NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

New Technology Enablement and Field Testing

NERC Security Integration and Technology Enablement Subcommittee White Paper

December 2024

RELIABILITY | RESILIENCE | SECURITY

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

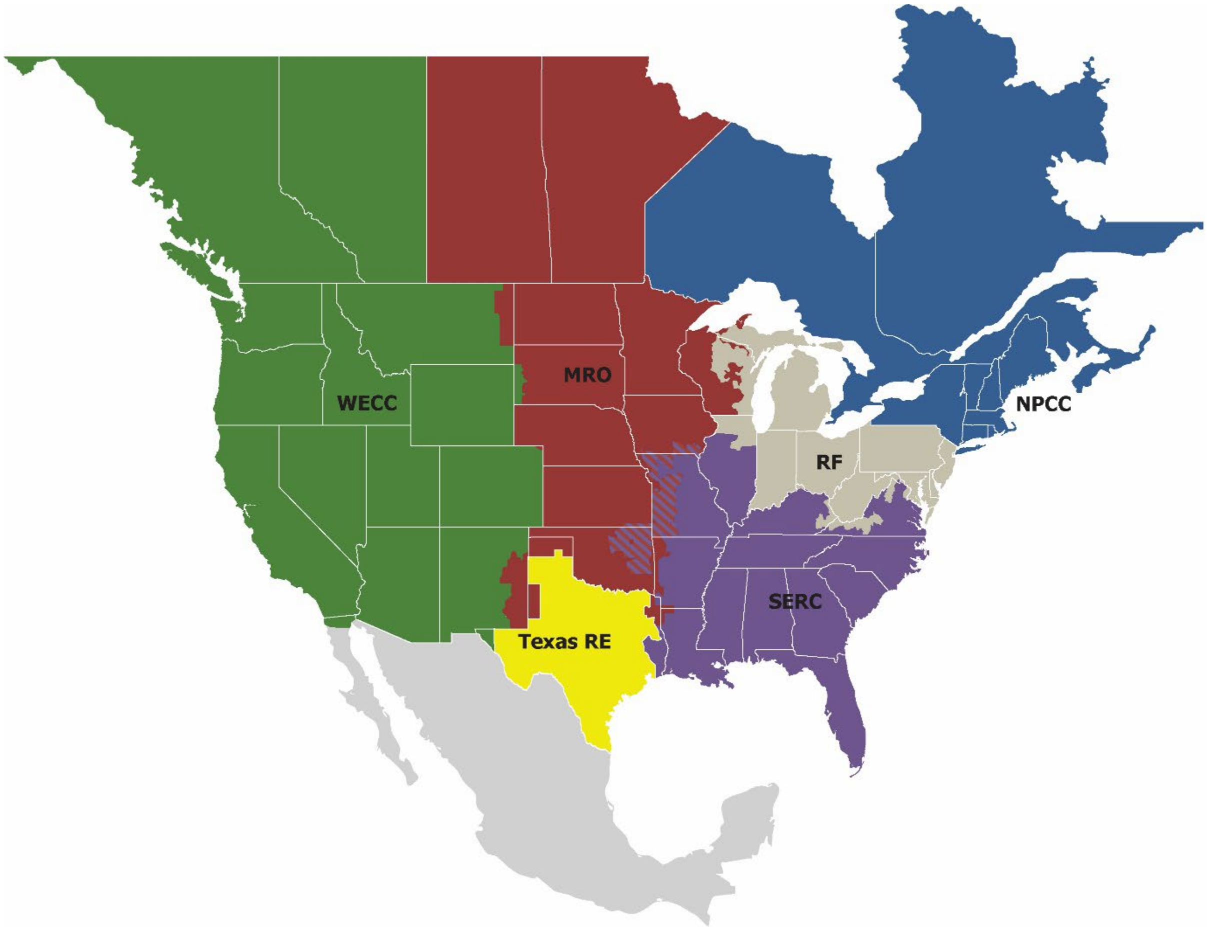
Table of Contents

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 the North American Electric Reliability Corporation (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

This white paper uses the term "utilities" to broadly encompass all entities involved in management of the electric industry and operation of the electric grid, including those responsible for transmission, generation, and distribution. This definition is inclusive of independent power producers (IPP) despite their traditional distinction from utilities. This document will collectively refer to both utilities and IPPs as utilities.

While this is a broad discussion that goes beyond the Bulk Electric System (BES), some of the mechanisms to address challenges that are discussed, such as the Regional Engagement for Technology and Integration Innovation Acceptance (RETINA) program, are meant to address challenges specific to those entities required to comply with NERC Reliability Standards.

Statement of Purpose

As a general principle, the Security Integration and Technology Enablement Subcommittee (SITES) believes that the exploration and adoption of new technologies—when implemented reliably and securely—should be accessible to utilities throughout the industry. As the electric grid evolves to meet the challenges of digitalization, renewable integration, and changing energy demands, utilities face significant barriers to adopting innovative technologies. This white paper aims to open and invite industry to the broad conversation about these challenges while emphasizing that minimizing risk through collaborative solutions is essential.

Chief among the challenges facing the electric sector in new technology innovation and adoption is the need to ensure that new endeavors do not compromise existing physical or electronic security protections. Utilities must maintain the security and reliability of the BPS while also mitigating the substantial risks of regulatory penalties for non-compliance. By uniting industry stakeholders to develop and endorse Reliability Standards and technologies that enhance security and reliability, risk profiles can be reduced while reliability is ensured.

Rather than providing prescriptive answers, this white paper encourages an expansive view that goes beyond the confines of the BES and the scope of the NERC Critical Infrastructure Protection (CIP) Reliability Standards.

As the electric grid transforms in response to digitalization, renewables, and changing energy demands, innovative technologies present opportunities to boost reliability and security and optimize operations. However, utilities face numerous challenges in evaluating and seeking adoption of new technology solutions, including regulatory Reliability Standards and requirements interpretations and conflicts, employee training and new skill development, and the ability to incorporate technology investments into existing rate structures. Utilities may struggle to simply understand the impacts of new technology on operations, including benefits or risks to reliability and security. The electric industry would benefit from greater collaboration between registered entities, the ERO Enterprise, and technology vendors who can innovate based on stakeholder needs. Collaboration can help ensure that the security, risk, and operational needs of the industry are not only met by new technology but that they can be demonstrated through technology pilots and trials, facilitating adoption at a pace that supports the speed of the evolving electric grid.

Broadly, industry shows a willingness to seek out and embrace new technology to support the changing grid and likewise supports the development and implementation of new security and Reliability Standards when appropriate. In fact, the electric industry is seeing a greater workload and pace of standards development than ever before, and these efforts deserve to be applauded. As the grid continues to evolve and the pace of technology rapidly accelerates, the electric industry needs mechanisms to enable and support entities willing to invest efforts in testing and deploying new technologies in secure, reliable ways that can be shared with peers.

To address the challenges that utilities face in adopting new technologies that must comply with the mandatory NERC Reliability Standards, this white paper proposes the development of a mechanism to facilitate pre-Standards Authorization Request (SAR) and pre-standards development coordinated field trials of emerging technologies, operating outside of the traditional standards development process. The proposed mechanism is conceptual and will require coordinated industry effort and buy-in to ensure that it meets the security, reliability, and efficiency objectives as outlined in this white paper. It is proposed as the RETINA program.

Utilities required to comply with the mandatory NERC Reliability Standards have mechanisms to test new technologies through existing programs, such as field tests that can be approved in conjunction with a standards development project. The field test process is limited by procedural constraints, such as requiring an approved SAR prior to seeking approval for the field test—meaning that the utility has to understand the security or reliability gap and how it aligns with the Reliability Standards prior to initiating the test. The RETINA program seeks to provide a more flexible and proactive approach. By conducting technology trials outside of the standards development framework, RETINA enables earlier exploration and assessment of new technologies without the immediate assumption of Reliability Standards revision work.

In addition to initiation and oversight provided by NERC and industry stakeholder technical committees, such as those under the Reliability and Security Technical Committee (RSTC), RETINA would leverage Regional Entities—given their connections across the industry and unique perspectives for each region's respective differences—to coordinate trials within their region. These trials would evaluate reliability, security impacts, and regulatory challenges of technologies like cloud computing,[1] artificial intelligence (AI) (including generative AI and machine learning (ML)), and real-time decision enhancement using synchrophasor data.

By cultivating guidance from trial results, RETINA aims to enable faster, secure, and reliable adoption of beneficial solutions. It complements the existing field test process by providing a pathway for industry collaboration on technology trials before determining that Reliability Standards revisions are necessary and the Reliability Standards development process is initiated. SITES believes that such collaboration will expedite new technology exploration, inform potential standards development when necessary, and increase education and awareness of thoroughly vetted technologies that support BPS security and reliability.

RETINA is proposed strictly as a high-level concept that SITES encourages each Regional Entity to independently implement with input from industry stakeholders. This approach allows industry to discover and adopt best-in-breed practices over time, fostering innovation while maintaining flexibility.

Continued improvements to the self-regulated industry necessitate Federal Energy Regulatory Commission and ERO Enterprise leadership commitment and support, flexible regulatory enhancements, and close coordination between stakeholders. Collaborative efforts like RETINA can modernize grid operations through secure technology integration, optimizing reliability, resilience, and cyber security for the future. Additional challenges described in this white paper can be addressed through collaborative efforts outside of the RETINA program, but these efforts are not directly proposed in this paper. The purpose in identifying these challenges is to spark conversation about what those efforts could look like.

[1] This white paper was developed before the development and submission of the SAR that led to Project 2023-09 Risk Management for Third-Party Cloud Services. However, the example is pertinent to the potential benefit of pre-SAR trials.

Introduction

Background

With the aim of supporting the BPS in a secure, reliable, and effective manner, SITES tasks itself with "identify[ing] potential barriers (e.g., regulatory, technological, and complexity) and support[ing] the removal of these barriers to enable industry to adopt emerging technologies."[2] Due to the nature of critical infrastructure and the unbending need for a focus on reliability, the electric industry is cautious about adopting newer and innovative technologies. Other critical infrastructure sectors, including healthcare (specifically pharmaceuticals), financial services, and the defense industrial base (DIB), have adopted newer technologies more rapidly thanks to factors including mature assessment processes (including third-party assessment processes) and clear engineering and design specifications. While the security, reliability, and resilience needs of these critical infrastructure sectors are not directly aligned with those of the electric sector, the implementation and use of advanced technologies in those sectors can serve as a foundation for consideration. This white paper discusses factors that are inhibiting adoption by the electric sector and that are stifling ongoing innovation of new technology. The paper makes a formal recommendation to address what SITES considers the greatest roadblocks to adopting new and advanced technologies within the industry.

Among the challenges related to new technology in the electric industry, this white paper gives special attention to assessing the industry's regulatory framework, including the NERC CIP Reliability Standards and the standards development process, with an aim to identify enhancements or complementary processes to better facilitate new technology adoption.

Appendix A further offers discussion and insights into industry struggles with workforce, financing, and internal regulatory compliance approaches, which can hinder the adoption of new digital technologies among utilities. These challenges are not addressed by the RETINA program.

NERC CIP Reliability Standards and Standards Development

The NERC CIP Reliability Standards are designed to protect the BES from cyber attacks and other threats. These Reliability Standards contain multiple requirements. One of the many processes outlined by the *NERC Standard Processes Manual*[3] is the development process for modifying or creating these standards, which begins (i.e., Step 0 in the *Standards Process Manual*) with a SAR, documenting the scope and reliability benefit of proposed projects for new or modified standards or the retirement of existing standards. This process involves a review by NERC Reliability Standards staff and action by the Standards Committee (SC), which decides whether to accept, remand, or reject a SAR. If accepted, the project is added to the list of approved projects and assigned a priority in the Reliability Standards Development Plan.[4] A drafting team is then formed, which reviews the SAR, makes necessary revisions based on formal or informal industry comment, and returns the revised SAR to the SC for the drafting team to begin. So begins a cycle of drafting, quality reviews, comments, balloting,[5] and, sometimes, SAR revisions. Eventually, the team ends with a successful ballot(s) and a final adoption ruling. For a given standards project, this process may take anywhere from a year to many years. While the pace of standards development depends on a number of factors, including prioritization and complexity, processes that include the development of technical support and/or scoping can help reduce timelines.

The collaborative nature of the standards development process is a success story for industry. SITES acknowledges that it takes time to get a Reliability Standard right given the consequence of noncompliance or reliability impacts. Often, a given standards development project for NERC CIP may take up to a year—which does not seem unrealistic for the entirety of the industry to develop, iterate on, and approve a Reliability Standard. In some cases, taking multiple years is justified. However, in this length of time, technology is likely to advance significantly, potentially

[2] https://www.nerc.com/comm/RSTC/Pages/SITES.aspx

[3] https://www.nerc.com/pa/Stand/Revisions%20to%20the%20NERC%20Standard%20Processes%20Manual%20SP/SPM_Clean_Oct2018.pdf

[4] https://www.nerc.com/pa/Stand/pages/reliabilitystandardsdevelopmentplan.aspx

[5] https://www.nerc.com/pa/Stand/Pages/Balloting.aspx

requiring additional iterations or a new SAR. This merely underlines the challenge faced by industry to achieve the balance of reliability and security along with the flexibility of supporting new technology adoption within the NERC Reliability Standards.

Technology Adoption

SITES views technology adoption as the process by which new technologies are embraced and used by individuals, vendors, utilities, or the electric industry at large. This process often begins with the initial awareness and understanding of a new technology, including its impact on reliability and security, followed by its evaluation against existing solutions in terms of efficiency, cost, and potential benefits. Once deemed beneficial, the technology is then implemented and integrated into existing systems or practices on an individual entity basis. The adoption process is influenced by various factors, including technological capabilities, funding, regulatory compliance, vendor support, and the overall impact on operational efficiency and productivity through the lens of each individual organization. New technology—when tested, assessed, and implemented in accordance with the security and reliability needs of the grid—can help the electric industry achieve modernization, improve grid reliability, efficiency, and security, and meet evolving Reliability Standards. This process is also key to addressing current challenges and leveraging opportunities presented by advancements such as renewable energy, smart grid technologies, and digitalization.

Technology Innovation

Innovation may originate from two main sources: direct utility needs and vendor-initiated development. Vendors may initiate technology development independent of expressed utility needs, forging forward based on internal research and development projections or perceived future market demands. This occasionally results in a mismatch between offered technological solutions and practical utility adoption. Therefore, a two-way collaborative dialogue between utilities and vendors, focused on co-developing solutions that are keenly attuned to specific operational and regulatory needs, is pivotal. Within this synergy between vendors and utilities, SITES recognizes that the drive for ongoing technology innovation is affected by the appetite for adoption among the utilities. Therefore, barriers to adoption negatively impact the drive to innovate as well.

Chapter 1: Drivers for Technology Innovation and Adoption

Grid Reliability, Resilience, and Security

Broad advancement of the grid through the combination of technological innovation and adoption is required to bolster grid reliability and security in the face of grid transformation and an emerging threat landscape. New technologies can enhance response mechanisms to grid disturbances, help ensure consistent service reliability and improve grid resilience to cyber threats. With the integration of new grid technologies, such as inverter-based resources, distributed energy resources (DER) and DER aggregators, and electric vehicle charging, innovation must advance to help industry keep up with energy demand and safeguard the grid from cyber and physical security threats. Cloud technology, including software as a service (SaaS), AI, and ML, is at the forefront of example digital technologies that may offer reliability, resilience, and security benefits to the BPS and yet may be inhibited by the challenges discussed in this white paper.

Utility and Innovator Relationships

Ensuring the relevance and applicability of technological innovations in the electric industry necessitates ongoing investment in a strong, synergistic relationship between utilities and innovators, including vendors, the National Laboratories, and universities. Ongoing dialogue between these entities, especially in the conceptual and development phases of technology creation, is crucial for relevant innovation and adoption. As an example, utilities can provide real-world perspectives and operational data, while vendors bring technical expertise and solution development capabilities to the real-world challenges faced by utilities. Co-developing technology ensures that the delivered solutions are not only operationally viable but also forward-looking, thereby paving the way for future-ready utility operations. Even with such cooperation, however, further collaboration is often required of these entities to participate at the regulatory level. This work is necessary to help ensure that Reliability Standards and audit practices can evolve, when necessary, to accommodate new leading technology solutions, no matter if vendors and utility operators agree that the technology is ready to be adopted and will conceivably result in a more reliable, resilient, and secure grid.

Risk Management Frameworks and Innovation

In a perfect world, compliance with Reliability Standards, like NERC CIP, as well as internal control frameworks and metrics, should be viewed as a tool that facilitates and iteratively drives maturity. The result of that maturing program could be modernization through technological advancement, or adding additional security, reliability, or risk management controls or internal validations to existing technologies over time. Entities can leverage compliance as a guide to embedding an ever-improving risk management framework, enabled through ongoing adoption of technological innovations securely and effectively, within their operational systems and processes. This speaks to a mature strategy that interweaves regulatory compliance and technology enablement. This strategy can only be realized when enacted through the ongoing effort of standards development to achieve a robust and flexible regulatory framework that is in sync with the scale and pace of new technology, as well as mature approaches to internal compliance strategy by registered entities that enables change in their organization rather than stifling change.

Chapter 2: New Technology Adoption Use Cases

Rapid advancements in available technologies are reshaping how utilities operate, manage resources, and interact with the grid. Nevertheless, the scale, pace, and outcome of any particular technology's adoption in the industry are subject to many of the roadblocks identified in this white paper. Some use cases are widely viewed as simply disallowed, even if indirectly, under current Reliability Standards, such as the broad scope of NERC CIP applicable systems used in cloud service provider environments. Other use cases, including some entirely outside of the scope of the NERC CIP Reliability Standards or even the BES and not intended to be addressed via the RETINA program, may currently see limited adoption but still face challenges that inhibit the technology's wider adoption. Wider adoption of some use cases below may be stifled from the perception of regulatory applicability uncertainty (present AND future), lack of industry awareness of the technology (including not just vendor or product availability but its reliability or security benefits and risks), and, finally, gaps in skilled labor to implement and use a given technology. Provided below is a non-exhaustive list of technology use cases that promise potential benefits to grid reliability, resilience, or security while not currently experiencing wide adoption due to one or more significant challenges for the average utility to adopt and implement:

- **Cloud – platform, infrastructure, or software as a service (PaaS/IaaS/SaaS)**: The adoption of cloud computing in the utility sector offers numerous benefits, including enhanced scalability and flexibility of computing infrastructure. It can facilitate advanced data analytics, improve operational efficiency, and reduce IT infrastructure costs. Cloud technology enables utilities to quickly adapt to changing demands and integrate new services without significant upfront investments in physical infrastructure. SaaS allows utilities to use cloud-hosted software applications, reducing the need for on-premises installations. This approach provides agility in software deployment and maintenance, leading to potential cost savings and/or enhanced operational efficiency. SaaS models enable continuous updates and access to the latest features without the traditional complexities of software upgrades.

- **Electronic Access Control or Monitoring System (EACMS) and Physical Access Control System (PACS) in the cloud**: By migrating EACMS to the cloud, including utilizing industry-leading cloud-based security tools such as Managed Security Service Providers (MSSP) and Managed Detection and Response (MDR) solutions, utilities gain enhanced capabilities in analyzing and triaging security data. This cloud-based approach allows for more efficient system and data integration, leading to improved cyber security measures with controls and architectures that are commensurate to the security objectives of the NERC CIP Reliability Standards. Cloud-based PACS offer utilities enhanced security management of physical perimeters across geographically dispersed facilities. By centralizing control, these systems allow for real-time monitoring and management of access points remotely, improving response times to security breaches and streamlining compliance with security standards.

- **ML/Analytics platforms**: ML and analytics platforms are critical for processing and interpreting large volumes of data generated by utility operations. These platforms aid in predictive maintenance, forecasting, and enhancing operational decision-making. They enable utilities to identify patterns and insights that would be impossible to discern manually, leading to more-informed, data-driven decisions.

- **AI large language models (LLM)/Generative AI**: AI, including LLM and generative AI, offers significant potential for optimizing grid operations, automating customer interactions, and advancing data analysis. These AI applications can predict demand, optimize resource allocation, and improve customer service through automation and enhanced personalization.

- **DERs/DER aggregators/DER management systems (DERMS)**: DERs and DER aggregators, combined with DERMS, provide a new flexible approach to grid management. They facilitate the integration of decentralized energy production and distribution. DERMS aggregate, simplify, translate, and optimize these resources, ensuring stability and efficiency in the grid.

- **Outage and vegetation management**: Modern technologies in outage and vegetation management enable more precise prediction and faster response to power outages. Advanced analytics and imaging technologies help in efficient vegetation management, reducing the risk of outages and maintaining safety standards.

- **Simulation and training environments**: By utilizing cloud-based simulation and training platforms, utilities can offer realistic, scalable training for their staff without requiring additional assets in the utility's electronic security perimeter. These environments simulate real-world scenarios, enabling employees to hone their skills and prepare for various operational situations in a cost-effective and controlled setting.

- **Asset management, inspection scheduling, and route planning**: Advanced asset management systems, coupled with intelligent inspection scheduling and route planning, optimize maintenance workflows. These tools ensure effective resource allocation, minimize downtime, and enhance the lifespan of assets through predictive maintenance strategies.

- **Grid planning studies and decision support in the cloud**: Cloud platforms for grid planning and decision support enable dynamic and complex analyses, facilitating better-informed long-term strategic decisions. They provide utilities with tools for scenario analysis, load forecasting, and resource planning, allowing for more efficient and sustainable grid management.

- **Common information modeling (CIM) and geographic information system** (**GIS) platforms in the cloud**: Integrating CIM and GIS in the cloud enhances the management and visualization of utility assets and infrastructure. This integration offers improved data accuracy, real-time updates, and better decision-making support for asset management and network planning.

- **Energy management systems (EMS) historical data management in the cloud**: Managing historical data from EMS in the cloud provides utilities with better access to and analysis of historical trends. This approach aids in operational planning, performance analysis, and long-term strategic decision-making, leveraging the power of cloud storage and computing for large-scale data management.

- **Synchrophasors/Phasor measurement units** (**PMU)**: Synchrophasors or PMUs represent a significant advancement in real-time monitoring of the electric grid. These devices measure the voltage, current, and frequency at specific locations on the grid, providing detailed insights into grid conditions. By utilizing PMUs, utilities can enhance real-time or near real-time decision-making in a multitude of ways.

Chapter 3: Regulatory Frameworks and Technology

Often, modifications or advancements in Reliability Standards may not coincide with the evolving technology innovation curve, potentially slowing the adoption of emergent, beneficial technologies. This misalignment could risk inhibiting early-stage technology adoption, as entities may exercise caution to ensure continuous compliance alignment, resulting in a tendency toward late-stage or post-maturation adoption of technologies. Consequently, the regulatory process, along with limited audit flexibility, may inadvertently stifle innovative endeavors and their subsequent potential advantages to the electric industry. With this in mind, we may examine regulatory adaptation mechanisms and audit methodologies around NERC CIP to assess the potential for fostering an environment even more conducive to technological exploration and adoption.

NERC CIP Assessment

NERC CIP, while embodying performance-based control objectives, adopts a notably device-centric and defined network perimeter approach that infuses a degree of prescriptiveness into the framework. The effective limitation to on-premises systems and the delineation of static network perimeters intrinsically guide utilities toward a structured, and somewhat inflexible, cyber security model. This methodology, while robust in establishing a secure, controlled environment, inadvertently restricts the deployment of more dynamic, distributed technologies, such as cloud computing, which inherently defy traditional perimeter and device definitions, while bringing potentially industry-revolutionizing technologies.

NERC CIP's current audit limitations for accepting third-party evidence add further administrative and operational burden onto both the regulatory bodies and registered entities when exploring available new technology. This constraint fundamentally diverges from practices observed in alternative industry regulatory contexts. Notably, the Payment Card Industry Data Security Reliability Standard (PCI DSS)[6] often permits entities to leverage third-party attestations and certifications, such as those from cloud service providers, to substantiate compliance. This approach not only pragmatically reduces the audit scope for entities but also alleviates associated operational burdens by capitalizing on externally validated secure solutions.

Due to registered entities owning all responsibility for evidence in NERC CIP assessments, there is a perceived distinction between permissible consultative services, like threat intelligence or incident response consulting, and the restrained adoption of managed security services. This points toward a nuanced, yet impactful, limitation on technological enablement. MSSPs and MDR solutions inherently operate on architectures that often integrate cloud technologies and external management of data—components traditionally scrutinized or complexly navigated under NERC CIP. Whereas consultative services might provide advice or analysis without directly interacting with or managing an entity's security systems and data, MSSPs and MDR solutions are often embedded within an entity's technology and security operations, thereby requiring more operations-centric evidence under NERC CIP. While regulations like the Health Insurance Portability and Accountability Act (HIPAA) offer more flexibility by recognizing external audits and certifications to some extent, NERC's CIP Reliability Standards' current audit constraints do not generally accommodate third-party (to the registered entity) evidence validations, thereby limiting utilities' capacity to seamlessly integrate with the broader, constantly evolving technological and cyber security landscape. This effectively hampers the adoption of globally recognized, secure, and innovative ideas and solutions.

As the NERC CIP Reliability Standards continue to be revised from standards development projects due to emerging threats and new technologies and cyber security paradigms such as zero trust, the electric industry should endeavor to evaluate the Reliability Standards with a fresh perspective beyond the traditional adding of new requirements. While standards development efforts continue to raise the security baseline through additional and revised requirements, it must also be recognized when it is appropriate to retire and relax outdated requirements.[7]

[6] https://www.pcisecuritystandards.org/

[7] https://www.nerc.com/pa/Stand/Project%20200812%20Coordinate%20Interchange%20Standards%20DL/Paragraph_81_Criteria.pdf

Ultimately, striving for compliance should be about enhancing performance and reliability, making compliance a driving force for positive change rather than a mere obligation.

Standards Development Process and Field Tests

To foster technology innovation and adoption, the electric industry must be able to conduct proof-of-concept deployments that extend beyond alternative or simulated environments. While preliminary testing in controlled settings is essential, there comes a stage in the evaluation process when a technology is ready for a limited deployment within a live operational system. At this point, the industry should be empowered to pilot and trial new technologies in real-world environments across various regions. This approach enables exploration of practical use cases, comprehensive assessments of reliability and security impacts, and a deeper understanding of the regulatory challenges that may arise.

However, for these trials to be effective, a collaborative framework between the electric industry and regulatory bodies must be established. There must be an understood "safe" space to promote beneficial experimentation, learning, and the responsible integration of cutting-edge technologies while ensuring that security, reliability, and public safety are not compromised.

Under the NERC Rules of Procedure, a precedent exists in the way of field tests that offer potential opportunities for compliance waivers, as needed, to establish that "safe" regulatory space for the testing—however, there are limitations. The current standards development process lays out a process for initiating field tests but only through their relation to a standards development project and SAR.[8] The tie-in to standards development limits the benefit that this field test process offers to industry because new technologies are often found in a limbo state of compliance ambiguity or perceived non-auditability, resulting in no SAR submissions for years.

With no other formal and endorsed process for conducting "safe" pilots and trials for new technology in production environments, and when there is insufficient direction and guidance being produced by industry collaboration with the ERO Enterprise regarding a given new technology to facilitate secure and reliable early adoption, registered entities may be left with few if any options to explore an affected technology use case. In the case of compliance roadblocks, the result tends to be a drastically slowed to outright stifling of adoption, such as with cloud technology and real-time decision use of PMUs. In other cases, where an applied technology is out of scope, limitedly or non-applicable, or non-jurisdictional, outright proliferation—such as in inverter-based resources, DERs, and electric vehicle charging—is seen. It should be noted that the proliferating technologies are also predominantly integrated with cloud technology, underscoring regulations as the primary barrier for cloud technology adoption for in-scope NERC CIP systems.

[8] https://www.nerc.com/AboutNERC/RulesOfProcedure/Appendix_3A_SPM_Clean_Mar2019.pdf

Chapter 4: RETINA

When a significant interest emerges in exploring new technology, industry readiness often follows, prompting a willingness to trial the technology in real-world settings. SITES believes that, through carefully managed voluntary field trials, it is possible to cultivate awareness, align interests, endorse good practices, and, ultimately, establish a precedent for the secure and reliable application of new technologies. Breaking these trials away from the standards development and SAR process can allow for greater responsiveness to technology innovation and permit industry to lead and direct the adoption curve thoughtfully and intentionally. These trials, and the subsequent reports and guidance produced, may not only help cultivate industry knowledge around the security and reliability risks or benefits of a given technology but may additionally identify regulatory needs (leading to SARs) or inform ongoing standards development. This further allows standards development work to function more effectively as a leading indicator, rather than a lagging indicator, of reliability and security risk mitigation. Above all, such trials may empower industry to achieve swifter adoption of secure and reliable technologies by utilities, even in cases where it is found that standards development work may be needed.

SITES envisions Regional Entities as the vanguard of conducting and coordinating these voluntary field trials with each volunteer entity in their region due to their deep-rooted connections with local utilities, policymakers, and stakeholders, enabling tailored and responsive trials. Likewise, the U.S. Department of Energy (DOE), the National Laboratories, universities, and other research organizations would be invited to coordinate their own field trials. High-level oversight and organization of each technology field trial project is recommended to be initiated, as well as facilitated by NERC in collaboration with industry stakeholders, through committees and working groups under the RSTC (such as SITES). These committee-sponsored field trial project groups would work directly with individuals from the Regional Entities leading the trial effort within their respective region.

In addition to consideration for waivers or specialized audits, parameters such as duration, goals, number of volunteers, and specific volunteer requirements should be clearly defined early on. Initial planning of a field trial may set its broad parameters, and, on a given trial basis, the Regional Entities may be offered flexibility to tailor certain aspects of the trial scope for entities within their region, where the added regional diversity may offer valuable additional insights to the trial.

Presented as a high-level concept rather than a prescriptive process, these voluntary field trials represent an opportunity for the electric industry to proactively walk hand in hand with regulators to seek secure and reliable implementations of emerging technology—technology that our increasingly diverse and complex grid will become dependent on, whether we are proactive or not in guiding implementation. By proactively and collaboratively exploring new technologies with field trials, we can reduce grid reliability risk in edge-case experimentation while safeguarding the grid's operational integrity and increasing industry's agility and efficacy in ensuring technology innovation and adoption and supporting a more secure and reliable energy future. To summarize, the following measures are proposed to ensure the effective oversight and execution of technology field trials for industry:

- Field trial project structure: While the Regional Entities are seen as a focal point of coordination for trials, the recommended organization structure for project oversight is the following:
  - The structure can include NERC, a stakeholder subcommittee or working group under the RSTC, the Regional Entities (or DOE, National Laboratories, etc.), and registered entities.
  - Initiation: Field trials are first incorporated and assigned as potential work plan priorities under the RSTC then initiated by the subcommittee or working group owning the work item. There are no SAR requirements.
  - Developing scope: Fixed and/or flexible parameters for each field trial project, including duration, goals, minimum or maximum numbers of volunteers, and volunteer requirements, should be identified.

- Regulatory approvals, waivers, and audits: Alongside developing the initial scope, necessary ERO Enterprise approvals should be secured for trials that might impact current Reliability Standards and necessitate temporary compliance waivers or specialized audits. Where uncertainty exists for a given field trial project, define milestone events for potential re-evaluation of criteria for compliance needs.
- Data sharing and analysis: Clear protocols for the collection, sharing, and analysis of trial data should be established, maintaining the strict confidentiality of participating utilities’ information.

Chapter 5: Conclusion

The electric utility industry stands at an inflection point as modernization and digital transformation accelerate. New and innovative technologies promise to transform grid reliability, resilience, and security if adopted at scale. However, as this white paper outlines, significant barriers inhibit widespread technology innovation and adoption across the industry. Workforce challenges, financial limitations, rigid compliance approaches, and a standards development process not fully aligned with the pace of innovation all contribute to lagging technology uptake. Looking ahead, collaborative solutions are needed to overcome these obstacles and propel the industry forward. More active participation from utilities and vendors in the standards development process will be crucial. By engaging in technical committees and working groups, industry organizations can help guide Reliability Standards that embrace new technologies while enhancing the security baseline of the grid.

Further, initiatives like the proposed RETINA program offer a path to organize real-world technology trials, cultivate guidance, and establish precedents that enable faster adoption within a compliant framework. Ultimately, overcoming barriers to technology innovation and adoption will require commitment from leadership, flexible yet prudent compliance approaches, supportive regulatory structures, and synergistic collaboration between utilities, vendors, regulators, and other stakeholders. By working together through initiatives like RETINA, the electric industry can collaboratively strengthen the electric grid, optimize operations, and help ensure the reliable, resilient, and secure delivery of power.

Appendix A: Demoing New Technology

Utilities have a significant opportunity to explore and assess new technologies by establishing or utilizing dedicated lab and pre-production or even alternate production environments (e.g., corporate network). These settings allow for rigorous testing and simulation outside of compliance-impacted systems, minimizing risk while assessing potential benefits and impacts. By collaborating with entities, including other utilities, external labs, and universities, utilities can gain insights into how new technologies might integrate into their current systems, ensuring that innovations align with operational goals and regulatory requirements before full-scale implementation.

Vendors often provide opportunities for utilities to trial new technologies through proof-of-concept installations, sometimes at low cost or even for free. These trials allow utilities to evaluate the technology's effectiveness and integration capabilities within their existing infrastructure before committing to a full-scale deployment. Proof-of-concept deployments are a valuable way for utilities to assess potential solutions with minimal financial risk.

All of these share the same challenge, however, in that these alternate environments have an eventual limit to their ability to effectively emulate a real-world production system and field asset. Eventually, risk-calculated limited field trials in production are often necessary to fully test integration in real-world scenarios, which is crucial to ensuring that the desired outcome is achieved.

Roadblocks for Technology Innovation and Adoption

To better enable technological advancement for industry with the aim of furthering grid reliability, resilience, and security, the challenges and obstacles that are hindering the introduction and utilization of new technology must first be explored. Effectively, these factors can be understood as bottlenecks to advancing the overall technological state of the BPS. The major factors that are slowing or impeding innovation and the widespread adoption of these advancements—including internal compliance strategies and workforce, financing, and regulatory framework challenges—are explored below.

Workforce Acquisition and Retention

The acquisition and retention of a skilled workforce is a challenge in the electric utility sector, crucially influencing the rate and scope of technology adoption. These struggles are not isolated but are common across the industry. An awareness of these challenges often leads organizations, intentionally or not, to adopt a conservative approach toward technological advancement. This can range from settling for a lower level of technological maturity to an outright avoidance of significant technological changes. This issue is especially pronounced for smaller utilities that are frequently unable to access a diverse talent pool. The ability to implement and efficiently manage new technologies depends heavily on the presence of skilled professionals. These individuals need to be not only technically adept but also versatile in adapting to the ever-changing technological environment. A shortage of such expertise can severely delay the introduction of innovative solutions, undermining efficiency and the utility's competitive edge. The continual loss (i.e., lack of retention) of skilled workers can create a knowledge vacuum, further hindering the electric sector's capacity to keep up with technological progress. These scenarios may lead to outsourcing, leading to increased remote access and other consequences that may further aggravate financial, compliance, and risk concerns. Compounded by the attractiveness of new industries, the evolving nature of required skill sets, and a highly competitive job market, these workforce challenges significantly shape industry's approach to embracing and using new technologies. This cautious, sometimes reluctant, attitude toward technological change highlights a critical link between workforce dynamics and the sector's technological evolution. The difficulties of acquiring and retaining a skilled workforce include several factors, as follows:

- Lack of expertise: Smaller utilities often struggle to attract the necessary expertise, especially in specialized areas like operational technology (OT), combined security and engineering skill sets, and cloud technology. This scarcity of talent is exacerbated by the rapid pace of technological adoption and innovation, requiring skills that are not only current but also adaptable to evolving technologies.

- Technology and equipment: The presence of outdated or legacy equipment and architecture can deter talent, particularly those who are seeking to work with cutting-edge technologies. Skilled professionals may see jobs that support older technology as a risk to their careers. Given the pace at which technology advances, security and IT professionals are especially likely to view the electric industry, with its lagged technology adoption, as a poor fit for their need for continuing technology education and experience. This results in fewer numbers of professionals crossing from other industries and increased numbers of professionals fleeing the electric industry for more appealing jobs. This can be contrasted with messaging from forward-thinking utilities that have begun adopting these new technologies, marketing themselves as “technology companies that deliver electricity,” and coupling that with a mission to “green and save the planet.” This kind of thinking and messaging is attracting younger workers, who will only stay if the utility continues to live up to that mantra through ongoing technological evolution.
- Process maturity: The degree of process maturity within a company can impact the perception of that organization’s readiness to evolve and achieve a steady pace of technological advancement, thus also playing a crucial role in retaining talent.
- Pay and benefits: Offering competitive pay and having the available budget to invest in ongoing employee learning are generally regarded across most industries as attractive and essential benefits to retain skilled employees.
- Culture: Increasingly, the organizational culture of a utility plays a pivotal role in retaining talent. A positive and supportive work culture can significantly enhance employee satisfaction and loyalty, encompassing aspects such as inclusivity and diversity, open communication, recognition and growth opportunities, work-life balance, an innovation-friendly environment, and a focus on psychological safety and wellbeing.
- Travel, training, remote work: Factors such as inadequate training, limited travel, and poor flexibility options (including remote work capabilities) can all affect employee satisfaction and retention. Utilities should review these policies and associated budgets with an aim for flexibility.

Utilities have a few considerations to address these challenges, as follows:

- Leadership priority: Making workforce development a leadership priority is crucial. This involves recognizing the importance of skilled personnel in driving technological innovation and operational efficiency.
- Technology refresh cycles: Adopting more aggressive technology refresh cycles can attract talent interested in working with advanced and emerging technologies. Implementing external or bolt-on solutions like gateways, security monitoring, and reporting/analysis can help retain the return on investment on old/legacy equipment while appealing to tech-savvy professionals.
- Training offerings: Enhancing training offerings to include the latest technological and security trends can increase the value proposition for potential and current employees.
- Improving pay, benefits, and flexibility: Improving compensation packages, including better pay, benefits, and travel and flexible working options, can significantly boost both acquisition and retention of talent.
- Prioritize a positive organizational culture: Ensure culture has a place in the priorities of leadership strategy. Fostering an attractive culture impacts an organization’s reputation outside of its current workforce and serves to draw new talent in addition to helping the organization retain its key-performing employees.

Finance and Accounting

In the electric industry, navigating financial and budget-related challenges is crucial for adopting and implementing new technologies. Decisions around investments are significantly influenced by factors such as capital expenditure classification, monetary or financial regulatory policy, and funding opportunities and strategies. Described below are some key financial considerations that utilities should manage in order to innovate more effectively:

- CapEx vs. OpEx: Utilities earn a return on capital expenditures (CapEx) (physical assets) but not on operating expenses (OpEx) (like fuel and maintenance), thereby impacting much of the decision-making around implemented technology in the industry. Some utilities may find success in classifying on-premises IT infrastructure (like servers and telecommunications equipment) and even software (like EMS and supervisory control and data acquisition (SCADA)) as CapEx. However, opportunities to do so are often highly dependent on state public utility commissions (PUC) and other oversight policies. Technology that fails to be designed-in and added to larger capitalized projects is often relegated to OpEx, as is often the case with software and hardware dedicated to cyber-security, in addition to new technology initiatives. Additionally, cloud services, such as SaaS, are often considered OpEx, which can be a deterrent due to the lack of return on these expenditures. This classification can disincentivize moving to potentially more efficient cloud services due to utility industry-specific financial and regulatory structures.
- Licensing flexibility: Vendors sometimes reclassify their software to help utilities capitalize on expenses, turning what might typically be operational costs into capital expenditures. This can make new technologies more financially feasible by spreading out their costs over time as a depreciating asset.
- Government subsidies and incentives: Utilities may be able to leverage government subsidies and incentives for updating infrastructure, incorporating renewable energy, enhancing grid resilience, and investing in cyber security. For example, the Inflation Reduction Act and the Infrastructure Investment and Jobs Act in the United States provide significant funding for energy security, renewable resources, and electric vehicle infrastructure. This funding supports various aspects of energy technology development, from generation to consumption, offering utilities financial support for adopting new technologies.
- Innovation pilots and research and development funding: Exploring new technologies often requires upfront investment in research and development. Government research and development funding can support innovation trials, especially for technologies at a lower technical readiness level. This external funding source can be crucial, as utilities might struggle to justify these investments directly through revenues that are tightly regulated by PUCs.
- Partnerships and collaboration: Utilities can partner with other industry players, such as the National Laboratories, research institutions, universities, industry consortiums, and government agencies, to leverage collective knowledge, resources, and, potentially, funding opportunities. Such partnerships can help utilities access new technologies and share the financial risks and rewards associated with innovation.
- Risk management and assessment: Utilities must assess the financial risks of new technologies, considering factors like initial investment costs, potential operational disruptions, and long-term returns. Implementing a robust risk management framework helps in evaluating these technologies' viability, aligning them with the utility's financial health and strategic goals. This approach ensures that utilities can balance innovation with financial stability and risk management.
- Consumer-centric strategies: Utilities should focus on understanding and segmenting their customer base to tailor their services and communication strategies effectively. This understanding can help them invest in technologies that directly benefit their consumers, making it easier to justify these investments to regulators and stakeholders. Understanding the connection between a technology initiative and the value to the customer can aid in the development of strong business cases and enable more successful CapEx applications.

Relationship Between Innovation and Regulation

Within the electric sector, a significant challenge arises in the relationship between innovation and regulation, particularly regarding vendor-produced technologies. This challenge is rooted in the inherent lag between technological advancement and regulatory response, which often slows or limits innovation. Explored below are the various ways this challenge manifests:

- Compliance as a prerequisite for adoption: Without clear compliance precedent, utilities, especially those sensitive to compliance risk, hesitate to adopt innovative solutions. The common question from utilities is, “How will it meet compliance?”, underscoring the need for compliance assurance before widespread adoption can occur. This scenario restricts innovation to the confines of existing Reliability Standards.
- Resource disparity and risk appetite: Larger utilities with more extensive staffing and resources are better positioned to navigate and articulate internal controls and compliance issues in comparison to smaller, more resource-constrained utilities. The resource disparity influences the risk appetite of utilities, with larger utilities more likely to explore and adopt innovative solutions compared to their smaller counterparts. This places larger utilities, through their vendor relationships, in a more influential seat than their smaller counterparts to drive innovation in directions that suit their needs.
- Innovation-regulation gap: Innovation almost always precedes regulation, making it challenging for regulators to define Reliability Standards for technologies that have yet to be fully realized. In the absence of explicit regulations, vendors may interpret or press industry definitions to align with their solutions. Vendors often lack direct access to compliance decision makers and their opinions before deploying technology at client sites, further complicating the landscape.
- Software lifecycle: The focus on available patches, rather than addressing vulnerabilities and/or inherent risk due to broader software architecture problems, exemplifies another issue. Situations like the end of support for software (e.g., Windows XP) that will no longer receive new patches highlight the limitations of current approaches. Vendors find themselves pressured to maintain outdated technologies simply because they meet existing Reliability Standards even when new technologies might offer enhanced security, performance, and scalability.
- Hardware lifecycle: Operations technology in the electric sector often faces extended lifecycles, sometimes ranging from 10 to 30 years. This longevity can challenge vendors striving to integrate modern solutions, as the hardware in place may not support or fully utilize the advancements that they offer. The discrepancy between the rapid evolution of technology and the slow turnover of OT devices creates a scenario where innovations may be technically feasible but practically unimplementable, leading to a slower pace of technological adoption and potential missed opportunities for reliability and security enhancements.

Internal Compliance Strategies

The electric utility sector often perceives compliance as a barrier, especially when it comes to adopting new technologies. This perception can be influenced by the level of rigidity of a registered entity’s internal compliance approach, fear of financial repercussions, and the variability in flexibility among different Regional Entities. This is explored in finer detail below:

- New technology and prescriptive Reliability Standards: Appropriately, innovative technologies are rarely defined in prescriptive standards, such as in the NERC CIP Reliability Standards. However, this can lead to inconsistencies in adoption, as entities may fear falling out of compliance due to a lack of, or unclear, implementation or security guidelines available to industry or the perceived lack of endorsement and audit support for a given technology by the Regional Entities. A strong relationship with the Regional Entities is thus crucial for utilities to maintain a state of compliance while pursuing innovative technology adoption.
- Innovation vs. regulatory cycle: Utilities aiming to rapidly adopt new technologies might find themselves in a constant state of conflict with demands for internal compliance evidence and, ultimately, auditors. Major patches to key technologies, such as virtualization and remote access tools, can introduce entirely new feature sets and even completely rework the underlying technical workings of a system. Something as obvious as keeping technologies updated and patched, as required by vendors for support, can inadvertently place entities at odds with compliance expectations, leading to a cycle of continuous adjustment.

- New approaches to mitigating risks: Technological innovation can introduce novel risk mitigation strategies that may initially seem restricted by classic interpretations of requirements and evidence measures. For example, the shift from signature-based antivirus software to heuristic or ML-based systems for malicious code detection requires a re-evaluation of compliance approaches to accommodate these advancements, especially where cloud technology plays a role. The transition between awareness and understanding, whether a Reliability Standard is truly restrictive of a new technology or not, happens at different timescales for individual entities and the electric industry as a whole. Traditional networking transitioning to software-defined is another example, challenging traditional static documentation evidence measures in the presence of policy-driven ephemeral configurations and baselines. Reliability Standards Project 2016-02[9] is an example of an industry-wide effort that leads the way for these transitions, with ongoing standards development even aiding existing technology adoption before standards development is completed, such as with on-premises virtualization technologies, software-defined networking, and zero-trust architectures.

- Ambiguity and lack of guidance: The absence of clear guidance can slow innovation. Whether simply for awareness or input, compliance staff should proactively engage with industry committees, regulatory updates, and discussions. This way, compliance staff can stay informed, take advantage of available guidance, and facilitate more flexible compliance approaches. Small utilities, which outnumber larger utilities more than 10 to 1, suffer this burden on their staffing resources and compliance programs disproportionately.

- Compliance as a foundation, not an end goal: Compliance should not be the ultimate goal but part of the overall security program. It should set the foundation for operational teams that can be built upon to achieve the risk-reduction objectives of the organization. Active participation in standard development teams, committees, and industry working groups like SITES is crucial for utilities to ensure that proposed Reliability Standards support their innovation roadmaps. This participation and interaction are the foundation of our self-regulated industry.

- Beyond minimal compliance: Aiming for mere compliance can lead to complacency. The threat actor groups targeting the grid are ever evolving, unencumbered by compliance, and never complacent. Therefore, it must be ensured that utilities are enabled to be appropriately nimble in the adoption of new technology toward securing the grid. Utilities should strive for overarching security where compliance is a component, not the entirety. Compliance is not security, and security is not compliance. The NERC CIP Reliability Standards should be viewed by industry as a minimum baseline, not a constraint on innovation nor a replacement for registered entities performing independent security risk assessments.

While compliance is necessary to establish the basics for safe and reliable operation of the electric grid, the advised approach is one that encourages innovation and flexibility. Utilities need to actively engage in the regulatory process and advocate for Reliability Standards that support technological advancements while maintaining grid reliability, resilience, and security. Additional recommendations to promote a more mature and flexible culture of compliance are provided as follows:

- Aim to be risk-adverse, rather than change-adverse.

- When evaluating new technology without existing available guidance, consider engaging regulatory bodies and auditors upfront.

- Improve awareness of available regulatory guidance papers. More knowledge creates more options.

- Toward cultivating a culture of compliance internally within an organization, create a safe and mutually beneficial space for both internal disclosure of compliance risks, and new technology adoption.

- Seek mock audits from outside consultants or regional entities after initial implementation of new technology.

[9] https://www.nerc.com/pa/Stand/pages/project%202016-02%20modifications%20to%20cip%20standards.aspx

Lessons from Alternative Regulatory Frameworks

In gauging the effectiveness and impact of Reliability Standards like NERC CIP, a comparative lens aimed at alternative frameworks and industries could be enlightening as the other reliability standards could offer insight into the symbiosis between technology enablement and regulatory landscapes. The PCI DSS and reliability standards applied in diverse sectors like insurance and safety present a spectrum of methodologies and outcomes concerning technology adoption and security governance. Various reliability standards embody different approaches and imperatives, potentially shaping and constraining technology adoption in distinct manners. The non-mandatory and non-enforceable nature of certain frameworks, unlike NERC CIP, might pave the way for a more flexible, albeit less controlled, technological adoption trajectory. Understanding how these alternative models influence technology enablement, risk management, and operational consistency across different sectors may unlock valuable insights.

Assessment of PCI DSS

The PCI DSS navigates a carefully structured, highly prescriptive path to ensure secure handling of cardholder information, stipulating explicit security protocols that, while bolstering a uniform cyber security posture across adherents, potentially impose constraints on expedient technological innovation and adoption. Such specific and articulated guidelines ensure a clear, auditable compliance trajectory but may inadvertently anchor organizations to established, certified technologies, potentially inhibiting exploration into emerging solutions. The Payment Card Industry Security Standards Council’s practice of validating specific vendors and products, effectively greenlighting them for use, has merit and risks. The certification and validation of specific products and vendors does provide entities with a clearer, predefined path toward compliance. The prescriptive nature and clear delineations within the PCI DSS serve to eliminate ambiguity regarding compliant technologies and practices, which can be especially advantageous for entities with limited cyber security expertise or resources. This approach to validation also fosters a degree of uniformity in security postures across entities, ensuring that baseline cyber security protocols are consistently upheld across the payment card industry. However, the downside surfaces in some potential stifling of innovation, as the explicit guidelines and rigid adherence to validated technologies might inhibit the exploration and adoption of emerging, potentially superior, technologies that have yet to be validated by the council. Finally, there is a bureaucratic element that potentially creates a lag between technological advancements and their subsequent validation and approval for use within the PCI DSS framework, presenting an inadvertent obstacle to immediate adoption.

Assessment of HIPAA

HIPAA ensures that protected health information (PHI) is secured through adherence to a set of administrative, physical, and technical safeguards. Noteworthy is its comparatively less prescriptive stance toward compliance, which enables healthcare entities to employ a variety of technological solutions as long as the foundational objective—safeguarding PHI—is met. This intentional flexibility, while fostering an environment conducive to technological innovation and adaptation, presents a potential drawback in the form of varied compliance interpretations and implementations across entities. Given HIPAA’s merging of both prescriptive and flexible elements, there is an implied security risk of inconsistency in technology implementation strategies across entities in the healthcare sector. Entities may engage with new technologies and innovate under the flexible aspects of HIPAA, potentially advancing the overall cyber security posture of the healthcare sector. However, without a centralized and standardized validation mechanism or clear-cut technological guidelines, entities with limited cyber security expertise might inadvertently integrate technologies that inadequately safeguard PHI, thereby elevating the sector’s susceptibility to cyber threats and data breaches. The industry, while potentially benefiting from more rapid technology adoption, may also contend with disparities in cyber security efficacy and resilience across different entities, pivoting the risk landscape toward a scenario where the security of PHI may be as strong or as weak as the most innovative or change-adverse entity, respectively. This dichotomy inherently creates an environment where technological innovation and adoption must be meticulously balanced with rigorous internal risk assessments and cyber security expertise to safeguard against the unintended elevation of cyber security threats within the healthcare sector.

Assessment of Sarbanes–Oxley Act

The Sarbanes–Oxley Act (SOX), centered around financial integrity, delivers guidelines without delving into technical cyber security specifications. This regulatory framework, while emphasizing financial accuracy, does not stipulate a detailed technological roadmap, potentially allowing entities to explore innovative financial or cyber security technologies freely. However, this general approach may also induce challenges where organizations, in ensuring compliance, could opt for established, proven technologies, potentially circumventing innovative but unvetted solutions. The resulting cyber security strategy, while adherent to SOX's overarching mandate, may navigate a path that, due to its inherent ambiguity, fosters a cautious, and potentially innovation-limiting, approach to technology adoption. Viewed in the lens of the electric industry in contrast, however, staple technologies are seen as appropriate, where the risk to adopting a technology with uncertain reliability or security impacts trumps achieving a competitive edge.

Assessment of Criminal Justice Information Services

The Criminal Justice Information Services (CJIS), crafted to safeguard sensitive criminal justice information, exhibits a distinctive blend of flexibility and precision in its policy framework, designed to accommodate the varied technological and operational contexts of diverse law enforcement entities. The policy delineates clear security controls but leaves room for entities to select and implement technologies that align with these mandates. These policies potentially foster an environment conducive to technology exploration and adoption. However, the very flexibility that allows for technological exploration can, paradoxically, render the compliance validation process somewhat ambiguous, particularly when considering innovative solutions that may not have a clear precedent in the CJIS context. This framework might oscillate between being an enabler and an inhibitor when it comes to technology adoption and innovation within the realm of law enforcement and related entities. The strategy of not binding entities to specific technologies or vendors implies that law enforcement agencies could, in theory, explore and integrate innovative technological solutions, provided they meet CJIS security controls. Conversely, ensuring that new and innovative technologies comply with CJIS's stipulations may prove resource-intensive and complex, particularly for smaller entities or those with limited cyber security expertise. Consequently, while CJIS provides a robust and flexible framework for safeguarding criminal justice information, its inherent complexity and the requisite resources for ensuring compliance might potentially curtail rapid technology adoption and innovation to a certain extent.

Appendix B: Contributors

SITES would like to thank the following individuals for their contributions to the development of this white paper:

- Larry Collier
- Lew Folkerth
- Dan Goodlett
- John Graminski
- Tom Hofstetter
- Kristine Martz
- Karl Perman
- Thomas Peterson
- Ryan Quint
- John Skeath
- Matthew J. Yourek
- Song Zhang