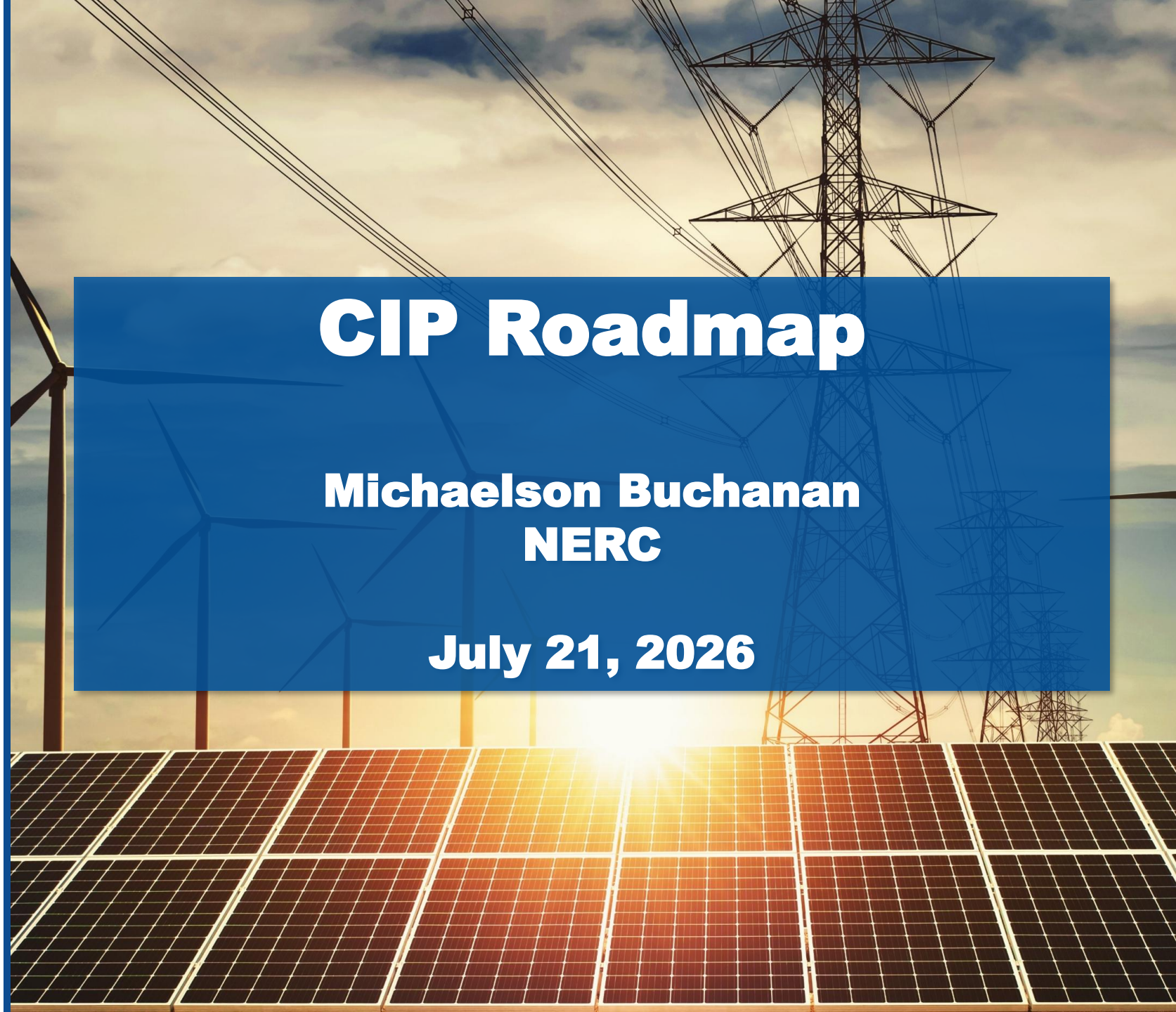
NERC

TEXAS RE



CIP Roadmap

Michaelson Buchanan
NERC

July 21, 2026

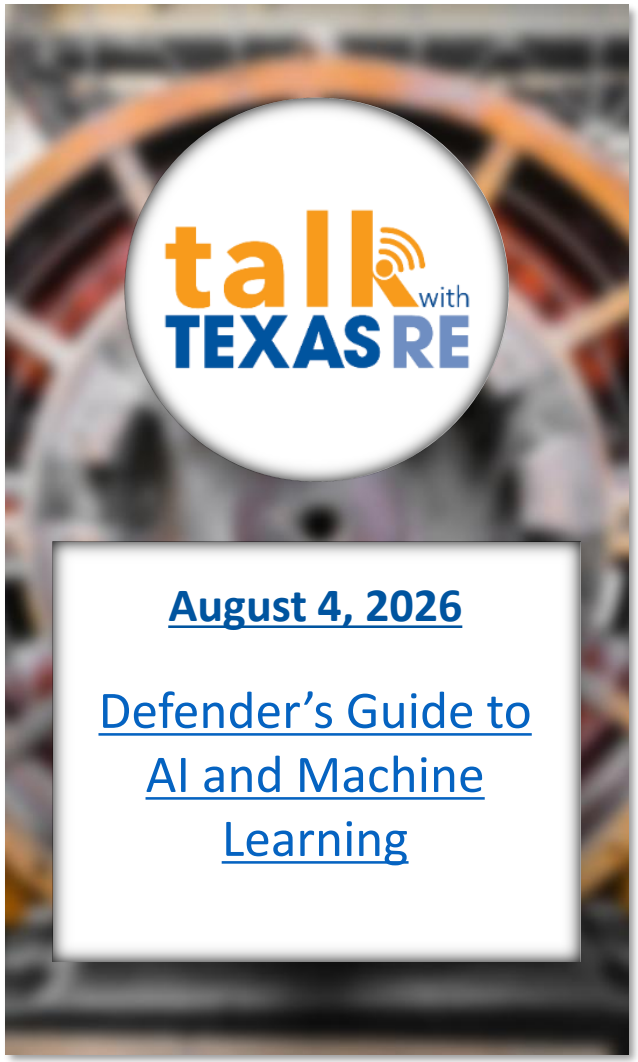
Antitrust Admonition

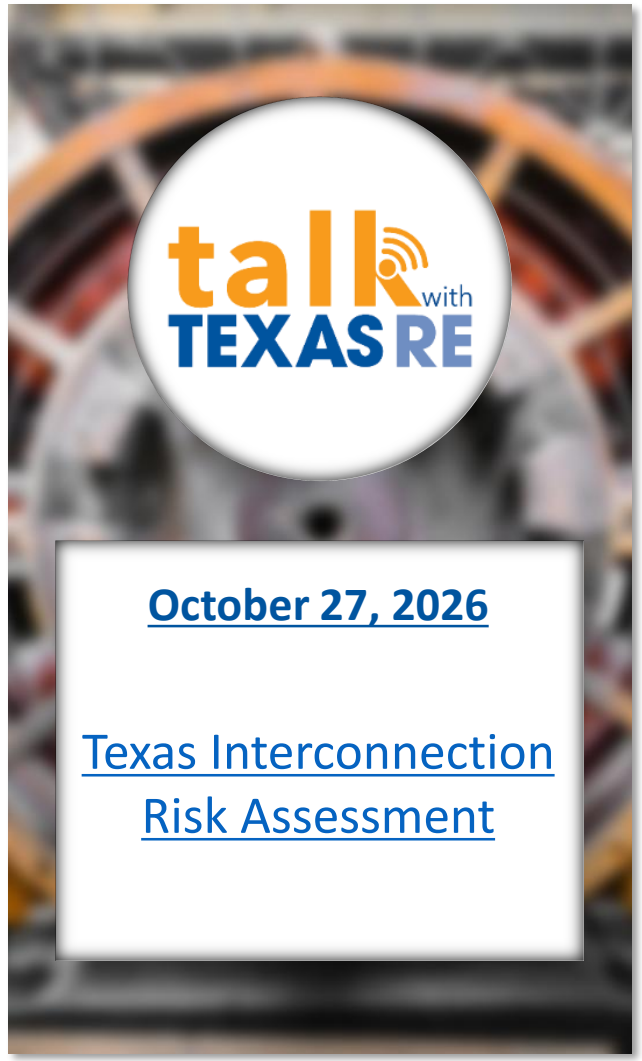
Because this event brings together market participants who may be viewed as actual or potential competitors, we must be mindful to conduct it in a manner that is consistent with the antitrust and competition laws. Participants should not disclose non-public, proprietary, or competitively sensitive information.

Attendees should exercise independent judgment and avoid even the appearance of discussions of agreements or concerted actions that may be viewed as restraining competition. For example, avoid discussions regarding current or potential vendors or suppliers that involve sensitive information like pricing or terms, or discussions involving employee wages or hiring decisions. 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 to compliance with applicable antitrust and competition laws. However, any questions on Texas RE's Antitrust Compliance Corporate Policy may be directed to Texas RE's General Counsel.

Upcoming Events at Texas RE





Upcoming Events at Texas RE

August 19, 2026

Winter Weatherization Workshop

September 16, 2026

Q3 MRC and Board Meetings

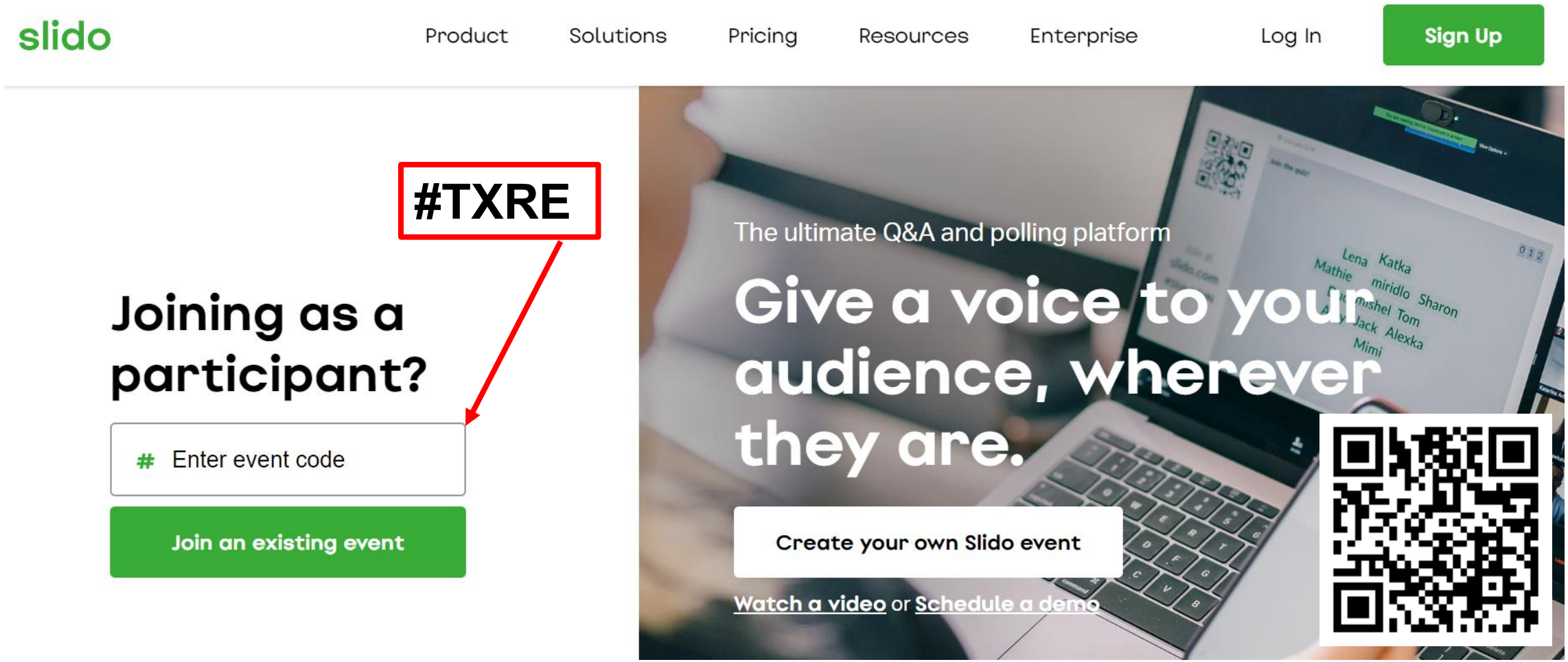
November 4, 2026

Fall Standards, Security, & Reliability Workshop

Upcoming ERO Enterprise Events

Date	Event
July 23, 2026	Future of Path Ratings in the Western Interconnection
July 29, 2026	SERC IBR Seminar #3
August 5, 2026	Protection Workshop
August 6, 2026	Planning Workshop

Slido.com


slido
Product
Solutions
Pricing
Resources
Enterprise
Log In
Sign Up
#TXRE
Joining as a participant?
Enter event code
Join an existing event
The ultimate Q&A and polling platform
Give a voice to your audience, wherever they are.
Create your own Slido event
Watch a video or Schedule a demo

RELIABILITY | RESILIENCE | SECURITY

POWERING TODAY. PROTECTING TOMORROW.

NERC

Talk with TexasRE

Critical Infrastructure Protection (CIP) Roadmap

Michaelson Buchanan
Manager, Engineering and Security Integration
July 21st, 2026

Background: CIP Roadmap Objective

Create a roadmap for ensuring CIP standards provide baseline protection for an evolving risk environment.

Evaluate CIP standards against emerging [cyber security and physical security risks] (e.g., network intrusion, new registrants, emerging cyber threats, cloud usage, AI, or other new technologies) and create recommendations and a roadmap to address gaps.

Background: Objective Approach

Identify

- Events
- ERO Reliability Risk Priorities Report
- E-ISAC, CISA
- Compliance
- Standards
- Complete Risk Scenarios
- Surveys

Assess & Prioritize

- Threats
- Vulnerabilities/Controls
- Likelihood
- Impact
- Relative Ranking

Mitigate

- Risk Appetite, Tolerance, Capacity
- Identify Mitigating Activities
- Prioritize Mitigation
- Evaluate potential changes to NERC CIP standards, and / or the potential to utilize other ERO Enterprise tools

Background: Collaboration and Communication

ERO Enterprise (2 Participants from each Region)

RSTC (SITES, SWG, SCS)

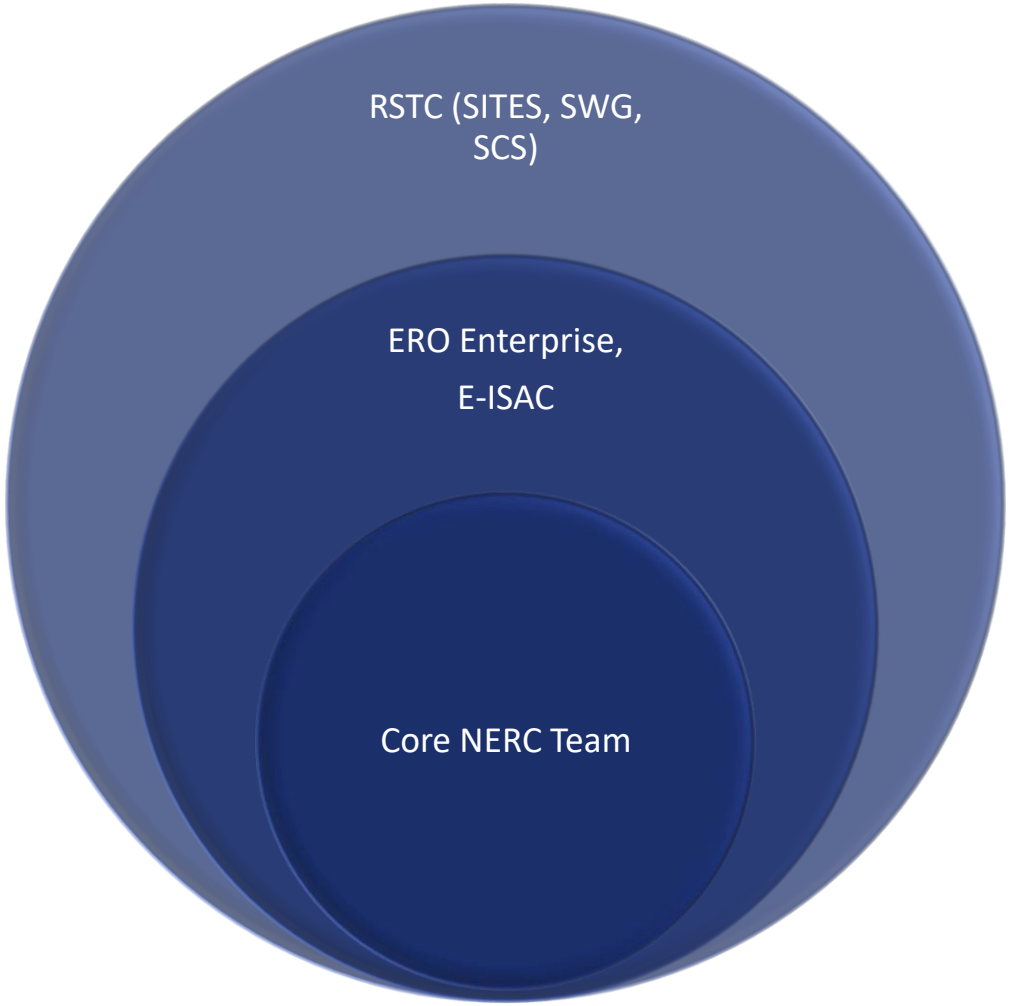
E-ISAC

Compliance Assurance

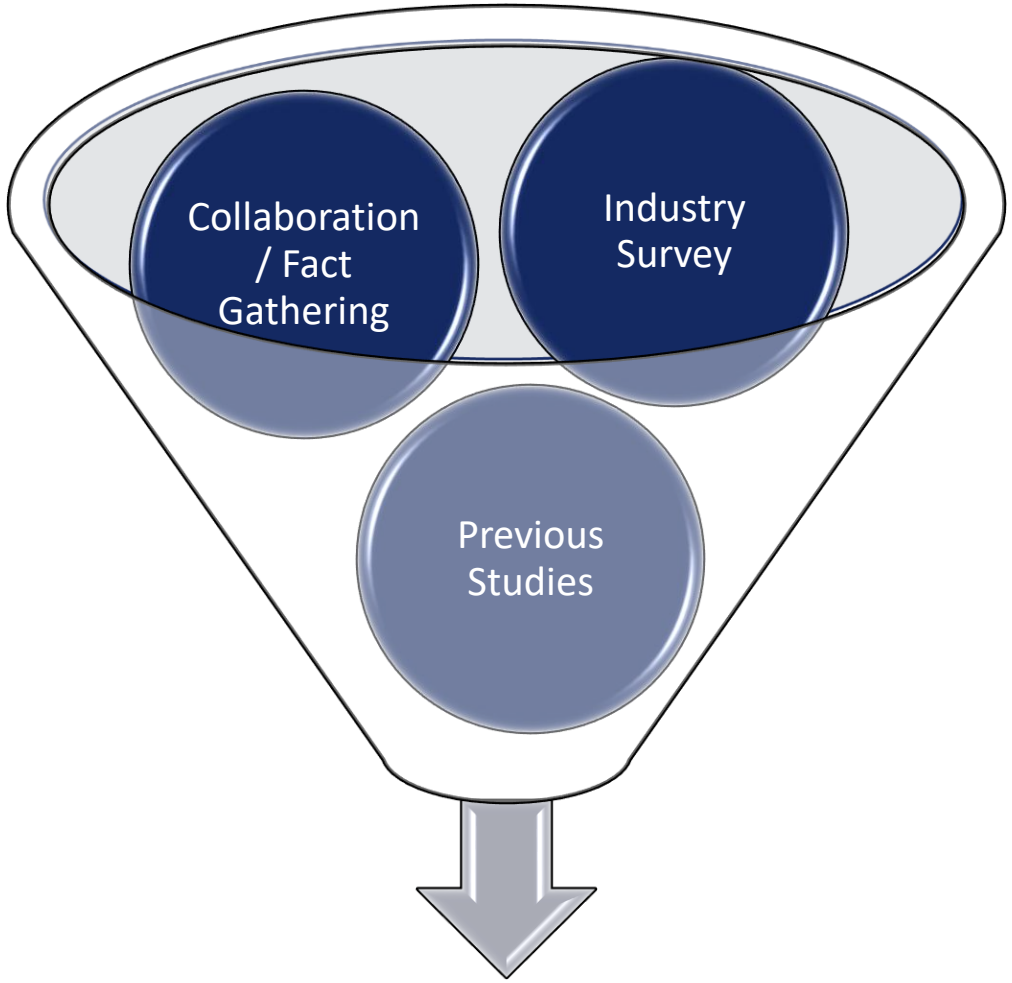
Standards

Engineering

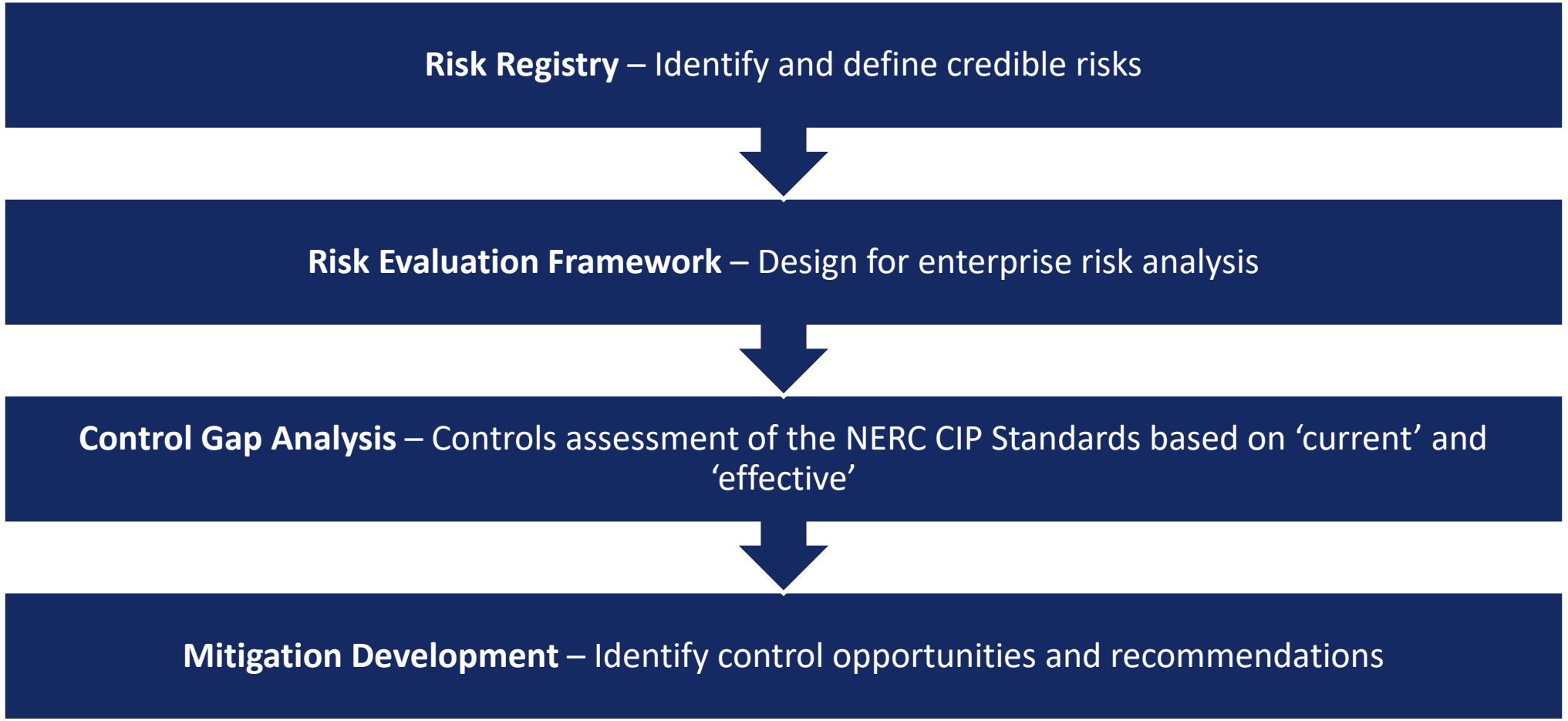
Situational Awareness



Background: Inputs



Process: Overview



Process: Building the Risk Registry

Purpose: Identify and define credible risks to the bulk power system (BPS)

Developed collaboratively with NERC and all six regional entities

Informed by E-ISAC, CISA, NERC Alerts, RSTC, and the 2025 RISC Report.

Included risks from threats, technologies, and asset categories (DERMS, EVSE, Cat-2 IBRs)

Included example scenarios with BPS impact

Process: Emerging Security Risk Survey

88 Survey Responses Received

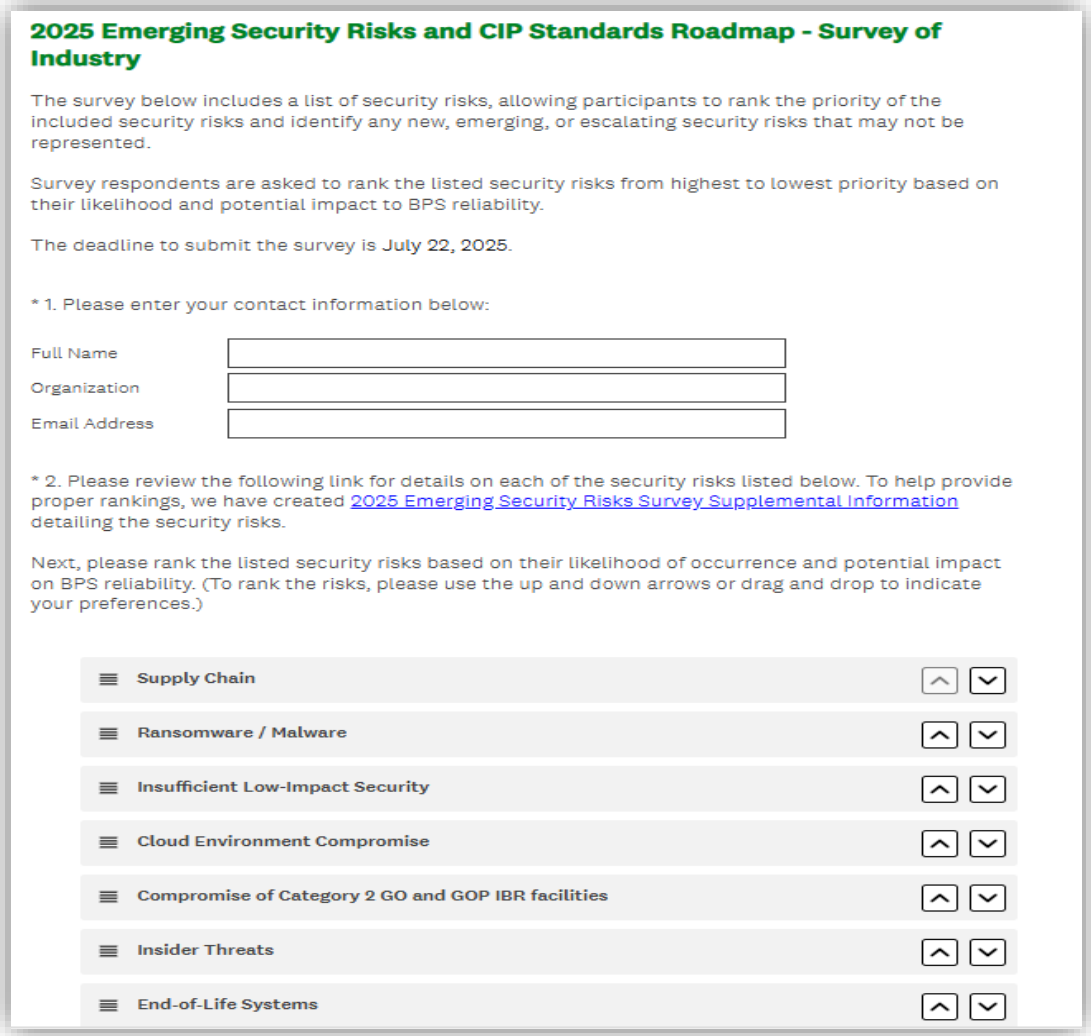
66 Comments Received

- 49 Response Validation
- 12 Survey Feedback

43 Responses Indicated Fatigue With Number of Risks

Tightly Coupled Distribution

Survey Results will be used as Input into Risk Assessment Process



2025 Emerging Security Risks and CIP Standards Roadmap - Survey of Industry

The survey below includes a list of security risks, allowing participants to rank the priority of the included security risks and identify any new, emerging, or escalating security risks that may not be represented.

Survey respondents are asked to rank the listed security risks from highest to lowest priority based on their likelihood and potential impact to BPS reliability.

The deadline to submit the survey is July 22, 2025.

* 1. Please enter your contact information below:

Full Name

Organization

Email Address

* 2. Please review the following link for details on each of the security risks listed below. To help provide proper rankings, we have created 2025 Emerging Security Risks Survey Supplemental Information detailing the security risks.

Next, please rank the listed security risks based on their likelihood of occurrence and potential impact on BPS reliability. (To rank the risks, please use the up and down arrows or drag and drop to indicate your preferences.)

- Supply Chain
- Ransomware / Malware
- Insufficient Low-Impact Security
- Cloud Environment Compromise
- Compromise of Category 2 GO and GOP IBR facilities
- Insider Threats
- End-of-Life Systems

Process: Survey Results (Risk Ranking)

1. Supply Chain
2. Ransomware / Malware
3. Insider Threats
4. Phishing & Social Engineering
5. Network Based Attacks
6. Physical Attacks on Infrastructure
7. End-of-Life Systems
8. Cloud Environment Compromise
9. Insufficient Cybersecurity Workforce
10. Insecure Protocols
11. Weaponization of Drones
12. Insufficient Low-Impact Security
13. Large Load Manipulation
14. Ineffective Incident Response & Recovery Planning
15. Compromise of Category 2 GO and GOP IBR facilities
16. Exploitation of Public Telecommunications
17. Targeting of DER Aggregator (DERA) Control Systems
18. Targeting of Artificial Intelligence (AI) Tools and Capabilities
19. Stolen Critical Energy Infrastructure Information or BES Cyber System Information
20. Regulatory Lag
21. Unregistered 3rd-Party Operators

Process: Security Risk Evaluation Framework

Liklihood Criteria							Impact Criteria						
Historical Precedent	Known Tactics, Techniques, and Procedures (TTPs)	Ease of Compromise	Exposure / Attack Surface	CIP Integration - Likelihood	Control Implementation - Likelihood	Control Efficacy - Likelihood	Scope of Impact (Single-Target)	Maximum Severity of Impact (Single-Target)	Coordination or Aggregation Potential	CIP Integration - Impact	Control Implementation - Impact	Controls Efficacy - Impact	Response and Recovery Preparedness

- Likelihood
  - *Historical Precedent*
  - *Known Tactics, Techniques, and Procedures (TTPs)*
  - *Ease of Compromise*
  - *Exposure / Attack Surface*
  - *CIP Integration - Likelihood*
  - *Control Implementation - Likelihood*
  - *Control Efficacy - Likelihood*
- Impact
  - Scope of Impact
  - Maximum Severity of Impact
  - Coordination or Aggregation Potential
  - CIP Integration - Impact
  - Control Implementation - Impact
  - Controls Efficacy - Impact
  - Response and Recovery Preparedness

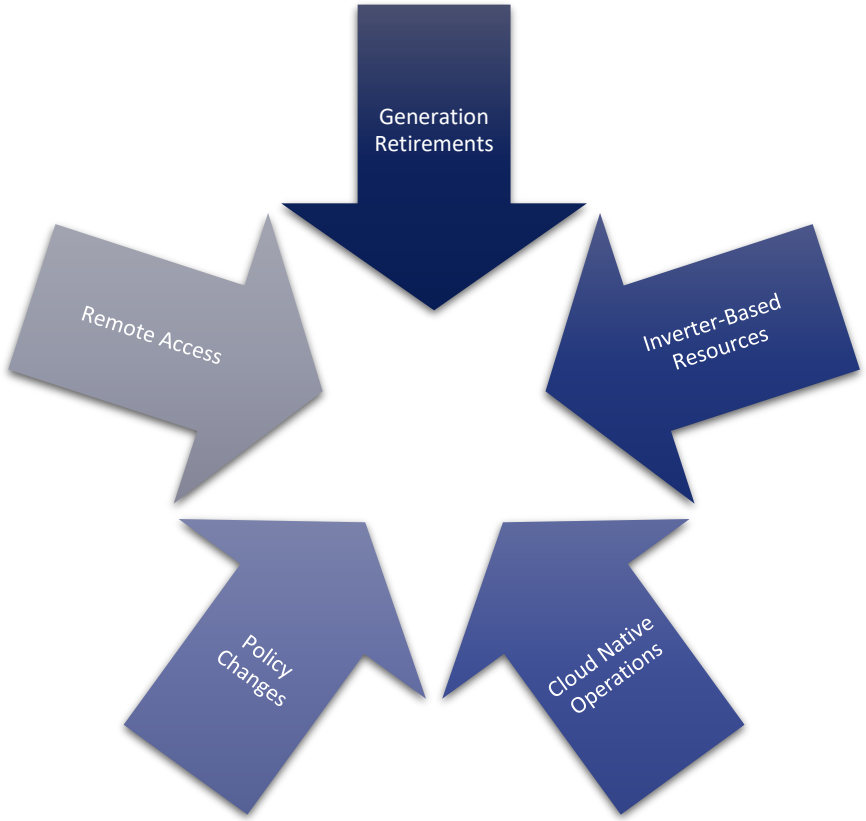
$$\text{Final Risk Score} = \Big[\underbrace{\frac{\sum LC}{n_{LC}}}_{\text{avg. Likelihood criteria}} \times \Big(1 - (1 - f_L) \underbrace{\frac{\sum LMC}{LMC_{\max}}}_{\text{mit. coverage}}\Big)\Big] \times \Big[\underbrace{\frac{\sum IC}{n_{IC}}}_{\text{avg. Impact criteria}} \times \Big(1 - (1 - f_I) \underbrace{\frac{\sum IMC}{IMC_{\max}}}_{\text{mit. coverage}}\Big)\Big]$$

Process: Identifying Mitigating Controls

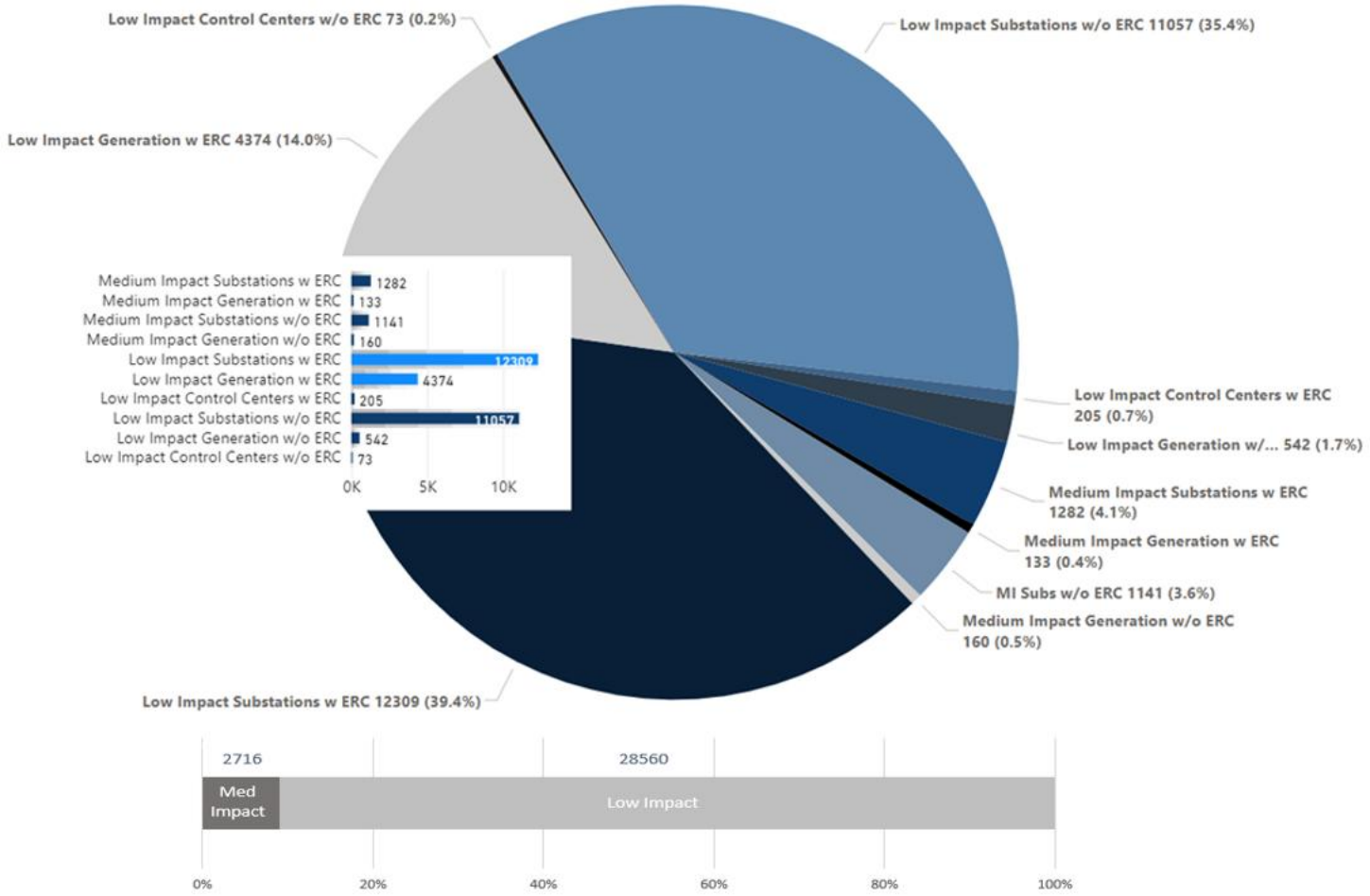
NERC

Table B.3: Risk-to-Control Mitigation Matrix																
								High-Level Control Enhancements								
Risks	*Risk Mitigation Tally*	Config/Change Management & Monitoring	Information Protection	Strong MFA	Network Documentation	Identity & Access Management	Strong RA Controls	Asset Management	Vulnerability/Patch Management	Internal Network Security Monitoring	Supply Chain / Third-Party Risk Management	Network Segmentation	Enhanced Logging & Alerting	Focused IRP Playbooks	Secure Protocol Management	Data Loss Prevention	Compensating Control Allowance
Control Mitigation Tally:		***14***	***14***	***13***	***12***	***12***	***12***	***11***	***11***	***11***	***10***	***10***	***10***	***8***	***7***	***6***	***5***
Supply Chain	***12***	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	
Physical Attacks on Infrastructure	***1***													1			
Phishing & Social Engineering	***11***	1	1	1	1	1	1	1	1	1		1	1	1	1	1	
Insider Threats to the U.S. Bulk Power System (BPS)	***8***	1	1	1	1	1	1	1		1		1	1			1	
Ransomware / Malware	***12***	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	
Cloud Environment Compromise	***12***	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	

Insights: Evolving Grid as a Risk Factor



Locations by Type and Impact Categorizations



CIP Roadmap Recommendations – Standards Modifications

Near Term | NERC-led Industry Team

- Develop a Standard Authorization Request (SAR) to establish use of Multi-Factor Authentication (MFA) for interactive remote access to low impact BES Cyber System (BCS).

Industry Volunteer Announcement released 3/9, kick-off 5/8/26

Near Term | NERC/RSTC-SITES Industry Team

- Assign a CIP-012 based study to develop a SAR addressing encryption and network security protections for public or carrier-dependent communications used in control center and facility operations.

RSTC Security Integration & Tech Enablement 2026 Workplan, Kick-off June 2026

Near Term | NERC

- Raise the Reliability Standards project 2023-09 Risk Management for Third-Party Cloud Services from a medium priority to a high priority.

Project Prioritized. Monthly in-person meetings. Informal comment period open through August 21

Roadmap Recommendations Standards Modifications

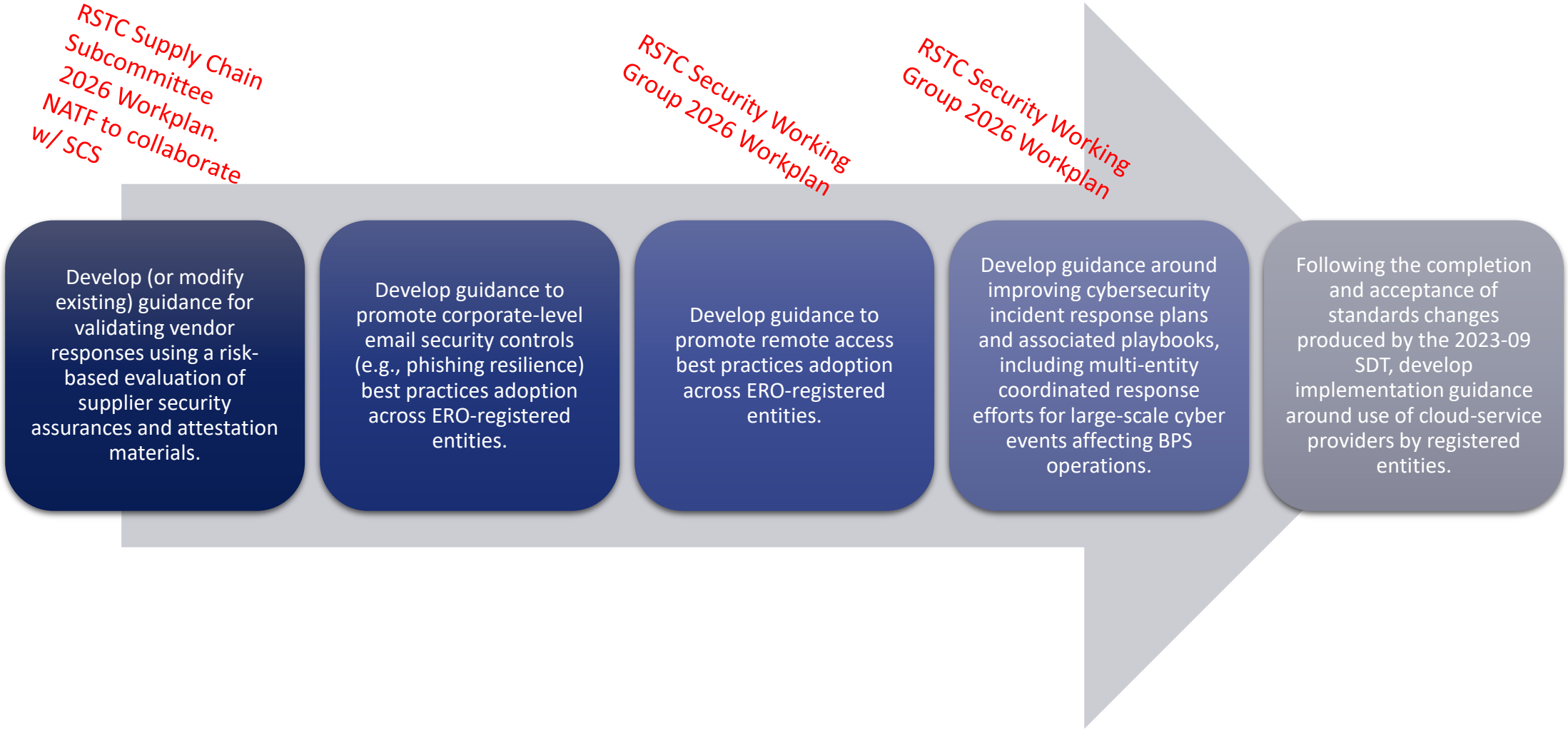
Intermediate Term | NERC-led or RSTC-led Industry Team (Q3)

- Conduct an evaluation of residual risk associated with inconsistent implementation of foundational controls (i.e., cyber hygiene) across all bulk power system (BPS) cyber systems to inform potential CIP applicability updates, especially low impact BCS. Focus areas to be considered should include but not be limited to:
  - Information protection
  - Identity and access management
  - Asset identification, configuration management, and lifecycle management
  - Network topology definition and trust boundary documentation
  - Vulnerability and patch management processes
  - Respond and mitigate threats from detected malicious code

Intermediate Term | NERC-led or RSTC-led Industry Team (Q3)

- Perform a focused risk assessment and control evaluation for Category 2 Inverter-Based Resources (IBR) to determine necessary cybersecurity control minimums and potential updates to CIP Reliability Standards.

Recommendations Guidance



NERC

Discussion