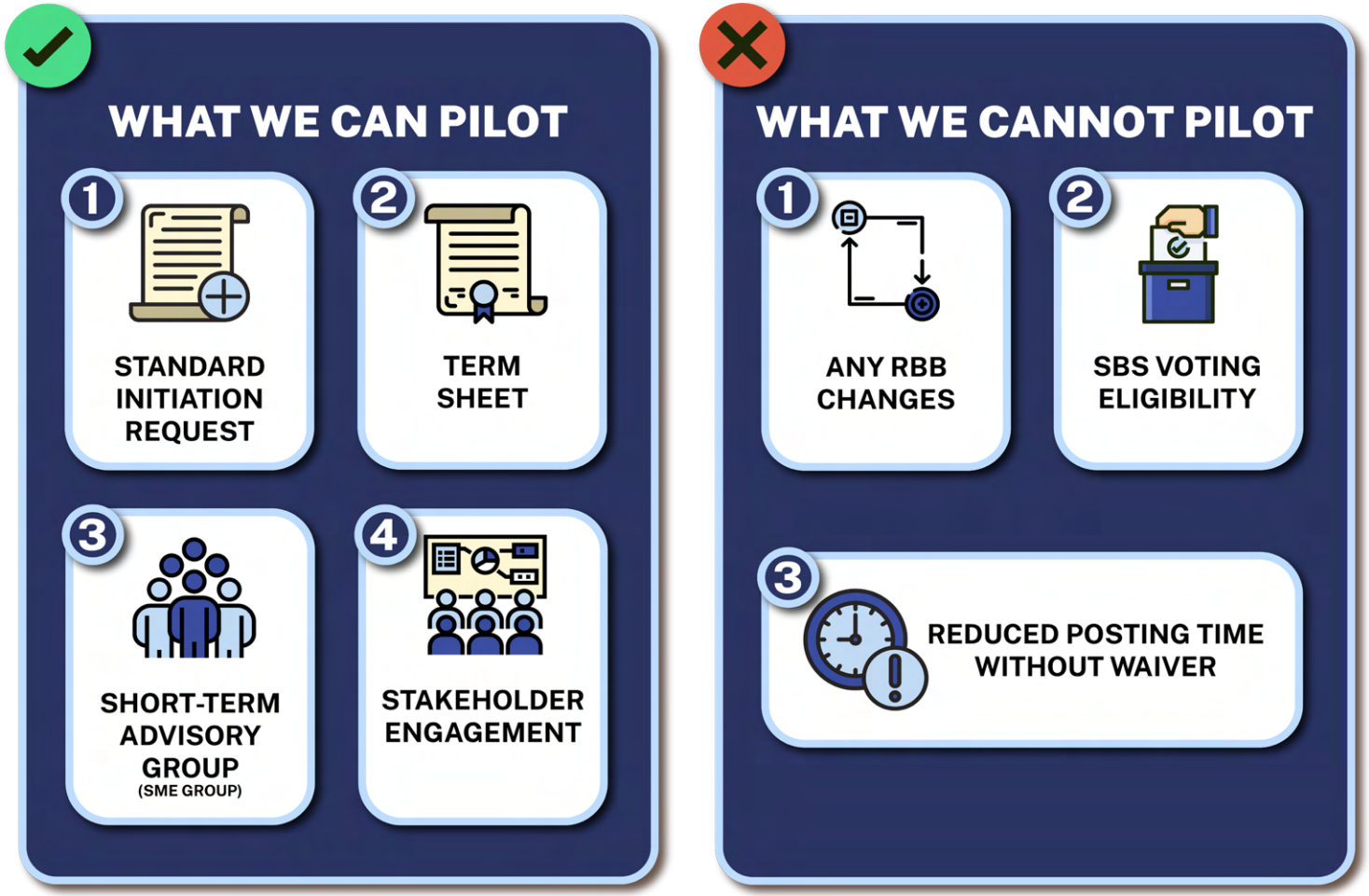
The NERC team has developed draft revisions to the RSTC and RISC charters and created a scope document for the new RISC subcommittee, referred to as to the Reliability Standard Development Subcommittee

These redlines are meant to…	These redlined charters are ***not*** meant to…
• Provide context for the draft ROP revisions by showing where certain MSPPTF recommendations will be implemented • Outline the proposed changes necessary to address MSPPTF recommendations	• Represent the final version of these charters or scope document as they are subject to committee and stakeholder comment • Capture every committee-specific process/procedure in the MSPPTF recommendations (e.g., the risk criteria used by the RSTC/RISC), as these are best developed by the committees/subcommittee via a process or procedure document

Charter amendments will have go through committee and Board approval processes

Pilots

PILOTING: WHAT'S IN AND WHAT'S OUT



Engagement

MSPP Implementation Webpage

Newsletters

Committee Updates

June Industry Workshop

Email

Informal and Formal Comment Opportunities

Presentations

Computational Load Project- SAR

"The goal of this project will be twofold and require developing:

1. Changes to the NERC Glossary to include large load entities, consistent with the proposed modifications for registration criteria in NERC's Rules of Procedure; and
2. a Reliability Standard addressing **reliability issues associated with integrating these large loads onto the BPS**."

"This drafting team will develop one or more Reliability Standard(s) to address in the near-term **essential actions** entities must take to assure the reliable integration of large loads into the BPS."

Drafting Team Goals & Areas of Alignment

Goal: Deliver Reliability Standard Requirements that…

1. Are essential actions that 'move the needle the most'
2. Can be most effectively delivered on the targeted Phase 1 timeline

Alignment: Focus on the core, process-related items in Phase 1…

1. Establish the right process that can set the foundation for subsequent phases
2. Leverage other existing process-related frameworks & concepts for integrating elements onto the BPS
3. Focus on process considerations (allow flexibility on process specifics, do not include technical specifics that are still evolving and/or may have regional variances)

Essential Actions – Phase 1

The drafting team is actively considering what are the "foundational" process-related requirements needed to support reliable integration of Computational Loads

Data Sharing

- **CL** Data → **Owners, Planners, Operators**

Interconnection Process & Requirements

- **TOs** have interconnection requirements specific to **CLs**
- **TOs** incorporate requirements from Planners & **Operators**

Protection & Monitoring (High-Resolution)

- Ensure protection is coordinated between **CLs & Owners**
- Ensure high-resolution monitoring for **CLs**

Commissioning

- **TOs** have a commissioning process (coordinated with **Planners** & **Operators**) specific to **CLs**

Interconnection Study & Modeling

- **Planners** have interconnection study process for **CLs**
- **Planners** ensure appropriate dynamic modeling for **CLs**

Operations Communication & Response

- **CLs** have communication protocols with **Operators**
- **CLs** respond to **Operator** Emergency Instructions

Phase 2 & Beyond

Other Important Gaps

(can build upon the foundational process-related requirements)

- Dynamic Model Validation
- Voltage & Frequency Ride-Through
- Annual Transmission Planning
- UVLS, UFLS, MLS
- Nuclear Coordination
- Balancing
- Critical Infrastructure Protection
- EMT Modeling
- Others

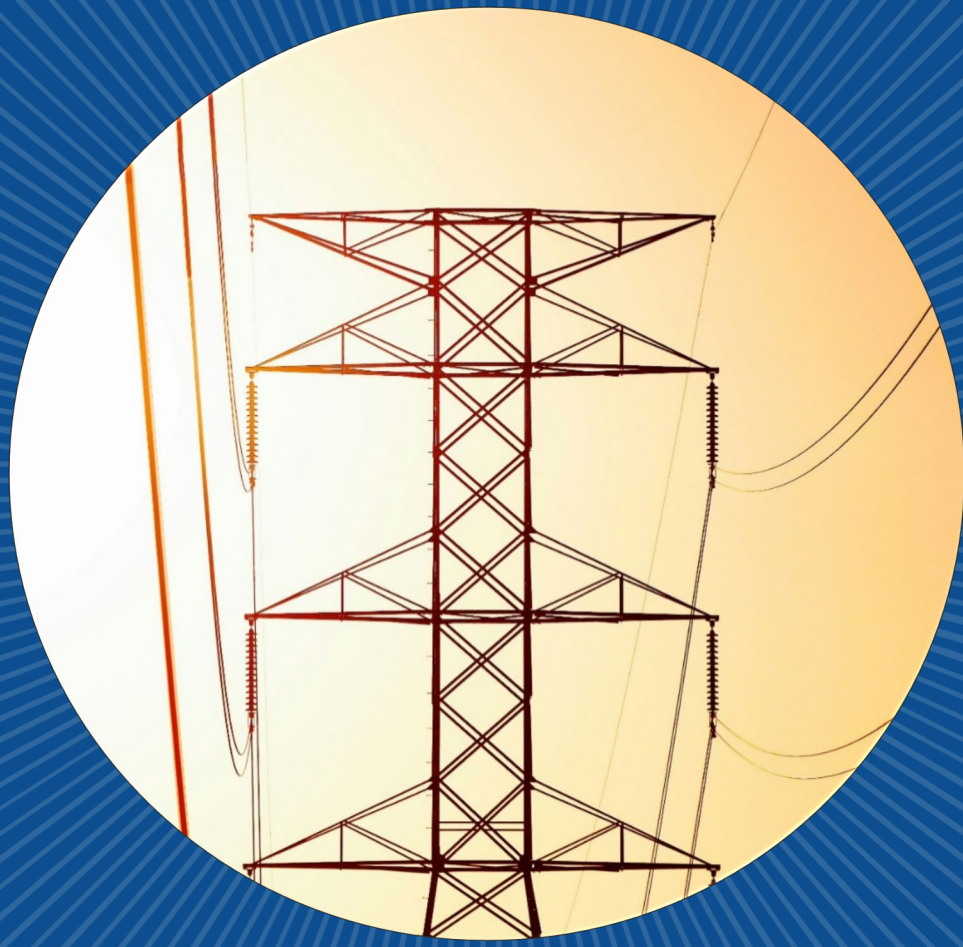
NERC

Discussion

NPCC

NPCC's Security Outreach

Strengthening Security Across the Power Sector



Doug Vitale – Manager, Security Outreach

NPCC Spring Compliance and Reliability Webinar | May 20, 2026

Agenda

- Purpose of Security Outreach
- Current Outreach Activities
- Physical/Cyber Threat Reports
- Security Outreach Webinars
- IST-5 Physical Security Working Group
- Fall Security Workshop
- Public/Private Sector Partnership
- Advancing NPCC Outreach

Purpose of Security Outreach

Protect the bulk power system in Northeastern North America by enabling information sharing, strengthening partnerships, and improving the collective resilience of the energy sector.

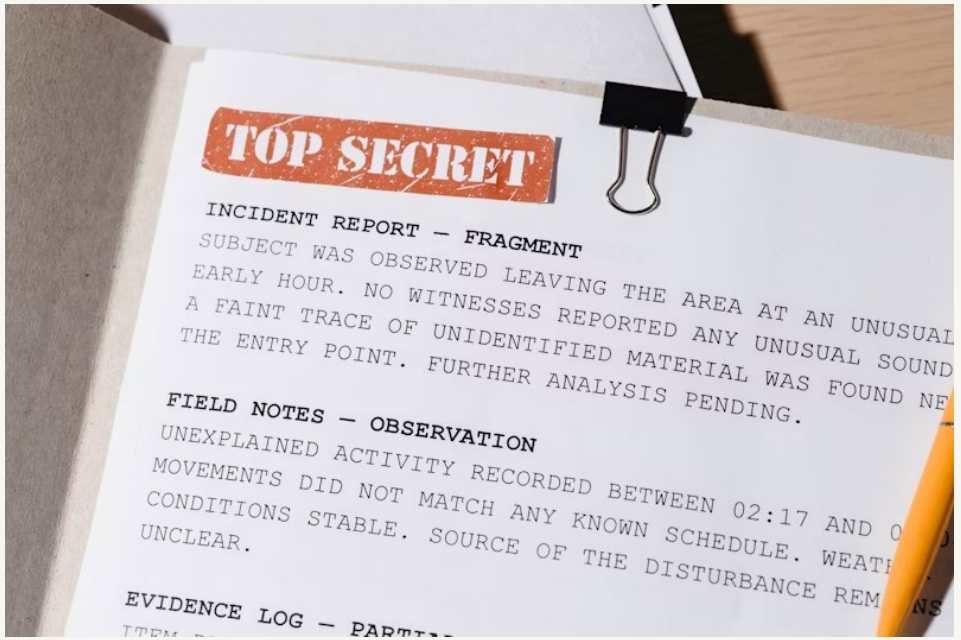
- Threat Intelligence and Information Sharing
- Collaboration and Partnerships
- Education and Training
- Exercises and Preparedness
- Assessments and Risk Management
- Awareness and Culture

Current Outreach Activities

- Physical/Cyber Threat Reports
- Security Outreach Webinars
- IST-5 Physical Security Working Group
- Fall Security Workshop
- Public/Private Sector Partnerships
- Entity Security Assessments

Physical/Cyber Threat Reports

- Review all intelligence and information documents to find relevant articles to the energy sector
- Articles include Cyber Threat, Domestic Threat, International Threat
- Reports are sent to a specific list of physical and cyber security representatives from NPCC's members and entities



Security Outreach Webinars

- Webinars are conducted on a periodic basis
- Relevant cyber/physical security topics and subject matter experts
- Past topics included: Drone Threat, Insider Threat, AI, Cloud Security, and Supply Chain Security

IST-5 Physical Security Working Group

- Meet quarterly
- Discuss relevant security topics
- Bring in external speakers
- Benchmarking within group
- Discuss and review CIP standard related discussions
- Physical and Cyber Security program development

Fall Security Workshop

- Held in conjunction with NPCC's Fall Compliance and Reliability Conference
- In-person participation of IST-5 and TFIST members
- External speakers invited to speak on relevant security topics
- In 2025, the NY State Police Intelligence Center briefed on an overview of their activities and responsibilities, terrorism threats to the US, and threats to the energy sector
- November 5, 2026, at Newport Marriott Hotel and Spa

Public/Private Sector Partnership

- One of the most important responsibilities of my job
- Help our mid-size and smaller entities develop relationships with local, state, federal, and provincial law enforcement (Left of Boom)
- Establish and maintain communication with local, state, federal, and provincial partners

Advancing NPCC Outreach

- Promote services to our stakeholders
- Increase entity security assessments
- Social media monitoring tailored to the NPCC region
- Design Basis Threat/Vulnerability of Integrated Security Analysis (VISA) Training
- Open communication with entities to improve their security resilience

NPCC

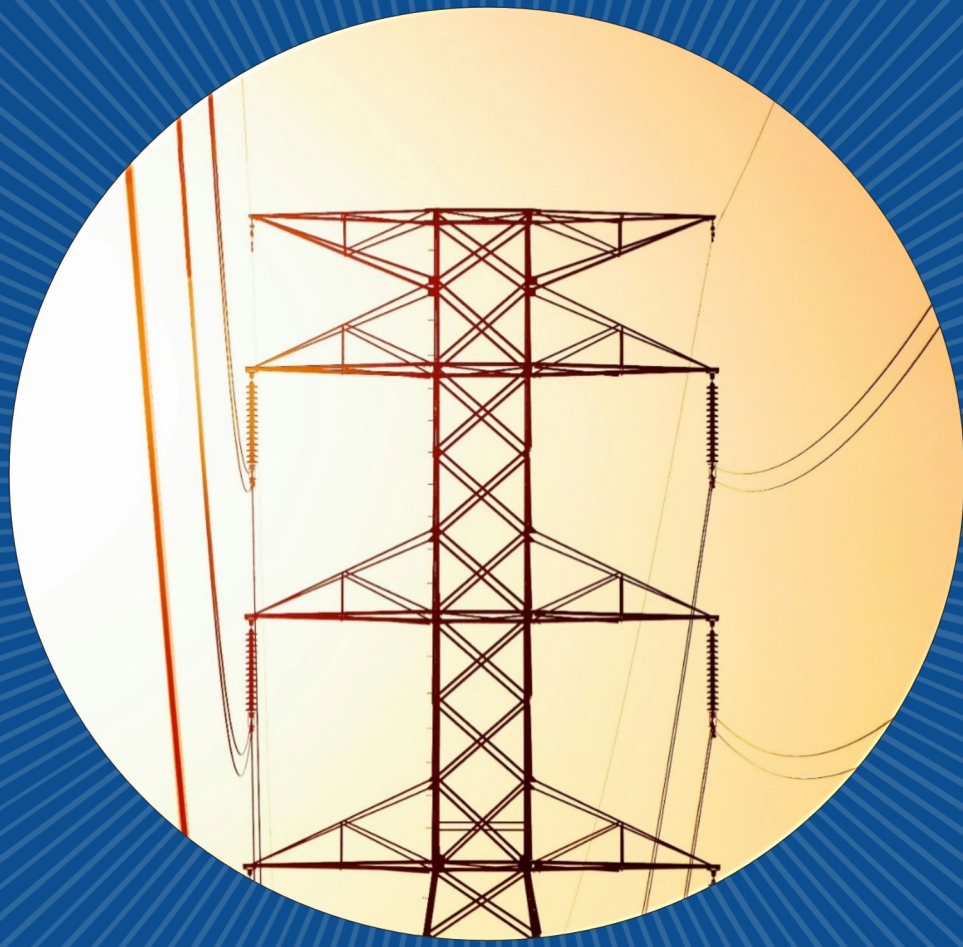
Questions?

Contact Us: npcc.org/contact

Situational Awareness
Doug Vitale

NPCC

PNC Abeyance Process



Arthur Brown
Associate General Counsel

NPCC Spring Compliance and Reliability Webinar | May 20, 2026

Public

What is the Value of Abeyance?

- To enhance the NERC standards development process agility that the ERO Enterprise and industry have focused on the past years.

- Help reduce the concern over compliance risk during standards development so that the focus can be on addressing risks to reliability.

Abeyance: When, What, Who?

- **When is abeyance considered and What is the initial criteria for consideration?**
  - During the standards drafting process
  - High priority project, new or modified standard, new technology needed to implement, high level of complexity, emerging reliability issue with no consensus on specific best practices
- **What is the purpose of abeyance?**
  - Develop insights from initial implementation of the standard that can then be fed back to NERC and industry to further refine standards as needed
- **Who determines which standards/requirements/parts for abeyance consideration?**
  - The ERO Enterprise will consider the candidates for the abeyance period

Abeyance: What it is NOT

Abeyance is NOT

- A free pass
- An extension of the implementation plan
- Time to sit and **wait** for feedback

What should you be doing?

- Working with NPCC
- Talking with your peers

Enforcement

- NPCC will **NOT** pursue an enforcement action during the abeyance period if registered entities implement the Reliability Standard in good faith.
- What is “Good Faith”?
- “Good Faith” in this context refers to a sincere intention to comply with the standard

Current Standards with an Abeyance Period:

- **EOP-012-3 Extreme Cold Weather Preparedness and Operations**
  - Where will be the abeyance language be within the Standard?
    - Section C. Compliance

- **MOD-032-2, R2 Part 2.1**

1.4. Compliance Abeyance Period: From the effective date of Reliability Standard EOP-012-3 until October 1, 2027, the CEA will not pursue an action under Sections 4A.0 or 5.0 of Appendix 4C to the Rules of Procedure for a failure to comply with Reliability Standard EOP-012-3 Requirement R1 Part 1.1 with respect to the calculation of the Extreme Cold Weather Temperature for an applicable generating unit, or any other failure to comply resulting from an incorrect calculation of the Extreme Cold Weather Temperature for that generating unit, against any entity acting in good faith to comply with the standard in accordance with the relevant implementation plan. "Good faith" in this context refers to a sincere intention to comply with Reliability Standard EOP-012-3 regarding all requirements based on the calculation of the Extreme Cold Weather Temperature for each applicable generating unit, following a reasonable and serious assessment by the entity in determining how this Reliability Standard should be applied to its particular facts and circumstances. Entities shall participate in any compliance monitoring activities undertaken by the CEA during this abeyance period and submit documentation as requested.

Abeyance: Common Questions

Will all Standards/Requirements have an abeyance period?	No, it will be evaluated by NERC and the Regions during the standards drafting process.
What if I'm not audited during the abeyance period?	Entities are expected to meet compliance on the effective date of the standard.
What will be the impact to the self-logging process?	There is no impact to the self-logging process.

Abeyance: Common Questions, cont.

How does the information feed back to standards for possible enhancements?	• The ERO Enterprise will be tracking and reporting on a periodic basis.
How will industry receive updates during the abeyance period?	• Periodic webinars/outreach activities
Can a SAR be introduced during the abeyance period?	• Absolutely, a SAR can be introduced at anytime.

Abeyance Process – NPCC Entities

How Does an Entity Submit PNC Abeyances?

- Step 1. Entities need to email PNCAbeyance@npcc.org to obtain direction on where to submit their completed spreadsheet.
- Step 2. **Within 5 business days** of receipt of a PNC Abeyance email, NPCC Enforcement will send the entity a:
  - Link to the applicable abeyance template
  - The submittal instructions for uploading the completed template to NPCC Portal
  - Request the entity send an email to PNCAbeyance@npcc.org again when information is uploaded
- Step 3. NPCC will evaluate the information uploaded.
- Step 4. NPCC will generally complete its evaluation **within 60 business days.**

Additional Resources

ERO Enterprise Guidance-Potential Noncompliance Abeyance Period

Template for EOP-012 PNC Abeyance

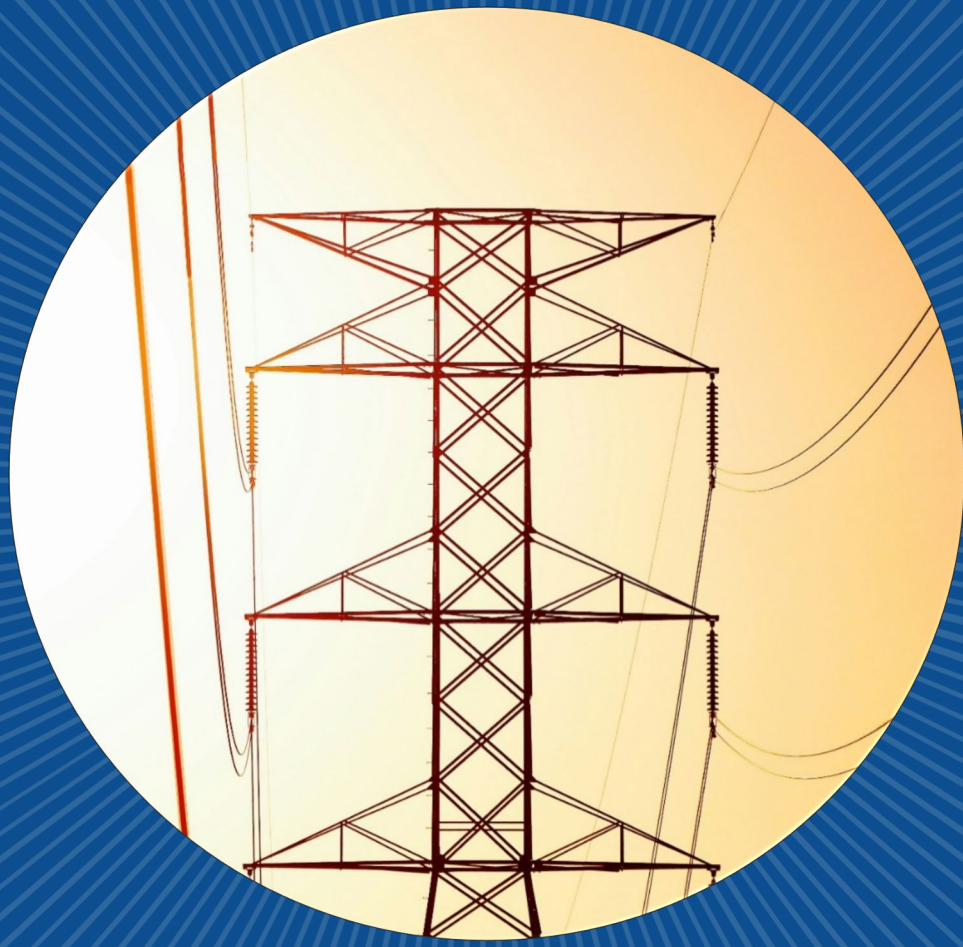
Questions?

Contact Us: npcc.org/contact

NPCC Enforcement
Arthur Brown

NPCC

NERC Large Loads Working Group Update



Diana Barsotti
Reliability Assessment and Performance Analysis

NPCC 2026 Spring Compliance and Reliability Webinar | May 20, 2026

NERC Large Loads Working Group

Level 2 Alert — Gather Industry Data, Extent-of-Condition

Level 3 Alert — Recommended Industry Actions

Characteristics and Risks of Large Loads
(White Paper 7/22/2025)

Assessment of Gaps in Existing Practices
(White Paper 3/11/2026)

Risk Mitigation for Emerging Large Loads
(Reliability Guideline 4/30/2026)

Large Load Disturbance Performance Ride-Through Recommendations

Dynamics Modeling Considerations for Large Loads

Plan Standard Authorization Requests Based on Assessment of Gaps

White papers available at: https://www.nerc.com/our-work/white-papers

Reliability Guideline available at: https://www.nerc.com/our-work/guidelines/reliability-guidelines

Alerts available at: https://www.nerc.com/programs/bulk-power-system-awareness/alerts

Questions?

Contact Us: npcc.org/contact

Reliability Assessments and Performance Analysis (RAPA)

Diana Barsotti

NPCC

NPCC 2026 Spring Compliance and Reliability Webinar Closing

Jacqueline Jimenez
Vice President, Compliance

May 20, 2026

Public

Thank you for Attending!

Presentation Slides

- Available on the NPCC website: https://www.npcc.org/events/npcc-2026-spring-compliance-and-reliability-webinar

Webinar Survey

- We'd love your feedback—please complete the webinar survey.

NPCC 2026 Spring Compliance and Reliability Webinar Feedback Survey

Upcoming NPCC Events

NPCC 2026 Fall Hybrid Compliance and Reliability Conference

- November 4 - 5, 2026
- Newport Marriott Hotel & Spa Newport, RI
- Register