NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

NERC Critical Infrastructure Protection Roadmap

2025 NERC Work Plan Priority

January 2026

RELIABILITY | RESILIENCE | SECURITY




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

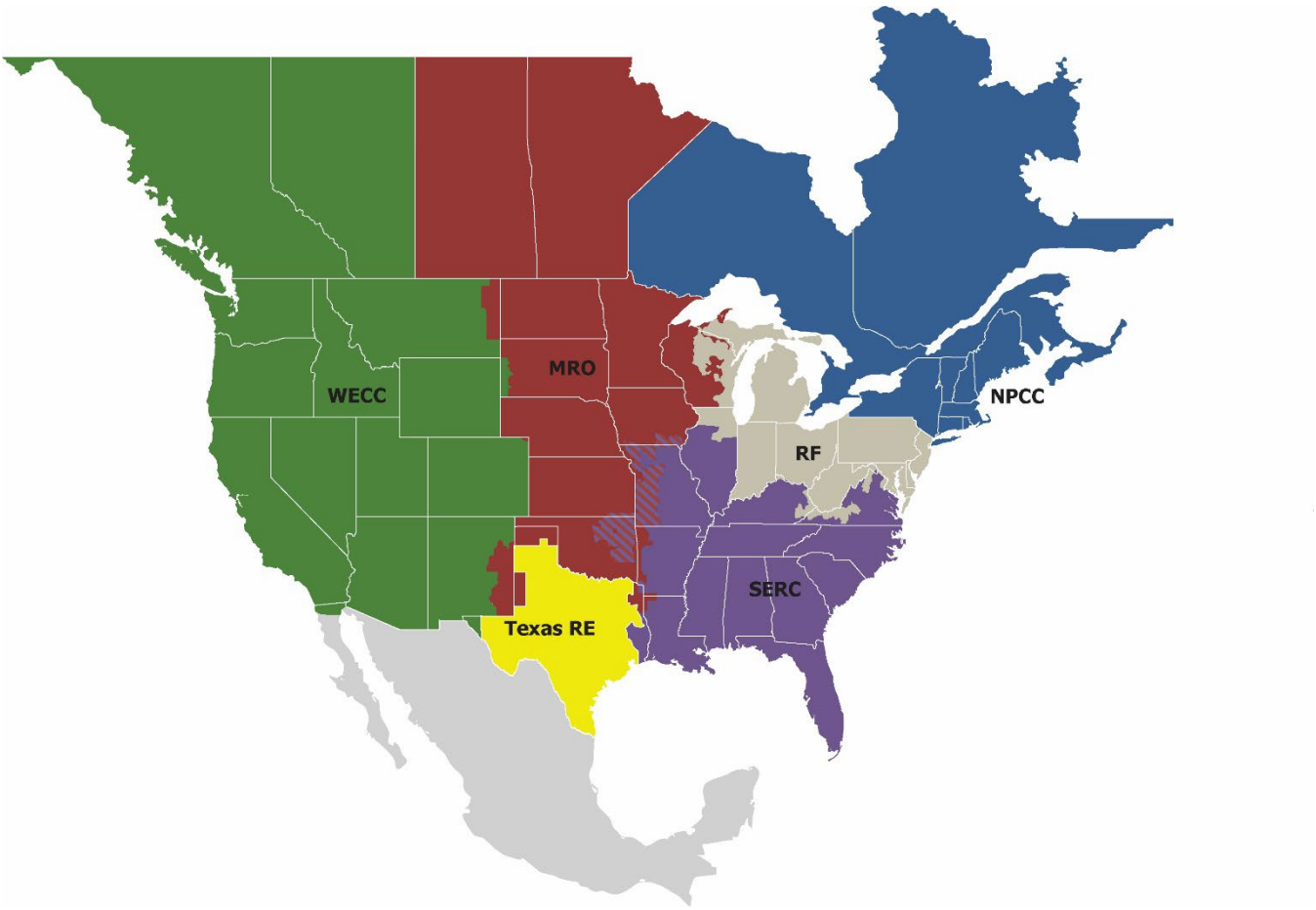
Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of NERC and the six Regional Entities, is a highly reliable, resilient, and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is made up of six Regional Entities as shown on the map and in the corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Regional Entity while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	WECC

Executive Summary

The North American BPS continues to evolve amid rapid technological, operational, and geopolitical change. As the grid becomes more dynamic, interconnected, and digitized, its exposure to sophisticated cyber and physical threats grows in parallel. Recognizing this shifting landscape, NERC's 2025 Work Plan[1] directed the development of a Critical Infrastructure Protection (CIP) Roadmap to evaluate whether existing NERC CIP Reliability Standards provide sufficient baseline protection against emerging and future risks and to chart a path for continued improvement.

This effort, led by NERC's Security Integration team in collaboration with the Regional Entities and industry subject matter experts, applied a structured, risk-based methodology to identify, assess, and prioritize the most consequential security risks to BPS reliability. The team compiled a comprehensive security risk registry, conducted an industry-wide survey to validate prioritization, and developed a consistent risk evaluation framework based on likelihood, impact, and mitigation maturity. Using these results, NERC evaluated current CIP coverage, ongoing standards projects, and potential enhancements that would most effectively reduce residual risk to the grid.

Findings indicate that, while the CIP standards remain the backbone of mandatory security controls for the BPS, the sector's operating environment has changed faster than the standards' scope and cadence of revisions. The bulk of operational technology (OT) that enables generation, transmission, and balancing operations now resides outside medium- and high-impact CIP coverage. Low-impact systems, third-party operators, and newly registered Category 2 inverter-based resource (IBR) registrants represent an expanding share of real operational dependency. As the grid transitions, these systems create new avenues for adversaries to aggregate small compromises into large-scale effects, a fact already recognized by both the Federal Energy Regulatory Commission (FERC) in its Notice of Proposed Rulemaking (NOPR)[2] for CIP-003-11 and the Low Impact Criteria Review Team (LICRT).[3]

The risk analysis revealed several recurring control themes with broad cross-risk mitigation value, alongside a small number of specialized risks that demand targeted, high-priority attention:

1. **Multi-Factor Authentication (MFA):** NERC should extend MFA requirements. Uniform deployment of MFA for all interactive remote access remains one of the most impactful and immediately actionable safeguards, substantially reducing risks tied to credential theft, remote access abuse, and insider threats.
2. **Foundational Cyber Hygiene:** Persistent gaps in basic controls - asset identification, configuration management, defensible network topologies, vulnerability management, and disciplined patching continue to undercut grid security maturity. The effectiveness of advanced capabilities, such as internal network security monitoring (INSM), ultimately depends on these fundamentals. A coordinated effort to ensure foundational cyber hygiene across all asset classes, including low-impact systems, would yield system-wide resilience improvements.
3. **Protection of Public Network Communications:** The electric sector's reliance on leased or carrier-provided telecommunications for supervisory control and data acquisition (SCADA) and automatic generation control (AGC) data remains a critical and under-secured dependency. Legacy protocols, such as DNP3, ICCP, and Modbus often traverse unencrypted links that fall outside the current CIP-012 scope. With recent state-sponsored campaigns (e.g., Salt Typhoon) targeting telecom infrastructure, expanding confidentiality and integrity protections to include facility-to-control-center communications is an essential priority.

The CIP Roadmap's recommendations are grouped into three action domains:

[1] 2025 Work Plan Priorities - Approved December 10, 2024
[2] Notice of Proposed Rulemaking for Reliability Standard CIP-003-11 (Docket No. RM25-8-000, 89 Fed. Reg. 66752, Sept. 23, 2025)
[3] https://www.nerc.com/globalassets/our-work/reports/white-papers/nerc_licrt_white_paper_clean.pdf

- **Reliability Standards Modifications:** Near-term standard authorization requests (SAR) to mandate MFA, extend network-security protections for use of public telecommunications infrastructure, and raise the Reliability Standards project 2023-09 Risk Management for Third-Party Cloud Services[4] from a medium priority to a high priority; intermediate-term evaluations to standardize foundational cyber hygiene controls and assess residual risk tied to low-impact BES Cyber Systems (BCS) and Category 2 IBRs
- **Guidance Development:** Security guidance for vendor assurance validation, email security (e.g., phishing resilience), drone-threat response, remote access best practices, and improved incident response playbooks
- **Ongoing Risk Monitoring:** Sustained ERO Enterprise attention to large loads, distributed energy resource (DER) aggregators (DERA), and electric vehicle supply equipment (EVSE) as their grid impact scales, as well as physical security risks

The CIP Roadmap emphasizes that improving grid security does not mean layering new compliance requirements indiscriminately. It calls for targeted, risk-driven evolution of the CIP standards, strengthening coverage where threats have outpaced current CIP scope, and leveraging guidance where flexibility is needed.

Ultimately, this effort reaffirms that reliability, resilience, and security are inseparable. The CIP Roadmap provides a blueprint for coordinated action between NERC, the Regional Entities, industry, and government partners to ensure that the CIP framework continues to evolve as an adaptable defense system capable of securing the North American grid through the next decade of transformation.

[4] 2023-09 Risk Management for Third-Party Cloud Services

Background

NERC's 2025 Work Plan Priorities[5] included a directive for NERC staff to "create a roadmap for ensuring CIP standards provide baseline protection for an evolving risk environment." To that end, NERC's Security Integration team began developing a risk-based methodology to assess the effectiveness of the NERC CIP standards in mitigating or reducing BPS risks to reliability both now and into the future.

Electric Reliability Organization (ERO) Enterprise

The team expanded its outreach to a broader group of subject matter experts across the ERO Enterprise. Representatives from all six Regional Entities contributed to the effort (see **Appendix C** for a full list of participants). Including the perspective of each Regional Entity was essential to developing recommendations that reflect the diversity of operational environments and challenges across the ERO Enterprise.

ERO Enterprise | Regional Entities
Nearly 400 million North American citizens depend on electricity in their daily lives. To pursue its mission of assuring the effective and efficient reduction of risks to the reliability and security of the BPS, the ERO Enterprise works with users, owners, and operators of BPS assets; government partners; and other stakeholders and industry participants.

Outreach

This work was conducted in coordination with Regional Entity subject matter experts and multiple NERC departments. Industry engagement was facilitated through the Reliability and Security Technical Committee (RSTC) and its subordinate groups: the Security Working Group (SWG), Supply Chain Subcommittee (SCS), and Security Integration and Technology Enablement Subcommittee (SITES). Additional subject matter expertise was gathered through an industry-wide risk survey and by soliciting targeted feedback on both the risk evaluation framework and proposed mitigations.

Process Inputs

NERC staff initiated the effort by developing a risk assessment methodology and compiling a registry of security risks facing the electric industry (see **Appendix A** and **Appendix B**). The assessment and resulting recommendations were informed by a wide range of inputs drawn from across the ERO Enterprise and the broader security community. These included NERC data sources such as alerts, internal analyses, NERC studies (e.g., *Internal Network Security Monitoring Feasibility Study Report*),[6] threat and incident intelligence from the Electricity Information Sharing and Analysis Center (E-ISAC), and publicly available advisories from organizations such as the Cybersecurity and Infrastructure Security Agency (CISA). The process also incorporated regulatory and policy materials, including FERC rulemakings, NOPRs, and final orders, as well as insights from the LICRT[7] and the *2025 ERO Reliability Risk Priorities Report* (RISC). Additional context was provided by technical papers and white papers from industry and government on emerging security threats and technologies relevant to the BPS.

Industry Updates

In addition to soliciting input and feedback from industry, the ERO Enterprise, and the various RSTC security groups, NERC staff provided periodic updates to the RSTC and industry through several means including the RSTC March, July, and September meetings; the joint security group meeting in September in Austin, Texas;[8] and a webinar in October.[9]

[5] NERC 2025 Work Plan Priorities
[6] https://nerc.com/FilingsOrders/us/NERC%20Filings%20to%20FERC%20DL/NERC%20INSM%20Feasibility%20Study%20Final%20Public.pdf
[7] https://www.nerc.com/globalassets/our-work/reports/white-papers/nerc_licrt_white_paper_clean.pdf
[8] https://www.nerc.com/globalassets/who-we-are/standing-committees/rstc/swg/joint-swg_sites_scs-meeting_september_9_agenda.pdf
[9] CIP Roadmap Webinar October 23 2025

Chapter 1: Process

Development of the CIP Roadmap was grounded in a risk-based approach designed to identify, assess, and prioritize security risks to the BPS while examining where the strongest opportunities exist to apply or enhance controls aimed at achieving the most comprehensive and effective mitigation across the body of risks. The team focused on building recommendations from an understanding of current threats, existing protections in the current applicable NERC CIP Reliability Standards, the ongoing body of regulatory activities (including guidelines development and NERC CIP Reliability Standards projects), and the practical realities of implementation across the industry.

The process began with creating a comprehensive security risk registry to identify, define, and comparatively rank the most credible risks to the BPS. Using that foundation, the team created a structured risk evaluation framework to assess each risk's likelihood and impact and the maturity of existing mitigations. Building on those results, the team analyzed where current NERC CIP Reliability Standards and related regulatory activities already provide coverage, where gaps remain, and where enhancements or new controls could most effectively reduce risk. This included reviewing complementary control frameworks, such as NIST SP 800-53, evaluating operational and architectural constraints within OT environments, and considering implementation feasibility across diverse entities. The outcomes were consolidated into a set of recommendations, including controls with the greatest potential to strengthen resilience across multiple risks and functions, providing a practical basis for the CIP Roadmap that follows.

Risk Registry

The first step in developing the CIP Roadmap was the creation of a comprehensive security risk registry to establish a common foundation for analysis. The registry was developed by NERC staff in collaboration with Regional Entity subject matter experts and informed by multiple sources, including NERC alerts, E-ISAC threat reporting, CISA advisories, and the 2025 RISC report. Input from across the ERO Enterprise ensured that the list reflected both ongoing and emerging risks facing the BPS, ranging from evolving threat vectors to technology, and asset-specific exposures such as distributed energy resource management systems (DERMS), EVSE, and Category 2 IBRs.

Each identified risk was defined and characterized. The team also developed hypothetical incident scenarios to illustrate credible pathways of compromise or failure and to support consistent interpretation across reviewers. To capture the full landscape of potential exposures, the registry incorporated risks at multiple tiers of detail, ranging from generalized threat vectors to discrete system and asset categories. Certain high-level systems and technologies were treated as distinct risk items because, while they may lie outside current CIP applicability, they maintain functional and operational interdependencies with the BPS. Evaluating these categories separately from traditional threats ensured that the registry reflected not only the risks explicitly governed by existing standards but also those that may affect reliability through upstream or cross-system interactions, despite possibly falling outside of CIP-002 scoping mechanisms or lacking relevant NERC registration of associated entities or assets. In this regard, during initial risk identification, the team's approach respected the idea that inherent risk exists without jurisdictional limits.

To validate and refine the registry, the team deployed an industry-wide survey in July 2025 titled "2025 Emerging Security Risks and CIP Standards Roadmap - Survey of Industry" and solicited targeted feedback from Regional Entity and industry subject matter experts. Respondents were asked to provide relative rankings of residual risk for the items in the draft list and propose any additional risks for consideration. Survey results closely matched the team's internal prioritization, and no materially new risk categories were identified, supporting the registry's scope. Respondent freeform comments also provided qualitative input on mitigation maturity, operational constraints, and sector acceptance that was incorporated into subsequent gap analysis and recommendation development. The close alignment between industry feedback and the original registry provided strong validation of its completeness and accuracy.

The survey consisted of 34 risks for participants' assessment and included a supplemental addendum (see Appendix A; **Supplemental**). The addendum provided a risk statement and hypothetical risk scenario(s) for each risk. The provided hypothetical risk scenario was only an example and was not meant to exclude other possible valid risk scenarios. Industry was asked to use these details to assist in completing the risk survey.

Following internal review of survey data, the risk registry was refined from the original set of roughly 34 risks to 22 risks for full assessment. Items removed generally represented a clear drop in relative risk compared to the remaining set, either due to robust existing mitigations within the NERC CIP Reliability Standards, low estimated likelihood or impact, or a consistent industry view that residual risk was already acceptable. For the internal NERC team, these items remain on the horizon for continued monitoring and future consideration as the threat and technology landscape evolves. The resulting registry formed the foundation for the subsequent risk evaluation and mitigation development stages of the CIP Roadmap effort.

Risk Evaluation Framework

The team designed and implemented an enterprise security risk evaluation framework to evaluate and prioritize the risks identified in the registry. The objective was to apply a consistent and transparent method for comparing diverse risk types, ranging from threat vectors to system or asset categories, while maintaining enough flexibility to accommodate varying data availability and quality, scope boundaries, and levels of abstraction. The framework sought to balance technical rigor with practical usability, ensuring results could directly inform actionable mitigation activities and NERC CIP Reliability Standards considerations.

The evaluation used a three-part model centered on likelihood, impact, and mitigation maturity. Each category contained a defined set of qualitative criteria and scoring rubrics designed to support consistent assessment across all risks (see Appendix B; **Methodology**). These criteria incorporated multiple factors, including observed threat activity, control coverage under existing NERC CIP Reliability Standards, the operational and architectural realities of the BPS, and relevant industry feedback. For mitigation scoring, a simplified control-based evaluation was used, considering control policy coverage, implementation maturity, and real-world efficacy. This structured approach provided a consistent analytical foundation for the subsequent development of targeted mitigation recommendations.

Residual risk scores were calculated by using a simple interpretive formula based on the relationship between likelihood and impact, with modifiers reflecting mitigation strength (see Appendix B; **Formula**). Criteria weighting and mitigation dampening were designed into the tool but were not found necessary to utilize. All criteria within their respective categories were weighed equally to preserve transparency and comparability.

The framework was then applied in a full-cycle assessment of every risk in the registry (see Appendix B; **Scoring**). Multiple scoring passes were performed by NERC staff, incorporating iterative feedback from Regional Entity subject matter experts and the same industry working groups engaged earlier in the process. After internal risk calculation, a final step included weighing the industry's relative ranking results from the risk survey to inform the comparative alignment of NERC's internal assessment results with industry's judgments.

Likelihood Criteria

The likelihood component assessed the plausibility of a given risk's scenario(s) based on threat behavior, exposure, and the degree of existing preventive control coverage. The evaluation considered factors such as the following:

- **Historical Precedent:** Documented or analogous incidents within the electric sector or comparable industries
- **Known Tactics, Techniques, and Procedures (TTP):** Use of known adversary behaviors, tools, or exploit patterns (e.g., as cataloged by MITRE ATT&CK or E-ISAC reporting)
- **Ease of Compromise:** Technical difficulty and resource requirements for a successful attack path

- **Exposure/Attack Surface:** The accessibility of systems, vendor pathways, or interdependencies that could enable exploitation

Each factor was scored on a standardized five-point scale to promote consistent comparison across diverse risk types.

Impact Criteria

The impact category measured the plausible operational consequences of a successful event, focusing strictly on reliability and grid stability outcomes. Factors included the following:

- **Scope of Impact:** The extent of operational disruption (localized, regional, or Interconnection-wide)
- **Maximum Severity of Impact:** Potential loss of control, visibility, or restoration capability
- **Coordination or Aggregation Potential:** Whether the risk could amplify through shared technologies, supply chains, or vendor ecosystems
- **Response and Recovery Preparedness:** Single-entity(s) and industry-wide readiness to detect, respond, and recover from the event

This assessment excluded financial or reputational effects to maintain focus on system reliability.

Mitigating Criteria

The mitigation evaluation measured how well existing technical and procedural controls reduce risk likelihood or impact. It incorporated the following:

- **CIP Integration:** Relevance and enforceability of existing CIP controls for each risk
- **Control Implementation (Maturity):** Observed adoption and consistency of relevant controls across industry
- **Control Efficacy:** Practical effectiveness of the implemented controls at preventing or limiting the event

Each criterion was assessed equally to avoid overemphasizing any single dimension and to maintain simplicity.

Constraints

While designed for consistency, the evaluation framework operates within several constraints. The analysis had to accommodate diverse risk paths, threat actor behaviors, and varying potential impact scopes across different risk categories. Several risks required abstract interpretation of rubrics, relying on professional judgment and domain expertise where quantitative data was unavailable.

The framework is a qualitative model at its core even though numerical scoring was used for structure. Consequently, resulting scores should be viewed less as precise rankings and more as categorical indicators of high, medium, or low relative risk.

Data limitations were also a factor. Objective data was often unavailable for high-bar criteria, particularly regarding control implementation maturity across industry, or the effectiveness of entity or sector-level incident response capabilities. Similarly, estimating the theoretical impact of rare or novel risks relied on analogous historical events or conservative assumptions. Despite these constraints, the framework provided a practical, evidence-informed structure for evaluating security risks to the BPS and prioritizing mitigation development.

Mitigation Development

Mitigation development began with a gap analysis against the existing NERC CIP Reliability Standards to evaluate both scope of applicability and the sufficiency of current control requirements in addressing the risks evaluated. This

analysis aimed to identify where effective mitigations were already present or not, where existing requirements could be enhanced or extended, and where entirely new control opportunities might be warranted.

External frameworks, such as NIST SP 800-53, NIST SP 800-82, and ISA/IEC 62443, were referenced to benchmark potential control options against established best practices and to ensure consistency with broader cybersecurity standards. Through this lens, the team identified opportunities to enhance existing CIP controls, extend their scope to better address emerging technologies and assets, and, in some cases, define new controls that could strengthen reliability through defense-in-depth within the NERC CIP Reliability Standards. This stage of work maintained a controls-first mindset, emphasizing open consideration of potential mitigations without prematurely narrowing options based on compliance boundaries, implementation challenges, or resource limitations. The intent was not to disregard those practical constraints but to ensure that they did not limit exploration of control opportunities.

The team first conducted this analysis on a risk-by-risk basis then consolidated the results into a comprehensive risk-to-control matrix (see **Table B.3: Risk-to-Control Mitigation Matrix**). This mapping enabled identification of two key insights: controls with the broadest mitigation benefit across multiple risks and individual risks that required specialized or unique mitigations.

Using these results, the team evaluated alignment with existing sector risk-prioritization efforts, such as the 2025 RISC report, and examined ongoing regulatory and standards development initiatives that will meaningfully reduce residual risk. These included FERC Order No. 912 and the resulting Supply Chain Risk SAR[10] as well as active projects led by Standards Drafting Teams 2023-09 (Risk Management for Third-Party Cloud Services)[11] and 2025-02 (Internal Network Security Monitoring Standard Revision).[12] The combination of analytical, regulatory, and industry inputs guided the development of the next phase of the CIP Roadmap, leading to the drafting of recommendations that are practical, grounded in shared priorities across the ERO Enterprise, and tempered by the cost-benefit realities of an industry operating with finite resources. The resulting recommendations are intended to enable continued collaboration to refine, validate, and advance prioritized security improvements to the NERC CIP Reliability Standards in a coordinated and transparent manner.

[10] https://www.nerc.com/globalassets/standards/projects/2025-06/informal-posting-1/2025-06-ferc-order-912-supply-chain-risk-management-sar_october2025.pdf
[11] Project 2023-09 Risk Management for Third-Party Cloud Services
[12] https://www.nerc.com/pa/Stand/Pages/Project202502InternalNetworkSecurityMonitoringStandardRevision.aspx

Chapter 2: Insights

The risk assessment, feedback reviews, internal deliberations, and analysis led to a number of key insights that are presented below and drove the team's final recommendations. These findings illustrate how the grid's security landscape is shifting and where targeted, collaborative action can most effectively reduce emerging risks.

Evolving Grid

The majority of the defense-in-depth protections in the NERC CIP Reliability Standards, particularly those associated with medium- and high-impact BCS, now cover a smaller share of grid assets than they did a decade ago, and that share continues to shrink. Most OT deployed across the BPS falls into low-impact or sub-BES categories.[13] The LICRT report[14] effectively highlighted how coordinated attacks on multiple low-impact assets could aggregate to a negative BPS impact, a concern echoed by FERC in its NOPR[15] for CIP-003-11,[16] which noted that-low impact BCS may introduce reliability risks of a higher impact when distributed low-impact BCS are subjected to a coordinated cyber attack. Recent NERC data collections, including the NERC Rules of Procedure Section 800 data request *Access to Bulk Power System Elements*[17] and the Level 2 NERC Alert *Cross Border Remote Access to BPS Elements*[18] as well as the *Internal Network Security Monitoring Feasibility Study*,[19] evidenced that a large portion of generation assets on the grid today, and perhaps nearly all new generation resources coming on-line, possess remote access capabilities both internally and through non-registered third parties that provide operational support through control, maintenance, or monitoring. Large loads, DERAs, and EVSE similarly represent growing vectors of BPS risk exposure that remain outside the enforceable minimum-security baselines of NERC CIP Reliability Standards at present. Furthermore, advanced persistent threat (APT) actor campaigns like Salt Typhoon[20] reveal the risk of the electric sector's reliance on leased or third-party telecommunications networks (e.g., carrier-provided fiber, copper, or cellular WAN circuits). These telecommunications networks are used to facilitate SCADA communications and fall outside the confidentiality and integrity protections required by CIP-012, which apply exclusively to control-center-to-control-center communication links. Rather than a doomsday signal, these realities illustrate an evolving grid where security risks constantly threaten to outpace current NERC CIP Reliability Standards, challenging industry to action.

Finally, cloud-native security solutions can offer enhanced visibility, detection, correlation, analytics, and responsiveness to help security teams reduce the potential impacts of security events and speed up recovery time. Additionally, cloud solutions can offer increased resiliency, scalability, high availability, and redundancy. The growing adoption of cloud-based systems designed to support grid operations is being seen predominantly in the spaces of big data analysis, AI, security tooling, IBR control systems, and distribution grid technologies. The application of cloud-based solutions also presents inherent challenges related to shared security responsibility between entities and cloud services providers; therefore, a measured regulatory solution should be risk-based and ensure that fundamental security objectives are met.

Multi-Factor Authentication (MFA)

MFA remains one of the most effective and broadly applicable defenses against unauthorized access, and consistent application was identified as a control that directly reduces both the likelihood and potential impact of compromise across many of the evaluated risks, particularly when attack paths involve credential theft, remote access abuse, or lateral movement through shared accounts. MFA especially serves as one of the single greatest mitigating controls for cyber risk presented by the growing trend of utilities enabling remote access to electric grid facilities, where such

[13] https://nerc.com/FilingsOrders/us/NERC%20Filings%20to%20FERC%20DL/NERC%20INSM%20Feasibility%20Study%20Final%20Public.pdf
[14] https://www.nerc.com/globalassets/our-work/reports/white-papers/nerc_licrt_white_paper_clean.pdf
[15] Notice of Proposed Rulemaking for Reliability Standard CIP-003-11 (Docket No. RM25-8-000, 89 Fed. Reg. 66752, Sept. 23, 2025)
[16] Project 2023-04 modifications to CIP-003-11 are pending FERC action and will address concerns highlighted in the LICRT study.
[17] https://www.nerc.com/comm/RSTC/Documents/section_800_request-grid_security_US_20231108_final.pdf
[18] https://www.nerc.com/programs/bulk-power-system-awareness/alerts/2025
[19] Internal Network Security Monitoring Feasibility Study Report, Docket No. RM22-3-000
[20] https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-239a

remote access may serve any operational use cases, be utilized internally or by a third party, and may be initiated domestically or internationally.

The latest revisions to requirements for low-impact BCS under CIP-003 present MFA as a suggested control measure for low-impact systems but stop short of making it an enforceable requirement. Given the continued and increasing usage of remote access across generation, transmission, and control center networks, the case for expanding MFA requirements strongly merits consideration. While entities have implemented MFA for interactive remote access to high- and medium-impact BCS under CIP-005-7, a significant volume of remote sessions supporting low-impact or sub-BES assets remain outside that minimum control baseline. In many such cases, especially where the remote access solutions are managed by a non-registered third-party operator or original equipment manufacturer (OEM) for some measure of key operational function, MFA is not present.

The value of MFA also extends beyond remote access. Applying strong authentication to *any* interactive access of privileged or administrative accounts can substantially limit the effectiveness of credential reuse, insider misuse, or unauthorized privilege escalation. In practice, MFA introduces friction at the precise points where adversaries attempt to transition from initial access to control, whether that access originates externally or from within a trusted network. Although this use case is not yet reflected in current CIP requirements, it aligns with established security practices across the broader cybersecurity community and is increasingly adopted among the more mature and risk-adverse entities in the electric sector.

Not all OT environments can technically or safely integrate MFA with existing access methods, particularly for legacy systems or during emergency operations. However, those constraints should not preclude defining MFA as a target baseline for all interactive access where it is technically feasible and operationally safe to deploy.

Foundational Cyber Hygiene

Across the risk assessment community, one consistent theme emerged: The strongest mitigations against nearly every major cyber risk facing the BPS stem from consistent implementation of foundational cyber hygiene controls. Effective security operations (SecOps) depend on these fundamentals. Without accurate asset inventories, defensible network topologies, and configuration management, even basic SecOps monitoring and response efforts may become unreliable and potentially operationally intrusive. The challenge is amplified as entities deploy advanced detection technologies such as INSM. Without a clear understanding of what assets and traffic should exist within an environment to fine-tune such tools, these systems may generate high volumes of ambiguous alerts that are difficult to triage and validate. This increases analyst workload, heightens the risk of overlooking subtle adversary activity such as “living off the land” techniques, and can lead to hesitation or error when response actions carry potential negative operational consequences.

Where minimally mandated requirements are absent for foundational cyber hygiene controls, such controls may be implemented inconsistently (e.g., such as across low-impact or sub-BES systems), potentially leaving systemic weaknesses that adversaries can exploit as entry points for malicious compromise. Core practices such as information protection, identity and access management, asset management, incident response, and network architecture documentation represent critical foundations of effective defense-in-depth. Knowing what assets exist, how they communicate, and who can access them remains the prerequisite for nearly all higher-order administrative, policy, or technical controls, which is true for both IT and OT networks. Likewise, disciplined vulnerability and patch management, coupled with processes for tracking and handling usage of end-of-life technologies and insecure or legacy protocols, materially reduces both the likelihood and impact of compromise across the spectrum of security risks, even when actionable mitigation must rely on compensating controls. Much of the residual risk in these areas arises not from deliberate inaction or risk acceptance but from limited visibility into where outdated or vulnerable technologies remain in use.

While the NERC CIP Reliability Standards establish more comprehensive requirements for high- and medium-impact systems, many of the foundational cyber hygiene controls identified in this assessment remain outside the current requirements for low-impact assets, even with the forthcoming CIP-003-11 revisions. This results in uneven layers of protection across environments, where controls beyond those explicitly required by CIP remain at the discretion of the registered entity. As a result, a portion of the BPS's residual cyber risk depends on how consistently entities choose to apply protections that exceed the minimum required in the CIP-003 standard. Therefore, the focus should be on working collaboratively with industry to narrow these gaps through continued, practical improvement of the CIP standards, ensuring their effectiveness as a framework for minimum security baselines that ensure the security of the BPS.

Unencrypted Public Network Usage

This risk stands apart from the broader category of foundational cyber hygiene. Even with strong asset management, access control, and monitoring in place, the inherent exposure of relying on external telecommunications networks for critical OT traffic cannot be fully mitigated without targeted controls. CISA[21] warns of the compromise of major global telecommunication networks through campaigns such as Salt Typhoon and encourages industries, including the electric industry, to apply key mitigations such as end-to-end network encryption to protect critical infrastructure reliant on these networks. Electric utilities may rely on leased or third-party network circuits for SCADA and AGC communications, such as carrier-provided fiber, copper, cellular links, or dedicated internet protocol/multiprotocol label switching circuits provisioned and operated by telecommunications providers. Even when such circuits are operated on a private or contractually dedicated basis, they still traverse carrier infrastructure that remains outside utility control, introducing risk. As previously noted, this risk exposure has been highlighted by ongoing APT campaigns targeting global telecommunications infrastructure. Use of these networks with critical but non-real-time OT data (e.g., data with timing requirements greater than roughly one second) is still particularly sensitive because standard protocols used in SCADA and AGC communications, such as DNP3, Modbus, ICCP, IEC 60870-5 (i.e., 101,103,104), OPC Classic, and other legacy or proprietary protocols, often lack native encryption capabilities, data integrity checks, or replay attack protections.

In typical SCADA use cases routed over these internet service providers' (ISP) contracted or leased networks—where remote terminal unit (RTU) data is polled and aggregated rather than used for time-critical protection functions—these protocols can tolerate moderate latency or retransmissions between the facility and its upstream control center. AGC signals, while somewhat more latency-sensitive, are frequently transmitted over the same communication paths and share similar exposure when unencrypted. This makes the use of encryption or tunneling technically feasible for both SCADA and AGC traffic, though the prevalence of such protections remains uncertain in practice, partly due to the common presumption of privacy within ISP-contracted communication circuits.

Because the security of contracted, carrier-provided telecommunications infrastructure lies largely outside a utility's control, and the Salt Typhoon campaign has demonstrated that telecommunications infrastructure is a target, assuming that carriers will safeguard confidentiality and integrity is not a reliable defense approach. Industry should regard all externally provided circuits as untrusted and apply encryption, segmentation, and monitoring accordingly where technical limitations can be overcome. The current CIP-012-1 standard provides confidentiality and integrity protection only for control-center-to-control-center communications, leaving facility-to-control-center and AGC traffic unaddressed. Expanding those protections to include any external or carrier-dependent links would close one of the most persistent risk exposures to the BPS.

[21] Enhanced Visibility and Hardening Guidance for Communications Infrastructure | CISA

Chapter 3: CIP Roadmap Recommendations

The NERC CIP Reliability Standards continue to serve industry well. An important feature of the standards is that they are not static and have continually evolved, including through monumental shifts such as the version 5 transition and the pending updates for virtualization technologies.[22] Efforts are underway to position the standards to allow for the adoption of cloud-native technologies.[23] In positioning cyber-physical defenses in a way that keeps pace with the changing threats and vulnerabilities that the electric grid faces, a point-in-time analysis of the effectiveness of the CIP standards is periodically necessary. The recommendations below contain action items, next steps, and proposals for further actions and, where applicable, specify the organization(s) or entities that should own the risk mitigation recommendations. Considering the various inputs, timelines, procedures, and constraints that surround these activities, we have elected to specify a timeline that is less specific than identifying weeks, months, or years and rather chosen to specify an order of operations using the labels Near Term and Intermediate Term. These terms are not meant to be vague but rather to provide flexibility and the time needed to complete such recommendations.

Reliability Standards Modifications and Assessment Recommendations

- **(Near Term) NERC-Led Industry Team:** Develop a SAR to establish use of MFA for interactive remote access to low-impact BCS.
- **(Near Term) RSTC Workplan:** 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.
- **(Near Term) NERC:** Raise the Reliability Standards project 2023-09 Risk Management for Third-Party Cloud Services[24] from a medium priority to a high priority.
- **(Intermediate Term) NERC-Led Industry Team:** Evaluate residual risk associated with minimum defense-in-depth achieved through foundational controls (i.e., cyber hygiene) across all BPS cyber systems to inform potential CIP applicability updates, especially low-impact BCS. Focus areas for consideration 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 Industry Team:** Expand upon NERC compliance assurance efforts assessing BPS risk of Category 2 IBRs by performing a focused risk assessment and control evaluation for cybersecurity risk of Category 2 IBRs to determine necessary cybersecurity control minimums and potential updates to NERC CIP Reliability Standards.

Guidance and Other Recommendations

- **Supply Chain Subcommittee (SCS):** Develop (or modify existing) guidance for validating vendor responses using a risk-based evaluation of supplier security assurances and attestation materials.

[22] 2016-02 Modifications to CIP Standards
[23] Project 2023-09 Risk Management for Third-Party Cloud Services
[24] 2023-09 Risk Management for Third-Party Cloud Services

- **RSTC Workplan:** Develop guidance to promote corporate-level email security controls (e.g., phishing resilience) best practices adoption across ERO-registered entities.
- **RSTC Workplan:** Develop guidance to promote remote access best practices adoption across ERO-registered entities.
- **RSTC Workplan:** Develop guidance around improving cybersecurity incident response plans and associated playbooks, including multi-entity coordinated response efforts for large-scale cyber events affecting BPS operations.
- **RSTC Workplan:** Following the completion and acceptance of standards changes produced by the 2023-09 SDT, develop implementation guidance around use of cloud-service providers by registered entities.

ERO Enterprise Risk Monitoring

- The E-ISAC, through the Physical Security Advisory Group (PSAG), should continue monitoring emerging physical security trends and their effects on BPS operations and recommend a course of action given relevant changes in the threat landscape.
- Continue monitoring emerging cyber risks associated with large loads and their growing integration into BPS operations.
- Maintain assessment and situational awareness of DERAs and their aggregate impact on reliability and security.
- Track developments in EVSE integration and evaluate potential reliability and cybersecurity implications as deployment scales.

Appendix A: Industry Risk Survey

This section includes materials used for NERC's 2025 Industry Security Risks Survey.

Announcement

The announcement below was sent out industry-wide in July 2025.

Table A.1: NERC Announcement

NERC Announcement

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

On December 10, 2024, NERC's Board of Directors approved NERC's 2025 Work Plan Priorities, which includes a work plan priority to create a roadmap for ensuring the NERC Critical Infrastructure Protection (CIP) Standards continue to provide an effective baseline of cyber and physical security risk management in defense of the bulk power system (BPS) amidst an evolving risk environment.

In support of this objective, the ERO Enterprise is conducting a survey of industry to help identify and rank the top emerging security risks facing our industry.

Survey respondents are asked to rank the listed security risks from highest to lowest priority based on their likelihood and potential impact on BPS reliability. In addition, respondents may identify any additional high-priority security risks that may not be represented.

The ERO Enterprise will assess responses from the survey participants and use the collected insights in further developing the CIP Roadmap for the 2025 NERC Work Plan Priority.

A subsequent report will provide an overview of the identified and prioritized emerging security risks to the reliability and security of the BPS, a review of current applicable NERC CIP Standards, an analysis of ongoing risk mitigation activities associated with each priority risk and provide recommendations for a CIP Roadmap to address identified gaps.

The deadline for completing the survey is July 22, 2025. Your input is crucial in shaping the future of BPS reliability and security risk management.

2025 Emerging Risks and NERC CIP Roadmap - Survey of Industry

2025 Emerging Security Risks Survey Supplemental Information (security risk descriptions and hypothetical examples)

For more information or assistance, please contact please contact Security Team (via email).

Supplemental

The below list of risks (not ranked or in any particular order) was provided to industry as a supplemental data sheet to accompany the risks that they were asked to rank. The security risks were accompanied by a risk statement and hypothetical risk scenario(s). The provided hypothetical risk scenario is only one example and was not meant to exclude other possible valid risk scenarios. Industry was asked to use these details to assist in completing the risk survey "2025 Emerging Security Risks and CIP Standards Roadmap - Survey of Industry" in July 2025. This supplemental information was provided for completeness. It also represented the effective first draft of the team's risk registry.

Table A.2: 2025 Emerging Security Risks

Risk Name	Risk Statement	Hypothetical Risk Scenario(s)
Supply Chain	Advanced Persistent Threat Actors (APTs) or cybercriminals could counterfeit or insert back-doored components into bulk-power system equipment, compromise software applications or software update channels, potentially compromising Confidentiality, Integrity, Availability (CIA) of Bulk Power System (BPS) elements resulting in widespread impacts to the grid.	Scenario 1) A manufacturer country embeds rogue hardware in replacement relays or other critical electric grid equipment; once installed, a remotely accessible backdoor allows an adversary to disable trips during a July heatwave, causing cascading outages across a reliability coordinator's footprint. Scenario 2) SolarWinds-style compromise inserts malware into Energy Management System (EMS) or component patch; The signed update spreads and the adversary then pivots into Operational Technology (OT) environments eventually coordinating an attack in conjunction with extreme weather events or with war time actions., SolarWinds-style compromise inserts malware into EMS; the signed update spreads and the adversary then pivots into OT environments eventually coordinating an attack in conjunction with extreme weather events or with war time actions.
Ransomware / Malware	Adversary malware infects Information Technology (IT) and OT systems by encrypting or simply wiping data.	Ransomware variant crosses IT-OT boundary through overly permissive firewall rules and encrypts several entity OT devices. A ransomware note is displayed on impacted Human Machine Interfaces (HMI).
Insufficient Low Impact Security	Low impact security controls mandated by NERC CIP standards may be insufficient to protect against emerging threats.	Grid assets without Multifactor Authentication (MFA) in place are compromised via valid account credential reuse after being stolen through a phishing campaign allowing an attacker to install a keylogger on an engineering workstation.

Table A.2: 2025 Emerging Security Risks		
Risk Name	**Risk Statement**	**Hypothetical Risk Scenario(s)**
Cloud Environment Compromise	OT/IT workloads in public clouds can expose entities to security misconfigurations and attacks arising from shared-tenant environments leading to data loss or unavailability of necessary critical workloads.	Misconfigurations of identity and access management (IAM) policies in a cloud service provider (CSP) allows an attacker to spawn virtual machines (VM) inside an Operational Technology (OT) virtual network (vNet), exfiltrate critical system data, and then execute a Distributed Denial of Service (DDoS) attack against a widely used distributed energy resource (DER)-control application programming interface (API) tripping offline 1500 MW solar.
Compromise of Category 2 Generator Owner (GO) and Generator Operator (GOP) Inverter-Based Resource (IBR) facilities	Cyber compromises targeting sub-BES facilities (i.e., falling below NERC CIP Reliability Standards applicability) constitute risk to grid reliability as coordinated attacks on CAT 2 GO / GOP could negatively impact grid operations.	Poorly secured IBR facilities could be attacked in a coordinated manner staged from one facility to another through a flat stretched network penetrating unpatched firewalls leading to attackers shutting down inverters or maliciously manipulating frequency and voltage signals.
Insider Threats	Intentional - Maliciously motivated employees illegitimately exploit privileged access or knowledge to IT or OT data, systems, or networks resulting in negative operational impacts or data exfiltration. Negligence – Exposes an organization to a threat through carelessness. Negligent insiders are generally familiar with security and/or IT policies but choose to ignore them, creating risk for the organization. (DHS) Accidental – Mistakenly causes an unintended risk to an organization (DHS).	Example of an “intentional” insider threat includes a disgruntled contractor uploads malware containing a logic bomb to several programmable logic controllers (PLC) across a Transmission Operator footprint. A timed failure of many devices during peak summer demand forces emergency load shed. Examples of a “negligent” insider threat includes allowing someone to “piggyback” through a secure entrance point, misplacing or losing a portable storage device containing sensitive information and ignoring messages to install new updates and security patches. Examples of an “accidental” insider threat includes mistyping an email address and accidentally sending a sensitive business document to a competitor, unknowingly or inadvertently clicking on a hyperlink, opening an attachment in a phishing email that contains a virus, or improperly disposing of sensitive

Table A.2: 2025 Emerging Security Risks		
Risk Name	**Risk Statement**	**Hypothetical Risk Scenario(s)**
		documents.
End-of-Life Systems	Aging and vendor unsupported operating systems, software, and / or hardware devices remain unpatched in OT environments.	A malware worm exploiting a vulnerable or overly promiscuous server message block (SMB) protocol firewall rule on an outdated Microsoft Windows HMI spreads to primary and backup Supervisory Control and Data Acquisition (SCADA) servers; operators lose control and visibility leading to outages.
Network Based Attacks	Low skill distributed denial of service (DDoS) cyberattacks are increasing and placing reliable operations of the grid at risk.	A DDoS attack disables both primary and back-up Control Center communications that utilize public networks causing a loss of visibility for a large generation company interrupting grid operations for several hours.
Insecure Protocols	Insecure legacy protocols without native security features create vulnerabilities that could lead to cyber compromise that negatively impact grid operations.	A threat actor takes advantage of the insecure distributed network protocol 3 (DNP3) protocol used in the electric grid, which lacks security protections, performs a man-in-the-middle attack, and is able to intercept valid signals and send malicious commands to disable remote terminal units (RTU) in the field.
Phishing & Social Engineering	Deceptive tactics allow harvesting of legitimate account credentials or bypassing physical security controls.	Spoofed vendor email entices a technician to download malicious files which install a Remote Access Trojan (RAT) on a substation HMI.
Insufficient Cybersecurity Workforce	A lack of qualified personnel could make energy sector entities vulnerable to increasingly sophisticated cyberattacks, which may include ransomware, phishing, and malware.	Grid Asset Owners and Operators (AOO) across the industry are unable to appropriately staff their OT security teams as they compete for talent with other industries, leading to a less secure system state.
Physical Attacks on Infrastructure	Theft, ballistic damage, vandalism, and intrusion (tampering) all pose physical security risks to grid assets which could impact reliability. The current challenges around the manufacture of transformers or similar equipment in a timely manner and resulting supply shortages could aggravate risk by inhibiting system restoration from a natural disaster or man-made attack. The long lead times, combined with	Scenario 1) A Metcalf style coordinated ballistic attack damages several transformers causing distribution-wide outages lasting for several hours. Scenario 2) Vandals cut fiber optic cables (unknown intentional or purely criminal) causing generation unavailability and customer outages. Scenario 3) A spike in copper prices

Table A.2: 2025 Emerging Security Risks		
Risk Name	**Risk Statement**	**Hypothetical Risk Scenario(s)**
	limited domestic production, increased load growth, and manufacturing capability, could all impact reliability.	motivates thieves to steal grounding from a substation causing customer outages.
Weaponization of Drones	Physical security attacks facilitated by drones, which could be equipped with explosives could cause disruptions to reliability.	An anarchist group equips several drones with homemade explosives and blows up several large transformers along with other equipment at several substations simultaneously causing regional outages.
Large Load Manipulation	Malicious manipulation of large loads could destabilize the grid.	Scenario 1) Control systems such as Building Management Systems (BMS), Heating, Ventilation, and Air Conditioning (HVAC), or other support systems are compromised which leads to a forced load drop at a data center. Scenario 2) A botnet infects a 100 MW crypto mining farm rapidly toggling miners, causing oscillations that trip a collocated gas plant and cause an outage.
Exploitation of Public Telecommunications	Nation-states compromise telecommunications entities allowing traffic associated with electric grid operators' infrastructure to be intercepted, modified, exfiltrated, or otherwise disrupted.	An adversary compromises internet backbone routers, intercepts traffic (all types, encrypted, unencrypted, or poorly encrypted), exfiltrates data associated with grid operations preparing for a larger future attack and executes a Distributed Denial of Service (DDoS) attack against the internet service provider (ISP) causing grid disruptions across an RC footprint.
Targeting of DER Aggregator (DERA) Control Systems	The cyber compromise of cloud-based DERA management platform via any attack method could enable manipulation of sizable DER generation or manipulation of demand response programs that could result in grid impacts.	A DERA cloud control system is compromised; Malicious control signals are sent to thousands of inverters which causes frequency oscillations triggering a load-shed event or load manipulation signals are sent to demand response program participants causing enrolled smart devices to increase load during demand response events.
Electric Vehicle Supply Equipment (EVSE)	Networked electric vehicle chargers and their physically unsecure nature creates new grid-edge attack surfaces.	Attackers exploit a Linux kernel vulnerability and eventually infect one thousand public charging stations with a Botnet. After using these stations for other malicious intentions, the Botnet owners send commands simultaneously to all the stations to exceed their

Table A.2: 2025 Emerging Security Risks		
Risk Name	**Risk Statement**	**Hypothetical Risk Scenario(s)**
		kilowatt draw thresholds. This causes feeders to overload, protective relays trip, and local instability occurs. (Scenario would require vehicles to be attached)
Unregistered 3rd-Party Operators	Non-NERC registered entities (operating within or outside of the United States) with remote access to generation facilities for monitoring, maintenance, or control capabilities could be targeted via cyber-attacks leading to risk to the grid.	Scenario 1) A breach at a wind generator OEM enables an attacker with remote access capability to US grid assets to push a malicious firmware update to multiple wind generators allowing for a future grid impacting attack to take place.
Ineffective Incident Response & Recovery Planning	Disjointed, out of date, or untested Incident Response Plan (IRP) playbooks delay containment, inhibit recovery, and allow attackers to erase forensic attack data.	Simultaneous substation shootings and a DDoS attack on an ISP effects SCADA communications and takes 8 hours to coordinate the response, prolonging local blackouts.
Targeting of Artificial Intelligence (AI) Tools and Capabilities	Targeting of AI through maliciously poisoned AI training inputs may destabilize grid operations for early adopters of AI technologies.	A poisoned dataset causes autonomous voltage monitoring systems to oscillate tap changers in several transformers causing instability and unplanned load shedding.
Regulatory Lag	Regulations inherently lag behind innovation and this uncertainty may delay or influence the adoption of new security technology that could improve defenses.	A large utility cancels a cloud enabled security solution while awaiting guidance in connection with NERC CIP Reliability Standards; An APT compromise a large entity and dwells in the networks for over 200 days undetected, triggering a timed load-loss event in a peak-demand scenario.
Compromised Application Programming Interface Keys	Insecure or leaked entity API security keys enable unauthorized access and data theft.	An entity's software developer accidentally posts API security keys to GitHub; An attacker obtains the API security key from the public repository and compromises the entity's CSP tenant allowing an attack that shuts down a 50 MW battery installation.
Compromise of Smart Distribution Switches	Smart distribution switches compromised through other interconnected systems allow attackers to disrupt power at the distribution level.	An Advanced Distribution Management System (ADMS) Software as a Service (SaaS) integration is compromised allowing an attacker to manipulate load causing a total loss of monitoring and control in a distribution provider (DP) footprint.
Compromise of Metering Infrastructure	Compromise of advanced distribution infrastructure such as Advanced	A successful phishing campaign targets a customer service agent working from

Table A.2: 2025 Emerging Security Risks		
Risk Name	**Risk Statement**	**Hypothetical Risk Scenario(s)**
	Metering Infrastructure (AMI) or metering integrated Customer Information Systems (CIS) potentially degrades operations and allows pivoting into OT systems.	home and steals credentials for logging into a SaaS CIS solution. The attacker remotely disables meters for several major industrial customers leading to voltage and frequency deviations at the Transmission & Distribution (T&D) interface.
Compromise of Synchrophasor Systems and Data Used in Real-time Operations	Manipulated Phasor Measurement Unit (PMU) data misleads a state estimator causing unsafe system conditions.	An unprotected Transmission Operator (TOP) PMU system is compromised, and the PMU data is spoofed sending incorrect Global Positioning System (GPS) timestamps; The RC's state estimator that receives the TOP PMU data miscalculates phase angles which triggers unwarranted remedial-action schemes.
Compromise of Blackstart Resources	Insufficiently secured blackstart restoration assets could be compromised and contribute to prolonged outages.	An attacker misconfigures generation remote start settings and tampers with diesel fuel sensors and logging; post-hurricane blackstart operations are delayed for hours.
Compromise of Power-Line Communication	Adversaries may exploit vulnerabilities in PLC systems used to communicate between substations leading to unauthorized access, disruption of protection schemes, or manipulation of substation controls systems resulting in grid instability or widespread outages.	An APT gains access to a poorly secured PLC endpoint via a compromised substation. Using this access the attacker injects false relay commands over PLC link triggering malicious breaker operations resulting in cascading faults and a blackout.
Insecure Usage of Protocol Converters	Converters used to bridge IT or OT networks expose insecure legacy devices without built in security features.	A critical OT network is bridged with an IT network using a serial to IP protocol converter. Lack of consideration of securing the created network bridge allows an attacker to maliciously communicate with downstream OT devices and alter relay settings degrading system resiliency.
Compromise of Mobile Devices	Vulnerable mobile devices utilized for various purposes (e.g., MFA, mobile badges, email, cloud services (O365), logs & alerts, etc.) could be leveraged to facilitate an attack.	A stolen phone, or e-SIM hijacked device, allows attackers to bypass MFA controls, or bypass Physical Security Perimeter controls via a mobile badge.
Unusable Backups	Asset owner(s) could be unable to operate for extended duration after a successful cyber or physical attack.	Malware encrypts mission critical servers at a Control Center. Backups are unavailable, out of date, or otherwise unusable.
Compromise of Market Systems	Manipulation of Independent System Operator (ISO) / Regional Transmission	API exploit alters bid data, causing ISO to mis-dispatch units; imbalance forces

Table A.2: 2025 Emerging Security Risks		
Risk Name	**Risk Statement**	**Hypothetical Risk Scenario(s)**
	Organization (RTO) energy market systems, data, bids, or awards disrupting dispatch orders leading to grid instability.	rolling blackouts and price spikes.
Quantum Computing	Advancements in quantum computing technology could break modern cryptography which underpins internet communications today allowing adversaries to compromise CIA.	Chinese APTs hack into telecom giants allowing them to steal large amounts of encrypted data which is then unencrypted offline using quantum compute.
Stolen Critical Energy Infrastructure Information or BES Cyber System Information	Exfiltration of communication network architecture, one-line diagrams and model data enabling more precisely targeted attacks.	Spear phishing the lead engineer at an RC allows an attacker to steal one-line drawings and modeling data; months later ballistic attacks target critical buses and infrastructure identified in the stolen data.
Compromise of Geographical Information Systems (GIS)	Compromise of GIS or Outage Management System (OMS) data and integrations could potentially inhibit system recovery after an incident (cyber or extreme weather) and degrade system operators' ability to recover.	A hacker exploits an unpatched vulnerability that allows access into the distribution provider corporate network. Poisoned data in these systems degrades the DP ability to recover from extreme events.

Appendix B: Process Documentation

This appendix includes some of the documentation produced across the NERC team's effort to deliver recommendations for the CIP Roadmap, including materials produced in the process of risk registry development, formation of a risk evaluation framework, final risk assessment scoring, and mitigation considerations.

Methodology

The table below describes the criteria that were evaluated for each identified risk along with a definition, factors, and a rubric for each. The table is divided into Likelihood and Impact, and each has a list of attributes that contribute to a higher risk score as well as a set of criteria that reduce the risk score. In the Likelihood Criteria category, "CIP Integration – Likelihood," "Control Efficacy – Likelihood," and "Control Implementation – Likelihood" are the mitigating factors for any risk being evaluated. In the Impact Criteria category, "CIP Integration – Impact," "Control Implementation – Impact," "Controls Efficacy – Impact," and "Response and Recovery Preparedness" are the mitigating factors for any risk being evaluated. These seven attributes lower the risk ranking in an inverse fashion as compared to the other attribute in the Likelihood and Impact categories. This documentation is being provided for completeness.

Table B.1: Identified Risk Criteria

Likelihood Criteria	Definition	Factors	Rubric
Historical Precedent	Measures the frequency and severity of documented past events similar to the risk under evaluation, including both direct incidents within the electric sector and relevant analogs from other critical infrastructure sectors.	• Documented past security events within the electric sector, the frequency of similar incidents over the last 10+ years and whether these incidents were regional or national in scope • Severity and operational impact of past incidents • Relevant sector analogs such as those affecting water utilities or gas pipelines • Incidents from non-analog sectors that may still offer insights into potential vulnerabilities or threat trends	**Very High (5):** Multiple well-documented, high-severity incidents within the electric sector in the past 10 years. Includes recent incidents with significant impact or repeat occurrences. **High (4):** One or more significant incidents within the electric sector, or multiple relevant analogs (e.g., pipelines, water utilities) with high similarity and operational impact in the past 10 years. **Moderate (3):** At least one documented incident or multiple lower-impact incidents in analog sectors in the past 10 years. Some evidence of recurrence, but not widespread. **Low (2):** Only indirect precedent, such as isolated, lower-impact incidents in non-analog sectors. No substantial

Table B.1: Identified Risk Criteria			
Likelihood Criteria	**Definition**	**Factors**	**Rubric**
			incidents in the electric sector. **Very Low (1):** No known precedent or meaningful analogs. Risk is speculative or highly novel.
Known Tactics, Techniques, and Procedures (TTP)	Assesses whether TTPs associated with this risk are known, documented, and actively used by plausible threat actors targeting the grid or similar infrastructure.	• Public or classified threat intel (e.g., MITRE ATT&CK, E-ISAC, CISA). Observed nation-state or criminal actor behavior • Maturity and prevalence of tooling (e.g., malware kits, industrial control system (ICS)-specific payloads) • Mapping of threat to adversary capability (Are they known to do this?) • Attribution confidence and alignment with grid-specific targets	**Very High (5):** TTPs are actively used by multiple threat groups targeting the electric sector. Well-documented in ICS/OT-specific advisories (e.g. MITRE ATT&CK, E-ISAC, CISA) with high confidence of applicability. **High (4):** TTPs are known, mapped to real-world campaigns against industrial or electric sector targets, and align with plausible threat actors' capabilities. Some electric sector-specific application. **Moderate (3):** TTPs are documented in open-source threat intel, but with less frequent targeting of the electric sector. May involve general-purpose tools adapted to ICS/OT. **Low (2):** Techniques are technically feasible but not commonly observed in the wild. Limited or no known use against relevant infrastructure. **Very Low (1):** TTPs are hypothetical or academic. No known use in real-world operations by plausible threat actors.
Ease of Compromise	Reflects the technical and operational difficulty an adversary would face in	• Technical and operational difficulty of achieving a successful compromise -	**Very High (5)**: Straightforward compromise path with

Table B.1: Identified Risk Criteria			
Likelihood Criteria	**Definition**	**Factors**	**Rubric**
	compromising the system or asset. Considers exploit availability, complexity of access, skill requirements, and internal dependencies.	i.e., difficulty for attacker to achieve their goal • Complexity of attack path (e.g., multi-hop, insider requirement, vulnerability chaining) • Availability of public exploits or zero-days • Degree of system design diversity (simplifies or complicates attacks) • Required skill level of attacker (e.g., script kiddie vs state actor) • Visibility of system design flaws or misconfigurations. • Insider threat risk or human error likelihood • Dependency on privileged access (e.g., insider threat, supply chain, administrative credentials)	minimal skill required. Publicly available exploits or default configurations. No specialized access needed. **High (4)**: Known attack paths exist and are moderately complex. Exploits may be semi-public or require mid-level expertise. May involve common misconfigurations or weak segmentation. **Moderate (3)**: Attack path is feasible but requires advanced skill or tool development. May require specific knowledge of system architecture or elevated access. **Low (2)**: Complex, multi-step compromise requiring insider knowledge, privileged access, or significant lateral movement. **Very Low (1)**: Highly constrained. May require insider access, multiple preconditions, or attack chains that are unlikely to succeed.
Exposure / Attack Surface	Assesses the degree to which the system or entity is exposed to external access or attack, either directly (e.g., internet-facing systems) or through interdependencies (e.g., supply chain, third parties, shared infrastructure).	• Number and type of internet-exposed endpoints • Third-party/vendor integrations (e.g., supply chain, cloud services, OEMs) • Geographic and jurisdictional spread (impacts coordination and defense)	**Very High (5)**: High volume of internet-exposed or remotely accessible systems. Multiple third-party integrations. Weak or absent network segmentation. High technological diversity. **High (4)**: Some direct exposure plus known interdependencies (e.g.,

Table B.1: Identified Risk Criteria			
Likelihood Criteria	**Definition**	**Factors**	**Rubric**
		• Level of segmentation/isolation between IT, OT, and physical infrastructure • Diversity of technology stack (increases chance of vulnerable components)	vendor access, shared platforms). Segmentation exists but may be partial. Exposure is externally accessible (e.g., Shodan, Censys). **Moderate (3)**: Limited external exposure. Attack surface is more indirect (e.g., through trusted partners or weak internal controls). Moderate segmentation. **Low (2)**: Mostly isolated systems with tight control over access paths. Minimal vendor integration and strong segmentation. **Very Low (1)**: Air-gapped or near-air-gapped. Highly restricted, purpose-built systems with no practical remote access or other attack vector.
CIP Integration - Likelihood	Evaluates the extent to which the NERC CIP Reliability Standards, and accompanied ERO materials currently provide relevant and technically applicable preventive or detective controls for each risk being evaluated. **(Prevention & Detection) (Mitigation)**	• Presence of specific NERC CIP Reliability Standards requirements that provide mitigation objectives for the evaluated risk • Asset types in scope for the relevant standards • Precision and enforceability of the standard (e.g., prescriptive vs policy-based) • Relevance of supporting guidance (e.g., Implementation Guidance, Technical Reference Documents, etc.) • Active SARs, SDTs or proposed modifications addressing this risk class	**Very High (5):** Risk is clearly and comprehensively addressed by current NERC CIP Reliability Standards. Controls are directly applicable to the risk and enforced across applicable NERC CIP systems. **High (4):** Risk is moderately addressed by current NERC CIP Reliability Standards. Controls are applicable, but may not be applicable to all NERC CIP asset/system types potentially impacted by the risk). Guidance supports implementation.

Table B.1: Identified Risk Criteria			
Likelihood Criteria	**Definition**	**Factors**	**Rubric**
		(use for future residual risk mitigation considerations)	**Moderate (3):** Risk is indirectly addressed but not in a targeted way. Incomplete or tangential coverage across NERC CIP system types potentially impacted by the risk. **Low (2):** Only partial or incidental overlap with existing NERC CIP Reliability Standards. Incomplete coverage across in-scope NERC CIP systems. **Very Low (1):** No NERC CIP Reliability Standards address the risk. Other security control frameworks may be available for applicability.
Control Implementation - Likelihood	Assesses how technically mature, operationally feasible, and widely implemented mitigation measures are across the industry for this class of risk, regardless of whether they are regulated. (Prevention & Detection) **(Mitigation)**	• Availability of reliable, commercial / open-source software tooling, or OEM integrations • Sector-wide implementation patterns (across entity sizes and regions) • Barriers to adoption (e.g., cost, skill requirements, integration effort) • Community maturity (e.g., vendor support, best practices, professional guidance) • Availability of voluntary guidance or implementation references • Sources to inform current state (e.g., industry surveys, CMEP-IP, FERC Reports, etc.)	**Very High (5)**: Controls are mature, proven in the field, and widely adopted across all major segments of the industry. High automation and vendor support. **High (4)**: Controls are mature and in broad use, though some entity types or regions may lag. Implementation is supported by documentation and services. **Moderate (3)**: Mixed adoption. Mitigations exist and are technically viable but vary in implementation quality or scope. **Low (2)**: Immature controls. Partial solutions exist but are fragmented, unsupported, or burdensome.

Table B.1: Identified Risk Criteria			
Likelihood Criteria	**Definition**	**Factors**	**Rubric**
			Very Low (1): No practical mitigation exists or adoption is extremely rare. Risk is not well controlled in practice.
Control Efficacy – Likelihood	Evaluates the effectiveness of current mitigating controls in directly reducing the likelihood of this risk by disrupting the attack path, blocking access, enabling early detection, etc. **(Preventive and Detective) (Mitigation)**	• Directness of control mapping to known TTPs or compromise steps (e.g., MITRE ATT&CK for ICS) • Potential for detection during early attack stages (e.g., initial access, lateral movement, etc.) • Alignment to ICS/OT cybersecurity frameworks (e.g., NIST, C2M2, etc.) • Historical or test-case evidence that these mitigations stop or slow threats • Effectiveness across system types and operational contexts	**Very High (5)**: Controls directly and effectively disrupt key steps in the attack chain. High confidence in prevention or detection before compromise. **High (4)**: Controls meaningfully reduce likelihood but may not cover all attack variants. Still offer strong protection in most cases. **Moderate (3)**: Controls provide some defense but may miss common evasion techniques or fail to detect initial access. **Low (2)**: Controls only partially address the risk or are easily bypassed. Minimal reduction in likelihood. **Very Low (1)**: Controls do not reduce likelihood in a meaningful way. Risk remains almost fully exposed.
Scope of Impact (Single-Target)	Reflects the plausible maximum service disruption resulting from a successful compromise of a single system or small entity (i.e., the scope of impact is localized)	• Load served or controlled by the system (MW / MWh) • Role in grid topology (e.g., upstream node, control hub, EMS, substation) • Estimated restoration complexity and time (assuming successful compromise)	**Severe (5)**: Scope of impacts may have widespread effects across the BPS throughout an Interconnection / North America. **Major (4)**: Scope of impacts may have widespread effects across the Reliability Coordinator (RC) area. **Moderate (3)**: Scope of impacts may have

Table B.1: Identified Risk Criteria			
Likelihood Criteria	**Definition**	**Factors**	**Rubric**
			widespread effects on portions of the RC area. **Minor (2)**: Scope of impacts may primarily affect the individual entity, with limited broader consequences. **Negligible (1)**: Scope of impacts are minimal or non-existent to the BPS.
Maximum Severity of Impact (Single-Target)	Represents the most severe operational effect this risk could plausibly cause such as loss of visibility, control manipulation, or full service denial based on known failure modes and threat behaviors (i.e., the severity of impact within the scope)	• Nature of disruption (i.e., loss of visibility / control vs data / signal manipulation vs asset / system destruction) • Detection latency or ambiguity • Operator actionability and diagnostic burden • Potential for unintended cascade or misoperation • Compatibility with standard restoration workflows	**Severe (5)**: Malicious control manipulation or silent misoperation; can cause false trust in stability, mis-coordinated recovery, or active sabotage. Coupled with loss of visibility/control. **Major (4)**: Total loss of control/visibility; operators are blind or paralyzed, with high risk of human error or cascading failures. **Moderate (3)**: Intermittent or partial loss of functionality; operations are degraded but remain somewhat manageable. **Minor (2)**: Noise or limited disruption; may affect operational speed but not core functionality. **Negligible (1)**: Disruption is easily isolated, identified, and mitigated without significant complexity.
Coordination or Aggregation Potential	Measures the degree to which a security incidents impact could be amplified by coordinated, simultaneous, or cascading effects across multiple entities, systems, or	• Presence of common technology or protocols across multiple entities (e.g., EMS vendor, VPN concentrators)	**Severe (5)**: A successful attack could plausibly trigger widespread, simultaneous disruptions across multiple entities or RC areas. Grid-wide implications possible (e.g.,

Table B.1: Identified Risk Criteria			
Likelihood Criteria	**Definition**	**Factors**	**Rubric**
	regions - whether through deliberate attack coordination or systemic aggregation (e.g., supply chain exposure, shared infrastructure).	• Use of shared cloud or remote access services Supply chain relationships with common OEMs or integrators • Insufficient segmentation between IT/OT systems or within OT systems • Known vulnerabilities or TTPs that could enable multi-target compromise • Targeting of resources that participate in regional coordination groups or interdependent restoration procedures	supply chain compromise, core protocol exploit, BPS interconnection dependencies). **Major (4)**: Coordinated impact possible across multiple key systems within a single RC area, or multiple entities using similar technologies or vendors. Disruption could affect regional grid stability. **Moderate (3)**: Aggregated effects plausible through shared vendors, cloud platforms, or system-wide misconfigurations. Effects may be visible in pockets or adjacent systems. **Minor (2)**: Some potential for correlated impact via shared practices or IT infrastructure, but limited scope and minimal impact on neighboring systems. **Negligible (1)**: Attack is highly localized, with little risk of spillover or concurrent effects beyond the targeted entity.
CIP Integration - Impact	Assesses whether the NERC CIP Reliability Standards provide relevant and technically applicable controls that reduce the consequences of this risk (e.g., blast radius, operational degradation, recovery difficulty). **(Mitigation) (Respond, Contain, Recover)**	• Presence of CIP controls related to containment, segmentation, or restoration (e.g., CIP-008, CIP-009, CIP-010) • Applicability of the standards to affected systems • Clarity and enforceability of the control objectives • Support through industry guidance or implementation documentation	**Very High (5):** NERC CIP Reliability Standards directly address consequence reduction for this risk (e.g., restoration, containment, misoperation detection). **High (4):** Clear alignment with NERC CIP Reliability Standards to reduce the consequences of this risk, but coverage may be partial (e.g., limited to BES Cyber Systems). Supporting guidance

Table B.1: Identified Risk Criteria			
Likelihood Criteria	**Definition**	**Factors**	**Rubric**
			exists. **Moderate (3):** NERC CIP Reliability Standards address the risk indirectly, but without specific requirements tied to the impact type (e.g., operational consequence, scope of impact). Supporting guidance exists but does not fully address the risk. **Low (2):** Minimal connection between the NERC CIP Reliability Standards and the scope and effect of the impacts of this risk. Guidance does not exist or guidance is in development but not approved/endorsed. **Very Low (1):** No relevant NERC CIP Reliability Standards exist for this class of consequence. Risk is outside CIP scope or control objectives. Other security control frameworks available for applicability. Guidance does not exist.
Control Implementation – Impact	Measures the electricity subsector-wide adoption, availability, and maturity of mitigation measures that reduce the impact of successful incidents—including containment, failover, and isolation capabilities. **(Mitigation) (Respond, Contain, Recover)**	• Are fallback systems (manual control, redundant EMS, etc.) commonly deployed? • Are containment mechanisms widely used and tested (e.g., zone-based architecture)? • Do OEMs support recoverability (e.g., firmware rollback, resilient designs)?	**Very High (5)**: Controls are widely implemented and well-integrated into operations. Restoration and containment capabilities are available across most environments. **High (4)**: Strong control adoption in most major entities, with some variation in less-regulated or distributed systems. Tooling is widely available. **Moderate (3)**: Mitigations

Table B.1: Identified Risk Criteria			
Likelihood Criteria	**Definition**	**Factors**	**Rubric**
		• Is tooling (e.g., forensics, integrity checks) available and adopted?	exist but are unevenly adopted or only deployed in specific asset classes or system types. **Low (2)**: Partial or immature adoption. Many entities lack implementation due to complexity, cost, or design limitations. **Very Low (1)**: Controls are rarely deployed or unavailable for affected systems. Industry relies on manual, slow, or incomplete recovery paths.
Controls Efficacy – Impact	Assesses whether the available and implemented controls are effective at reducing the actual impact of this risk - by isolating the blast radius, enabling early operator intervention, or minimizing downtime. **(Mitigation) (Respond, Contain, Recover)**	• Controls align with likely disruption mode (e.g., segmentation for visibility loss, fail-safes for control manipulation) • Ability to quickly detect and isolate impact • Functional fallback (e.g., manual operation, alternate paths, regional independence) • Resilience of interdependencies (e.g., supply chain, redundant capabilities needed for recovery such as remote access, effective IRPs) • Difficulty of control circumvention	**Very High (5)**: Controls clearly minimize disruption. Misoperation is detected early; systems fall back safely; outages are limited in scope and duration. **High (4)**: Controls are effective in most scenarios, but some degradation or recovery delay may occur. **Moderate (3**): Some impact reduction is likely, but controls may not respond fast enough, or only contain part of the effect. **Low (2)**: Controls provide limited containment; misoperation or large outages are still plausible. **Very Low (1)**: Controls do little or nothing to reduce consequences once the attack is successful.
Response and Recovery Preparedness	Represents how well entities are trained, exercised, and procedurally	• Industry-wide availability and regular use of response	**Very High (5)**: Regularly tested procedures, high operator awareness, clear

Table B.1: Identified Risk Criteria			
Likelihood Criteria	**Definition**	**Factors**	**Rubric**
	ready to recover from this class of disruption - independently of whether the technical controls exist. **(Mitigation)**	playbooks (e.g., SCADA loss, grid isolation) • Frequency of industry drills or table-tops targeting similar disruption modes • Institutional knowledge of this risk class • Recovery staffing, escalation paths, and coordination frameworks (RC/BA/TO) • Operator situational awareness and alerting when disruption occurs	recovery protocols. Industry is operationally ready. **High (4)**: Recovery plans and staff are prepared, tested occasionally, and documented. **Moderate (3)**: Partial preparedness; plans may exist but are outdated or untested. Recovery depends on ad-hoc judgment. **Low (2)**: Minimal preparation. No drills or clear playbooks for the potential impact of this risk category. **Very Low (1)**: Unprepared. Disruption would lead to extended downtime or unsafe conditions due to poor organizational readiness.

Formula

The formula below was used to compute risk scores for each of the identified risks in the team's risk evaluation framework.

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

Figure B.1: Risk Score Formula

Scoring

The table below shows the final scored results of the NERC team's completed risk assessment and resulting relative ranking for each risk.

Table B.2: Completed Risk Scoring								
Identified Risks	**Likelihood Score**	**Impact Score**	**Mitigation Score**	**Computed Score**	**Survey-Incorporated Weighted Score**	**Internal Rank**	**Industry Survey Rank**	**Final Weighted Ranking**
Supply Chain	***4***	***4.67***	2.57	10.3	**10.3**	2	1	1
Physical Attacks on Infrastructure	***4.75***	***4.00***	2.57	10.6	**9.9**	1	6	2
Phishing & Social Engineering	***4.75***	***4.33***	**3.29**	9.4	**9.4**	3	4	3
Insider Threats to the U.S. Bulk Power System (BPS)	3.75	***4.67***	**2.86**	9.1	**9.1**	4	3	4
Ransomware/ Malware	***4.25***	***4.00***	**3.14**	8.1	**8.8**	8	2	5
Cloud Environment Compromise	3.75	***4.00***	2.57	8.3	**8.3**	7	8	6
Weaponization of Drones Targeting Physical Electric Grid Assets	***4***	3.67	2.29	8.9	**8.1**	5	11	7
End-of-Life Systems (EOL Systems)	3.75	3.67	**2.71**	7.4	**8.0**	13	7	8
Insufficient Cybersecurity Workforce in U.S. Bulk Power System Entities	3.25	***4.33***	**3.00**	7.0	**7.8**	17	9	9
Insecure Protocols	***4***	3.67	**2.86**	7.6	**7.6**	10	10	10
Exploitation of Public Telecommunications	3.5	***4.67***	**2.71**	8.7	**7.5**	6	16	11
Insufficient Low-Impact Security	3.75	3.33	2.29	7.4	**7.4**	12	12	12
Ineffective Incident Response & Recovery Planning	3.75	3.67	**2.71**	7.4	**7.4**	14	14	13
Compromise of Category 2 GO/GOP IBR Facilities	3.5	3.00	***1.71***	7.2	**7.2**	15	15	14
Network-Based Attacks	3.75	3.67	**3.43**	6.0	**7.2**	19	5	15
Targeting of DER Aggregator (DERA) Control Systems	2.75	***4.00***	***1.71***	7.6	**6.9**	11	17	16
Unregistered 3rd-Party Operators	3.25	***4.00***	***2.14***	8.1	**6.8**	9	21	17
Electric Vehicle Supply Equipment (EVSE)	3.25	3.00	***1.43***	7.2	**6.6**	16	22	18
Large-Load Manipulation	**2.5**	3.67	***1.86***	6.1	**6.5**	18	13	19
Stolen Sensitive Information (CEII or BCSI)	***4***	3.00	**3.00**	5.9	**5.9**	20	19	20
Targeting of Artificial Intelligence (AI) Tools	**2.25**	3.33	2.29	4.5	**4.5**	21	18	21
Regulatory Lag	**1.5**	3.33	2.29	3.0	**3.0**	22	20	22

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	
Weaponization of drones Targeting Physical Electric Grid Assets	***0***																
End-of-Life Systems (EOL Systems)	***10***	1	1	1	1	1	1	1	1	1	1	1	1				1
Insufficient Cybersecurity Workforce in U.S. Bulk Power System Entities	***0***																
Insecure Protocols	***11***	1	1	1	1	1	1		1	1	1	1	1		1	1	1
Exploitation of Public Telecommunications	***10***	1	1	1	1	1	1	1	1	1	1	1	1		1		
Insufficient Low-Impact Security	***5***	1	1	1	1	1		1	1	1							
Ineffective Incident Response & Recovery Planning	***1***		1								1						
Compromise of Category 2 GO/GOP IBR Facilities	***7***	1	1	1	1	1	1	1	1		1						1
Network Based Attacks	***4***	1					1		1	1			1				
Targeting of DER Aggregator (DERA) Control Systems	***12***	1	1	1	1	1	1	1	1	1	1	1	1	1	1		1
Unregistered 3rd-Party Operators	***1***	1		1										1			

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**
Electric Vehicle Supply Equipment (EVSE)	***6***	1	1		1	1	1	1			1						1
Large-Load Manipulation	***1***			1								1					
Stolen Sensitive Information (CEII or BCSI)	***0***		1														
Targeting of Artificial Intelligence (AI) Tools	***1***													1			
Regulatory Lag	***0***																

Appendix C: Contributors

NERC would like to acknowledge the following individuals and groups for their input, feedback, and review of the materials and processes needed to deliver this CIP Roadmap white paper.

Table C.1: Contributors	
Name	**Organization**
Andrea Koch	EEI
Kristine Martz	EEI
Carl Epping	MRO
Jess Syring	MRO
Dan Goodlett	NERC
Darko Kovac	NERC
Larry Collier	NERC
Michaelson Buchanan	NERC
Holly Peterson	NERC
Sushil Subedi	NERC
Michael Bilheimer	NPCC
Douglas Vitale	NPCC
David Sopata	RF
Lindsey Mannion	RF
Supply Chain Subcommittee Members	RSTC Subcommittee
Security Integration Technology Enablement Subcommittee Members	RSTC Subcommittee
Security Working Group Members	RSTC Working Group
Etinnie Burnett	SERC
Brian Allen	SERC
Paul Hopson	Texas RE
William Sanders	Texas RE
Scott Brooksby	WECC
Morgan King	WECC