The Challenges and Opportunities with Cybersecurity Regulations: A Case Study of the US Electric Power Sector

Sena Sahin
Georgia Institute of Technology
Atlanta, Georgia, USA
ssahin8@gatech.edu

Burak Sahin
Georgia Institute of Technology
Atlanta, Georgia, USA
buraksahin@gatech.edu

Robin Berthier
Dragos
Chicago, Illinois, USA
rberthier@dragos.com

Kate Davis
Texas A&M University
College Station, Texas, USA
katedavis@tamu.edu

Saman Zonouz
Georgia Institute of Technology
Atlanta, Georgia, USA
szonouz6@gatech.edu

Frank Li
Georgia Institute of Technology
Atlanta, Georgia, USA
frankli@gatech.edu

Abstract

In various industries, cybersecurity regulations have been enacted in an effort to drive improvements to organizational security postures. Despite the prominent influence of these regulations, there has been limited prior investigation of how organizations engage with these regulations and the challenges that they face. Assessing these factors is vital for understanding the impact of cybersecurity regulations in practice and how to enhance them moving forward.

In this paper, we take a step towards filling this gap by investigating in depth the mature cybersecurity standard regulating the US electric power industry, NERC CIP (North American Electric Reliability Corporation Critical Infrastructure Protection), mandatory across the industry for the past 15 years. Seeking to improve this existing regulation, we assess the challenges with how this regulation is developed, adopted, and audited, and provide directions for improvement. Given the human-centric nature of regulation compliance, we do so by conducting in-depth semi-structured interviews with a diverse set of industry professionals who have direct experience with the regulation. While this standard is specific to the US energy sector, the challenges and insights uncovered through this qualitative exploration have broader lessons on how regulatory frameworks shape the security of various other industries. Our study reveals varied issues that can arise with a cybersecurity regulation, such as with the standard's specificity, burdensome compliance documentation, auditing subjectivity and inconsistency, and development processes that result in outdated guidelines. These findings in turn shed light on promising directions for policymakers, industry stakeholders, and regulatory bodies to improve cybersecurity regulations and their compliance.

CCS Concepts

• **Security and privacy → Usability in security and privacy**; • **Social and professional topics → Governmental regulations**; • **Hardware → Power and energy**.

CCS '25, Taipei, Taiwan

ACM ISBN 979-8-4007-1525-9/2025/10
https://doi.org/10.1145/3719027.3765184

Keywords

Compliance; Audit; Standard Development; Critical Infrastructure Security; Cybersecurity Regulations; User Study; Interviews

ACM Reference Format:
Sena Sahin, Burak Sahin, Robin Berthier, Kate Davis, Saman Zonouz, and Frank Li. 2025. The Challenges and Opportunities with Cybersecurity Regulations: A Case Study of the US Electric Power Sector. In *Proceedings of the 2025 ACM SIGSAC Conference on Computer and Communications Security (CCS '25), October 13–17, 2025, Taipei, Taiwan.* ACM, New York, NY, USA, 15 pages. https://doi.org/10.1145/3719027.3765184

1 Introduction

Across various industries, from finance to health to critical infrastructure, cybersecurity regulations have been enacted that prescribe how organizations should manage security and privacy. While there may be debate about whether such regulations ultimately lead to net positive improvements in an organization's security posture, what is clear is that these standards heavily impact organizational decisions, including how organizations approach risk management, allocate resources, and implement security policies.

Despite the significant role that regulations play in organizational security operations, there has been limited investigation of how organizations engage with regulatory requirements and the challenges they face. Prior studies have studied such regulations, focusing on specific aspects such as what organizations do to complement compliance mandates [58] and assessing the requirements themselves [57]. However, prior work has not examined the regulatory lifecycle holistically—from standards development to implementation and auditing—missing the interconnections and challenges that span across these stages. A fragmented view of any single stage may overlook upstream or downstream issues that influence compliance in practice. Understanding the full lifecycle is essential for identifying opportunities to enhance regulations and their compliance moving forward.

In this work, we take a step towards filling this gap through a case study deeply investigating the challenges faced by the stakeholders involved with a prominent cybersecurity regulation: NERC CIP (North American Electric Reliability Corporation Critical Infrastructure Protection) [42]. We focus on this particular standard as: 1) it regulates the cybersecurity operations of the entire US electric power sector, a nearly $500 billion industry [67] that the US government considers a critical infrastructure sector [16] due

to society's heavy dependence on its continued operation, and 2) it is a mature regulation, having been *mandatory* across the industry for the past 15 years [44]. Despite centering our study on a specific standard, we explore generalizable properties and challenges of cybersecurity regulations, to synthesize insights and lessons that can apply to such regulations broadly across other contexts.

Note that power utilities widely acknowledged the importance of regulatory requirements, seeing it essential to provide baseline security to critical infrastructures [37, 54]. However, challenges related to it are widely discussed within the industry [5, 47, 53]. In this paper, we examine issues that arise throughout the entire lifecycle of regulation compliance, from the standard's development to its implementation to auditing, to identify constructive improvements. Our research aims to answer four primary questions aligning with those lifecycle stages:

RQ1. What are the main challenges in implementing and complying with NERC CIP standards?

RQ2. What are the main challenges in auditing processes of NERC CIP standards?

RQ3. What are the main challenges in the NERC CIP standards development process?

RQ4. What improvements can be made to implementation, auditing, and development of NERC CIP standards to enhance efficacy?

Given the human-centric nature of the regulation lifecycle, we conduct our evaluation through in-depth semi-structured interviews with industry professionals who have directly engaged with the regulation. Our participants span diverse roles across all three lifecycle stages, affording a holistic investigation.

Our qualitative analysis uncovers significant challenges throughout a regulation's development, implementation, and auditing. During development, we identify process constraints that result in requirements that lag modern needs or cater to a subset of stakeholders. Implementation challenges include issues interpreting regulatory requirements as well as significant overhead required for proving compliance. Meanwhile, audits can engender substantial friction between regulatory stakeholders, especially due to subjectivity, inconsistency, and conflict of interest during the audit process. From these difficulties, as well as suggestions on improvements by our participants, we identify directions for enhancing regulatory requirements and compliance.

Ultimately, our study offers a systematic investigation into the challenges encountered when engaging with a particularly impactful cybersecurity regulation. Through this analysis, we provide concrete, stakeholder-informed recommendations for improving cybersecurity regulations more broadly. As NERC CIP serves as a foundational framework for grid cybersecurity, our work is motivated to further improve it. We emphasize targeted refinements—many drawn directly from practitioner experience—that can strengthen implementation and auditing while preserving the standard's core intent. Our goal is to guide regulators and utilities toward feasible, actionable enhancements and to advance the role of cybersecurity regulations in shaping operational security.

2 Background on NERC CIP

The North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards [42] are a set of mandatory cybersecurity regulations that aim to secure the Bulk Electric System (BES) in North America. Originally established as a voluntary organization following the 1965 Northeast blackout in the United States [44], NERC was later empowered by the U.S. Energy Policy Act of 2005 to develop enforceable reliability and security standards. These standards became mandatory in 2008 and are enforced through oversight by regional entities and penalties for non-compliance.

NERC CIP consists of 14 interrelated standards (CIP-002 through CIP-015), each targeting different aspects of cybersecurity and physical protection. The scope of these standards ranges from identifying and categorizing critical cyber assets (CIP-002), to personnel training (CIP-004), perimeter security (CIP-005), system security management (CIP-007), incident response (CIP-008), configuration change management (CIP-010), and supply chain risk management (CIP-013). For example, CIP-005 governs network security perimeters and access control for systems that communicate externally, while CIP-007 mandates patch management, antivirus protections, and logging for devices. These standards collectively define baseline security expectations for utilities operating within the BES.

Importantly, NERC CIP is tailored to operational technology (OT) environments, where cybersecurity must address both digital systems and the physical infrastructure they control. Unlike traditional IT systems, OT environments involve real-time control of industrial processes, making the consequences of a cyber compromise potentially catastrophic [62]. OT cybersecurity involves a hybrid of physical safeguards (e.g., access to control centers) and digital measures (e.g., authentication), adding layers of complexity to implementation and compliance [66].

Oversight of the CIP standards is an ongoing and iterative process. FERC (Federal Energy Regulatory Commission) plays a critical role by reviewing and approving NERC-proposed standards, issuing directives, and occasionally mandating revisions in response to national security concerns or lessons from cybersecurity incidents. This governance structure enables regulatory adaptation while preserving industry participation through NERC's standards development process. However, the regulatory framework reflects a consensus-driven model, which may result in incremental rather than rapid changes to address emerging risks.

The NERC CIP lifecycle comprises three main stages, as illustrated in Figure 1: compliance, auditing, and standards development. Compliance involves utilities interpreting and implementing the standards, maintaining documentation, and reporting qualifying cybersecurity incidents. Auditing encompasses the preparation for and execution of compliance assessments by regional entities. Standards development is an industry-driven process through which NERC proposes updates to FERC for approval. This paper examines stakeholder challenges across these stages and offers insights to improve regulatory implementation and policy effectiveness for implementers, auditors, and standards drafters alike.

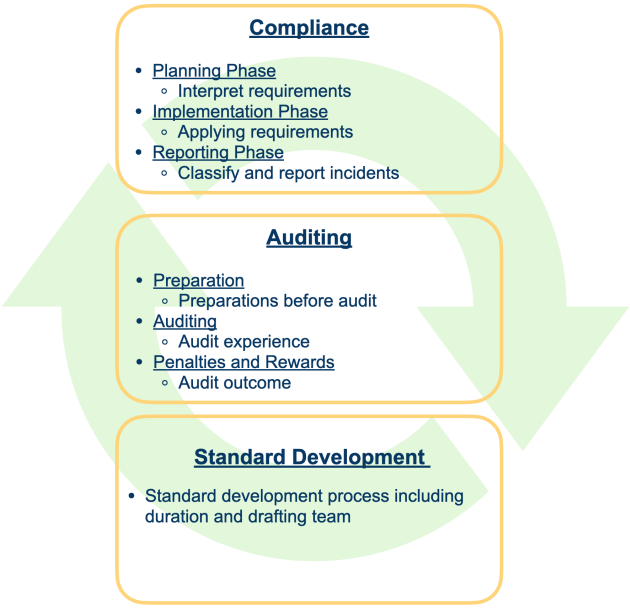

Figure 1: The NERC CIP lifecycle examined through our study.

3 Related Work

Here, we provide an overview of prior work related to our study, including those applying similar study methods or investigating similar topics (particularly cybersecurity regulations).

User Studies of Cybersecurity Professionals. Recently, security researchers have increasingly studied the experiences and perspectives of cybersecurity professionals. For instance, Armstrong et al. and others [3, 7, 8, 22] explored expert views on cybersecurity challenges and the role of knowledge in overcoming them. Similarly, Ion et al. and others [33, 39, 61, 63] examined the perception and implementation of security practices across sectors, while Votipkat et al. and others [71, 72, 75] studied the behaviors and skills of hackers and security experts. These works highlight ways to enhance cybersecurity experts' management of security and privacy tasks.

Investigating the Security of Critical Infrastructures Previous research has focused on the security of critical infrastructures, highlighting their vulnerability to cyber-attacks and the role of human factors. For example, Singer et al. [55] and Gallardo et al. [26] examined the perspectives of professionals in the electric power grid sector. Singer et al. [55] explored potential attack vectors and the outcomes resulting from incorrect grid modeling, while Gallardo et al. [26] explored how differing motivations and skills of computer security and energy operations professionals influence grid management. Their findings emphasized the value of collaboration between these professionals to enhance grid security. However, they do not specifically consider the integration and impact of regulatory standards like NERC CIP, which is the focus of our study.

Role of Cybersecurity Regulations. Several recent studies have specifically investigated the role that cybersecurity standards and guidelines play in security operations. For example, Stevens et al. [59] analyzed the NIST playbook for incident response, offering practical guidelines for organizations to prepare for, respond to, and recover from cybersecurity incidents.

Stevens et al. [57] manually analyzed the requirements from three cybersecurity standards, finding 148 potential issues. They confirmed 49 of these through consultations with industry experts. This study focused on auditing the standards' requirements, rather than how stakeholders engage with the requirements in practice. The most closely related study to our work is by Stevens et al. [58], which investigates additional steps organizations take to enhance security beyond compliance. They identify challenges faced by organizations across six sectors, including education and IT, as they aim to exceed basic compliance requirements.

Fischer et al. [24] explored the challenges of standardizing and adopting cryptography. They highlighted how cumbersome standardization processes discourage implementer participation and slow progress. They discuss conflicting interests among stakeholders, including corporate and governmental pressures, which can compromise security outcomes. Additionally, the lack of investment in standard development creates flaws and adoption barriers, while communication gaps between academics and engineers lead to misunderstandings and vulnerabilities. Overall, prior studies have provided valuable insights into cybersecurity regulations. However, our study expands upon this literature by investigating the standards compliance lifecycle holistically, identifying the challenges at each stage, grounded in the experiences and perspectives of stakeholders who have extensively engaged with a standard.

IT Security Certifications. Prior research highlights the role of IT security certifications—both organizational (e.g., ISO/IEC 27001) and individual (e.g., CISSP)—in enhancing cybersecurity posture and governance. ISO/IEC 27001 has been shown to improve risk management, regulatory compliance, and strategic alignment with business goals [34, 49]. Folorunso et al.[25] confirm these benefits but also note the challenges of resource demands and ongoing maintenance. Certifications contribute to professional development and compliance readiness when embedded in organizational learning structures [74]. Still, researchers warn against over-reliance on checklist-style compliance, advocating for more adaptive, human-centric security practices [38, 77]. Overall, certifications offer a foundational framework, but their effectiveness depends on sustained integration with evolving threats and organizational capabilities.

Evaluations of NERC CIP. Several studies have examined the effectiveness of NERC CIP standards in enhancing cybersecurity for the U.S. power grid. Ginsberg et al. [15] provided a foundational analysis, finding that NERC CIP standards mitigated many cyber risks, improved grid preparedness, and provided baseline security to energy grids. Ladendorff et al. [36] supported the view that CIP standards have fostered a baseline security culture across utilities, with improved procedural controls and heightened awareness. However, critiques persisted around the tendency for organizations to treat CIP as a "check-the-box" compliance exercise, potentially diverting attention from more proactive risk reduction efforts [45]. The implementation process of CIP, described as a co-production between regulators and industry stakeholders, helped bridge the IT-OT divide, but tensions remain between security mandates and operational feasibility [56]. Overall, the literature acknowledged that CIP has brought awareness and baseline security practices, but emphasizes the need for improvements in the standards. In this

study, we examined how the framework could be further improved, focusing on challenges and gaps based on firsthand experiences of those engaged in compliance, auditing, and implementation.

4 Methodology

NERC CIP is a well-known, well-established, and mature cybersecurity standard as discussed Sections 1 and 2, and its importance on security is acknowledged by our participants (in Section 5). Thus, in this study, we explore the challenges experienced by stakeholders throughout the lifecycle of regulatory compliance to uncover potential areas for improvement in standard development, standard understanding and implementation, and the associated audit processes to enhance regulatory compliance. Our research focuses on four primary research questions listed in Section 1.

To address research questions, we conducted a qualitative study involving professionals in the power sector who have directly audited, implemented, or developed standards. Our study included semi-structured interviews with 22 professionals. The interview structure remained unchanged throughout the interviews. Each participant's interview questions were tailored (removing irrelevant questions based on participants' roles/experiences) to their specific expertise, ensuring relevance and depth. This approach ensured consistency across all interviews. Our findings allowed us to identify weaknesses in the standards and insights into potential improvements to the compliance process in practice.

4.1 Recruitment

Recruiting security-related professionals for qualitative studies is challenging, as noted in prior work [60, 64]. Our study required participants with real-world experience in power utilities, specifically those who have directly audited, implemented, or developed standards. Consequently, our pool of prospective study candidates was a small subset of energy sector professionals. Participants must also be at least 18 years old and reside in the United States.

To recruit such professionals, we created advertisement posters and text blurbs providing information about our study and its goals. From May 2024 through July 2024, we distributed the posters and blurbs through a diverse set of communication channels, including LinkedIn and several emailing groups serving power grid administrators. Finally, we reached out through personal social networks. For anyone we engaged with during the recruiting process, including those who did not ultimately participate in our study, we employed snowball sampling [28] by requesting that they share our study information with others who may be relevant. Through our recruiting effort, we interviewed 22 professionals. This sample size is commensurate with similar qualitative studies of administrators, developers, and other specialized populations [9, 11, 12, 14, 32, 50, 52, 65]. Our analysis reached thematic saturation after the 14th interview, indicating that our data collection was appropriately scaled.

Compensation. Offering monetary compensation to research participants is ethically complex and context-dependent. While it is important to acknowledge participants' time and effort, ethical principles like Respect for Persons emphasize voluntary participation free from coercion. In high-income populations, offering substantial incentives may attract those primarily motivated by money, potentially skewing the sample. For these groups, omitting monetary compensation can encourage participation driven by intrinsic motivation or altruism, which may enhance data quality. Many studies [1, 2, 19, 20, 27, 29–31, 52, 70] have relied on such motivations. Nonetheless, researchers should still recognize contributions through non-monetary means, such as reimbursing expenses, sharing results, or formally acknowledging participation. In this study, we honored participants' time and insights by sharing our findings, but no monetary compensation was offered.

Pilot Participants. To evaluate the quality and clarity of our interview guide(Section 4.2), we initially conducted a pilot study with our first three participants. During this phase, we closely monitored the relevance and consistency of participant responses and actively solicited feedback on the structure and flow of our questions. After the pilot, we made minor adjustments to the protocol by removing a few redundant questions. However, the core structure, content, and intended insights of the interview guide remained intact. The final protocol was used for all subsequent interviews. As the pilot data aligned with the revised guide and mirrored later responses, we included pilot participants in the final study sample.

4.2 Semi-Structured Interview

We conducted semi-structured interviews with individuals who worked in the energy sector to discuss their experiences implementing, auditing, or developing the standards. To address our first research question (**RQ1**), we asked participants about how they handle compliance and challenges at each of the following stages: 1) Planning Phase, 2) Implementation Phase, 3) Incident Reporting, and 4) Improvement Suggestions. For our second research question (**RQ2**), we inquired about participants' experiences with the NERC CIP audit process, including: 1) Audit Preparation, 2) Auditing, 3) Penalties & Rewards, 4) Improvement suggestions. For our third research question (**RQ3**), we examined participants' experiences with the standards development process, including: 1) Standards development process, 2) Improvement suggestions.

The interview guide consisted of 22 potential questions (available at [51]). As our interviews were semi-structured, the interviewer adjusted the questions asked and made follow-up inquiries as necessary. To minimize organizational bias, we designed the interview questions to focus on participants' professional experiences rather than on their specific organizations. We explicitly encouraged participants to reflect on their personal expertise across roles—including implementation, auditing, and particularly standard development, where many participants had served in multiple capacities. From May 2024 to July 2024, we conducted interviews with 22 suitable participants. (As discussed in Section 4.1, we used the first three participants for a pilot study, and included their collected data as we did not identify consequential changes to our study instruments.) One researcher conducted all interviews for consistency. The interviews were conducted and recorded using an online video conference platform, lasting an hour on average.

4.3 Data Analysis

We transcribed all recorded interviews and analyzed the data using inductive thematic analysis [13]. First, coders read the interviews to get familiar with the data. Then, for each section of the interview,

ID	Edu.	Yrs.	Auditor	Impl.	Conslt.	Drafter
P1	Ph.D.	10	-	-	✓	✓
P2	M.S.	13	-	✓	-	✓
P3	M.S.	17	✓	✓	-	✓
P4	A.S	15	-	✓	-	-
P5	B.S.	15	-	✓	-	✓
P6	A.S.	20	-	-	✓	-
P7	M.S.	15	✓	✓	-	✓
P8	M.S.	10	-	✓	-	-
P9	M.S.	15	-	✓	-	✓
P10	M.S.	11	-	✓	✓	-
P11	B.S.	10	-	✓	-	-
P12	M.S.	13	✓	✓	-	-
P13	A.S.	20	-	✓	✓	✓
P14	Ph.D.	20	✓	-	✓	✓
P15	Ph.D.	5	-	✓	-	-
P16	M.S.	18	✓	✓	✓	✓
P17	M.S.	21	-	✓	✓	-
P18	A.S.	15	✓	✓	-	✓
P19	M.S.	12	-	✓	✓	-
P20	A.S.	16	-	✓	-	✓
P21	M.S	20	✓	✓	✓	-
P22	A.S.	17	✓	✓	✓	-

Table 1: Summary of participant demographics. All were male except P13. All participants had primary roles related to NERC CIP, falling into four groups: 1. Auditors, 2. Implementers (Impl), 3. Consultants (Conslt), and 4. Standard Drafters (Drafter). (Yrs = Years of Experience with NERC CIP)

two researchers independently developed a set of codes across participant responses and met to finalize a codebook. Both researchers then independently coded all participant responses using the finalized codebook (available at [51]). To evaluate the consistency of the coding process, we calculated the Kupper-Hafner inter-rater reliability scores [35] (other scoring calculations are less suitable when multiple codes are assigned per response [6]), finding an average agreement of 0.91, indicative of highly consistent coding. The two researchers then converged on the final codes for each response. Finally, coders generate initial themes, which are the central organizing concepts. Our diverse research team spans Cyber-Physical Systems (CPS), CPS security, and usable security, met to discuss disagreements and ensure alignment with the resulting themes. This interdisciplinary expertise allowed us to analyze regulatory challenges both from a technical standpoint and a human-centered viewpoint while generating themes. In Sections 5 to 7, we list the primary themes identified with bolded paragraph labels.

4.4 Participants

Our study consists of 22 U.S.-based participants, all of whom held primary roles directly tied to the NERC CIP cybersecurity lifecycle. Recruitment focused specifically on stakeholders with firsthand expertise in at least one of three key lifecycle stages: standards development, implementation, or auditing. This targeted recruitment ensured that all participants were qualified to speak to the practical realities of power grid cybersecurity under NERC CIP.

Participants were categorized into four main role groups: *(1) Standards Drafters (Drafter)*, who are involved in drafting NERC CIP standards and requirements; *(2) Auditors (Audt)*, who assess compliance at utilities through documentation reviews, site visits, and interviews; *(3) Implementers (Impl)*, typically utility personnel responsible for interpreting and applying CIP requirements within operational environments; and *(4) Consultants (Conslt)*, who advise utilities on how to achieve and demonstrate compliance. Role abbreviations are used throughout the paper, particularly to indicate the participants' roles in the Sections 5 to 7.

Recruitment efforts were primarily focused on U.S. stakeholders due to the research team's stronger professional network within the U.S. energy sector, which enabled more direct access to qualified participants familiar with NERC CIP. Our sample is male-dominated, with only one female participant, a distribution that reflects the broader structural gender imbalance in the energy and industrial control systems sectors. Female electrical engineers and electricians represent 3.75% and 2.16% of the workforce respectively [73]. While gender diversity remains a challenge across the field, this imbalance also influenced our participant demographics. All participants had some level of higher education: 6 held associate degrees, 2 had bachelor's degrees, and 14 had graduate degrees. On average, participants had 15 years of experience working with standards, with a range of 5 to 21 years. Table 1 provides an overview of participant demographics and professional backgrounds.

4.5 Limitations

Like many interview-based qualitative studies, our research has inherent limitations, including the potential for social desirability bias—participants may present responses they think are socially acceptable due to the sensitive nature of security and privacy topics. To address this, we implemented several mitigation strategies: assuring participants of the anonymity of their input, fostering a neutral and supportive interview atmosphere, and clarifying that all perspectives on regulatory standards—whether positive or negative—were equally welcome. These approaches aimed to promote honest and genuine responses.

Participants were primarily recruited through purposive sampling, drawing from professional networks within the energy sector, resulting in a sample mainly composed of U.S.-based professionals. This may limit the applicability of our findings to international contexts. Additionally, the participant pool was predominantly male, despite efforts to include individuals with varying levels of education and experience. While this limitation impacts the generalizability of our findings, it is suitable for our study's exploratory objectives. Future investigations could benefit from expanding to more diverse and international populations, possibly integrating larger-scale quantitative analysis.

While our sample includes broad representation across all roles involved in compliance, the majority of participants have stronger implementer experience, which may skew the findings toward the implementers' perspective.

Participants were not financially compensated. We discussed our decision influences in Section 4.1 under the Compensation subtitle. As a benefit to our participants, we shared our findings with them.

Finally, recruitment presented some challenges due to the targeted nature of the participant group, focusing on industry experts involved in cybersecurity compliance and standards development. While the sample size was sufficient to reach thematic saturation, enabling robust qualitative analysis, the findings should be interpreted as illustrative rather than representative of broader population trends. Similar studies focusing on administrators have also been conducted with comparable sample sizes [9, 11, 12, 14, 32, 50, 52, 65].

4.6 Ethical Considerations

Our study was approved by our university's Institutional Review Board (IRB). We obtained consent for the study and informed participants that they need not answer questions they were not comfortable with and could halt participation at any time. We also informed the participants and obtained approval to record the interviews. Our regulations require data and research records to be stored for a minimum of three years. All collected data was anonymized and stored securely, with access restricted to our research team.

5 Compliance

Note that our questions allowed participants to identify challenges related to standards only if they experienced them. All of our participants acknowledged the importance of regulatory standards and how those standards provide the baseline security for the energy sector. P19 (Impl, Conslt) emphasized the value of these standards by saying *"Look at NERC CIP, it is the best of what is out there. Even in the face of some other people complaining about it, it is something that at least gives you a place to start from. And that is what NERC says; it is a baseline for security."*

In this section, we explore our first research question on the main challenges in implementing and complying with cybersecurity standards. Specifically, we examine issues across three key phases: planning (understanding and interpreting standards), implementation (applying requirements), and reporting (detecting and documenting compromise attempts). Lastly, we present participants' suggestions for improvement. When we asked our interview questions, some participants indicated no issues related to the standards for different questions. For example, when we asked P1 whether industry people think any part of the standards is counterproductive or unnecessary, P1 (Conslt, Drafter) stated *"Not really. I think that they are useful. I think they are a good starting point."*, suggesting that our framing did not force problem identification. Our interview study focused on constructively exploring NERC CIP challenges to improve it.

5.1 Planning Phase

As a first step, utilities understand the requirements of the standards. This section delves into the challenges faced during this phase, highlighting key themes identified from participant interviews.

Prescriptive Standards Are Helpful but Can Hinder Flexibility and Security. Prescriptive standards are detailed, specific requirements that outline exactly how to perform a task or achieve compliance [23]. The majority of the participants (N=19) consider most of the standards very prescriptive. For example, P5 (Impl, Drafter) said *"It is the most prescriptive, most comprehensive, highly regulated standard in the world."* Prescriptiveness is necessary to ensure utilities and auditors understand the requirements correctly, according to 8 participants. For example, P18 (Audt, Impl, Drafter) highlighted that the prescriptive nature of standards is essential due to subjectivity, saying, *"The problem with not being prescriptive is subjectivity... if the auditor does not agree with utility, we have no appetite for any legal action. If we go to court, we already lost."*

Most participants (N=18) noted that the prescriptive approach, while useful for providing clear and actionable requirements, may not be applicable or feasible for all. For example, P16 (All Roles) discussed that Systems Security Management-Security Patch Management Requirement (CIP007-R3) is very demanding, time consuming, and hard to comply with by saying *"An entity has to have somebody, first of all, know your entire sources of patches every 35 days....The problem is many software developers and vendors do not distinguish a security patch from an operational patch or from a regular patch. So what ends up happening is you have people just gotta figure out which ones are security patches and which ones are regular patches within 35 days and show documentation that is reviewed. It is the biggest, probably the number one, waste of time."*

Sixteen participants highlighted that if prescriptive standards are not updated frequently, it could lead to outdated recommendations, which can cause insecure applications. For example, CIP-007 Systems Security Management-Account Management requires passwords to be at least eight characters, and a minimum password complexity of three or more different types of characters, and a password change requirement in a specific time frame [41]. As an example, P22 (Audt, Impl, Conslt) pointed out the security issues related to non-updated, very prescriptive password requirements by saying, *"Password requirements have very specific requirements for passwords on length and complexity. With the move in security now to longer, less complex passwords like passphrases, that is not allowed under the standards."*

Outcome-Based Standards Offer Flexibility but Create Implementation and Audit Challenges. Although the majority of the standards are prescriptive, most participants (N=17) mentioned that newly-released standards are outcome-based, just specifying what utilities need to achieve without dictating how these objectives should be met. Fourteen participants mentioned that outcome-based standards could be challenging for the utilities. For example, P1 (Conslt, Drafter) mentioned CIP-013- Supply Chain Risk Management presents challenges for utilities due to the lack of specific guidance on implementation by saying *"NERC is finding a lot of utilities have not done that [implementing supply chain risk management plan]. They struggle with actually putting that out there. And part of the reason is ... it just says, give me a supply chain risk management plan; we are not going to tell you every little part of what you have to do. But you have to say that. And I find that is a big challenge for utilities."* Another discussion was about small utilities' need for detailed guidelines. According to 7 participants (from small and large utilities and also vendors), flexibility might be beneficial for large utilities, but it is indeed challenging for small utilities since they do not have enough resources in terms of personnel and financial to come up with their technical solutions. They emphasized that small utilities need prescriptive, detailed step-by-step guidelines; otherwise, they can not figure out what to do. For example, P4 (Impl) said that *"Small utilities want NERC to tell them exactly what to do. Generally speaking, a large utility will say do not tell me what to do. We have people that can figure that out."*

Six participants mentioned that outcome-based standards lead to a more complex and exhausting audit process due to interpretation differences. For instance, P4 (Impl) said *" It created this new problem, and then the whole process of trying to figure out what the interpretation of that...That is a very long, drawn-out process and does not result well in folks that are up against the wall on an audit and the auditors saying, no, I do not think your evidence is correct here. I do not think you interpreted the language of the standards correctly."*

Vague Standards Create Industry-Wide Confusion. Several participants (N=6) noted that vague descriptions of the standards have also resulted in considerable confusion within the industry. P17 (Impl, Conslt) exemplified this sentiment *"The entire industry argues about the word "programmable" and what that means. Standards can clarify further and eliminate confusion...You must report an attempt to compromise physical or electronic security. That creates tons of confusion about how you define "an attempt" versus how I do. You are gonna put in internal network security monitoring to look for "anomalous traffic", what anomalous means to you, what it means to me, and what it means from one vendor to the next very different."*

In addition, four participants mentioned that if the standards provide a very long and unclear description of a term, it also becomes very challenging for the utilities to determine the scope. For example, P5 (Impl, Drafter) said, *"The definition of a cyber asset is about a page long, and so a lot of people get tripped up over that because identifying what is in scope is so difficult."*

5.2 Implementation Phase

In the second step, utilities focus on implementing the standards' requirements. We asked participants which standards are the most challenging to implement and the specific difficulties they encounter, as well as their struggles with aligning to new standards. This section discusses those challenges.

Resource Limitations Undermine Effective Standards Implementation. One of the most prominent themes discussed by 18 participants was financial and workforce resource constraints while implementing the standards. For example, P7 (Audt, Impl, Drafter) said, *"We have to buy new tools, install new tools, and get through the budget cycle. So things that are going to take a couple of years to accomplish."* Similarly, P20 (Impl, Drafter) discussed limited resources' effect on implementation time *"I do not think you could implement what they're asking in one year. If you had all the money and all the people in the world, you probably could. But we have only got limited resources."*

For 7 participants, smaller utilities faced more challenges due to limited resources and expertise. P5 (Impl, Drafter) remarked, *"Smaller utilities face more difficulties in implementing these standards due to limited resources,"* highlighting the excessive burden standards placed on smaller organizations. Similarly, P18 (Audt, Impl, Drafter) mentioned that operating primarily as non-profit entities, municipal utilities must navigate limited financial resources while supporting extensive operational demands, including significant contributions to municipal budgets.

Along with financial constraints, 8 participants mentioned that utilities face a significant workforce shortage, exacerbated by an aging employee base. For example, P18 (Audt, Impl, Drafter) said *"People are aging out. If you look at the average age of the folks [in utilities], it is over 40. So in the next 2 decades, we are going to be out of people...We do not have a lot of folks coming out of school getting into the energy industry. That is going to be a challenge,"* highlighting demographic shift poses a serious threat to the continuity and effectiveness of infrastructure operations and security.

Six participants also noted that budget-constrained utilities struggle to attract and retain high-quality IT security personnel. For instance, P3 (Audt, Impl, Drafter) said that *"The utility employees are city employees and city employees must live in the city. And when you have this little tiny municipal in one of the poorest counties, you can not hire anybody because of that silly city rule, it is tough. Nobody wants to live in this very, very poor, lousy school community."*

Tedious Procedures Drive Frequent Violations. Many participants (N=17) mentioned that the most violated standards, as mentioned in the NERC report [43], are CIP-005, CIP-007, and CIP-010, which demand a continuous real-time effort that involves constant monitoring and adjustment. They highlight that those standards have tight deadlines and the intensity and complexity of these standards contribute to their high violation rates. For example, P22 (Audt, Impl, Conslt) mentioned how challenging implementing CIP-010 Configuration Change Management and Vulnerability Assessments *"It is a scope issue. There are a lot of devices that are in scope. A lot of entities seem to struggle with maintaining the baselines. Even though there are tools available, you have a baseline that needs to be tracked and maintained. And then, for all the changes that are made, you have to track those changes, you have to do testing on security controls and verification and documentation of that for the controls. So there are a lot of moving parts."*

Zero Tolerance Standards Create Burdensome Compliance Pressures. Standards enforce a zero-deficiency policy, which mandates that every requirement be met without any deviation according to 14 participants. They mentioned that this stringent approach, while intended to ensure absolute compliance, has proven to be extremely difficult to maintain. For instance, P5 (Impl, Drafter) mentioned *"You have your change management and patch management happen continually. Every single one of those can be a violation, and 99.9% effectiveness is still non-compliant. So if you have just one that you miss, you have to report that."* This shows zero-tolerance standards force utilities to spend considerable time and effort on administrative tasks, and minor oversights can lead to violations.

Operational Constraints Require Meticulous Planning. Many participants (N=13) mentioned OT environments present unique challenges compared to traditional IT settings where OT assets such as power generation units must remain functional around the clock, meaning any changes to these assets must be meticulously planned to avoid disrupting operations. For example, P17 (Impl, Conslt) mentioned *"There is operational scheduling, you are gonna go touch something that can never go down and you need to potentially take it down to do your work...Even if the units are not running that does not mean you can just start ripping out all the controllers and doing all kinds of other stuff. It is still dangerous. It was very intentional who was gonna work and how we planned safety into the work. This is not a traditional IT where we are protecting data at rest data and motion data use."* emphasizing services like pressurized lines remain operational, requiring careful consideration before any maintenance or upgrades can be performed.

5.3 Reporting

Utilities report incidents as a final step. We asked participants what works well and what doesn't in the reporting process.

Ambiguity in Incident Classification Lead to Inconsistent and Overwhelming Reporting. All participants mentioned that the ambiguity in classifying reportable incidents is particularly challenging for utilities, leading to inconsistent reporting practices. They noted that the standards provide insufficient guidance on what constitutes a reportable incident, which results in varied interpretations and potential underreporting of incidents. P7 (Audt, Impl, Drafter) stated, *"We have to report attempts to compromise, and this is poorly defined. There are hundreds or thousands of attempts to compromise every day. We could report a bunch of noises or we report nothing."* and emphasized that this ambiguity can lead to both under-reporting and over-reporting. For example, P18 (Audt, Impl, Drafter) mentioned whether a failed login, a port scan at an electronic security perimeter (ESP), or an unsuccessful badge swipe at a physical perimeter should all be reported as attempts to compromise emphasizing its lack of clarity has the potential to overwhelm the reporting systems.

Lack of Trust Hinders Timely and Transparent Incident Reporting. According to several participants (N=8), utilities are hesitant to report incidents promptly due to the lack of trust between utilities and regulatory agencies. They mentioned that utilities are uncertain about the post-reporting phase including the consequences of reporting. P5 (Impl, Drafter) said *"A lack of trust between the reporting agency and the utility makes that very difficult. If federal agencies don't have people who can help to fix the issue, then utilities will probably not be as quick to report"* emphasizing the building of trust. Similarly, P4 (Impl) discussed unclear steps after reporting *"A lot of utilities are very concerned about reporting because there are not many clear examples of what happens with that information... I think that a big part of the lack of reporting is around the fear of what happens after that."*

Two participants mentioned that a significant issue identified is the distrust organizations feel toward external entities when sharing sensitive incident data and concern over the security and handling of this information once it leaves the organization's control. P18 (Audt, Impl, Drafter) emphasized that mishandling such data could introduce new risks, underscoring the need for more secure and trustworthy sharing mechanisms

Strict Reporting Timelines Clash with Limited Resources and Incident Response Priorities. Standards mandate a strict timeframe for reporting incidents, but the process of gathering accurate information, classifying the incident, and preparing the necessary documentation can be time-consuming and difficult to execute quickly, according to five participants. For example, P12 (Audt, Impl) discussed how time limit can cause a lack of reporting *"Once you determine an actual compromise, you have an hour to report it. A good portion of utilities do not have 7/24 monitoring staff. They do not have full-time cybersecurity people watching alerts...So actually executing upon that requirement when it comes time to execute is a very ad hoc and human performance latent condition. Everyone's 1st trust is stopping the compromise. Reporting to the industry is the second thought for them."* In addition to that, P5 (Impl, Drafter) highlights knowing lack of help can slow down the process said *"If NERC does not have people that can help, and they can send in and fix the issue then you are probably not going to be as quick to report or consider that a valuable partnership."*

5.4 Improvements

We asked participants for suggestions on improving compliance and implementation of the standards. Here are the direct responses to our inquiry, even though there are more improvements implied by their other comments.

Updating Detail Level of the Standards Is Necessary. Fifteen participants highlighted the need to update old and overly prescriptive standards to align with modern security requirements and threats. Additionally, 7 participants noted that smaller utilities often struggle to fill the gaps objective-based standards leave because they lack sufficient resources; these smaller utilities find it challenging to develop secure solutions independently. They recommend that standards should consider the needs of all types of utilities and provide more prescriptive guidelines for smaller organizations.

Extended Compliance Timelines Ease Operational Burdens. Thirteen participants mentioned that the stringent timelines for compliance performance, particularly in areas like patch management, baseline updates, and log reviews create significant operational challenges, leading to a call for extending these timelines. They argue that by lengthening the timeframes, utilities could run more effective programs without compromising the reliability of the electric grid.

Holistic Evaluation Could Strengthen Overall Security. Ten participants suggested that NERC CIP compliance would benefit from shifting away from penalizing minor infractions toward a more holistic evaluation of security. They mentioned that currently, even minor issues, like a missed patch, are escalated through a rigorous regulatory process, which burdens organizations and detracts from a comprehensive security assessment. They suggested that enforcement should assess security at a system-wide and organizational level, allowing for minor variances as part of continuous improvement, rather than penalizing every small infraction.

6 Audit Process

In this section, we consider our second research question regarding the challenges during the audit process. We list the main themes derived from the interviews below.

6.1 Preparation

We asked participants about the most important steps they take in preparing for an audit, and how much effort it requires.

Documentation & Evidence Collection Diverts Resources and Undermines Security Priorities. According to all participants, preparation for the audits, which includes gathering and organizing the necessary evidence, requires an extensive amount of time. To emphasize the required time P1 (Conslt, Drafter) said *"We had a company. I think they spend a good 2000 hours just trying to gather evidence."* Sixteen participants mentioned that some utilities need to pull personnel away from their regular duties related to operations and maintenance to focus on gathering evidence and preparing for the audit. P13 (Impl, Conslt, Drafter) discussed this situation and its possible security effects *"I do not think it is an*

effective use of our resources. Entities have to ramp up and redirect their people away from other critical initiatives to fully support audits. And anytime we have to pull people away for the purposes of audit, it is a distraction to security and reliability." The effort utilities spent for audit preparation is even considered unworthy when compared to its security value, according to 10 participants. P5 (Impl, Drafter) exemplified this *"Many more resources could be applied to security. We have not found the balance between the carrot and the stick in the regulation to get that right. The time spent in audit preparation exceeds the value to security."*

Mock Audits Add Extra Burden Without Direct Security Benefit. Audit preparations require more effort than collecting evidence, where utilities perform mock audits for rehearsing responses and scripting interactions with auditors, according to 9 participants. P13 (Impl, Conslt, Drafter) explained it *" I bring people in for a session. I pulled up the evidence that they provided. I have some questions about that evidence. I turn into a completely different person, and I play the mean auditor, so they understand what that will feel like, and they know I'm going to do this. I play the overly friendly auditor to get them talking about stuff they should not be talking about. And I play the one that is in the middle."* P5 (Impl, Drafter) emphasized the consequences of unprepared audits, which highlights the reason why utilities put that much effort into mock audits *"Audit is not a friendly environment; it is more of a legal proceeding. In many cases, there are a lot of high stakes for communicating the wrong thing, providing your own context in a way that takes the auditor down a certain path. And once you establish that context, it can be very challenging to take a step back and give a different context."*

Necessity to Consultant Adds Cost Without Security Benefit. Another theme discussed by 6 participants is audit preparations can be resource-intensive, leading to the hiring of consultants to assist either with the audit preparation or to cover day-to-day operational tasks during the audit period. For example, P16 (All Roles) emphasized its cost with no security value *"You have a full-time team that has to respond to auditors. Most entities will have a compliance team, or they will hire consultants to come in who will be the intermediaries and prepare them for audit...So that is all costing industry, but it is really not adding security value to address risk."*

6.2 Auditing

We asked about participants' experience with auditing and auditors.

Auditor Knowledge Gaps Undermine Audit Efficiency and Frustrate Utilities. For 20 participants, it is very important that auditors possess domain knowledge in areas such as electric system operations, reliability, IT security, OT security, and industry-specific regulatory requirements. For example, P7 (Audt, Impl, Drafter) mentioned *"Having a fundamental understanding of how the systems work makes them a better auditor. The ones that lack understanding are the hardest to communicate with and convince."* According to 16 participants, some auditors come from IT backgrounds and lack the essential knowledge of the OT domain, and this forces utilities to spend valuable audit time educating auditors on fundamental differences between IT and OT environments, detracting from the audit's primary objectives (N=16). For instance, P20 (Impl, Drafter) pointed out, *"We have had auditors asked very basic questions that they should know the answer."* Similarly, P4 (Impl) illustrated the challenges caused by such gaps, saying, *"A lot of auditors come in with just an IT background. They think that because they know a firewall, they understand ICS. That is a huge problem. I have had arguments with auditors over just complete and total miscomprehension around what a term means or how it is actually implemented."*

Poor Communication and a Punitive Approach Undermine Audit Collaboration. According to 14 participants, if auditors and utilities can not communicate effectively, pursuing a smooth audit process is becoming very challenging. P6 (Conslt) remarked *"They have gotta have good communication skills. They need to be able to communicate and talk at the various levels to the more executive folks, the security leaders as well as, the technicians and the practitioners."* indicating that regular and transparent interactions helped ensure that both parties were on the same page.

Four participants mentioned that if auditors focus on finding violations during audits, this prevents open communication between utilities and auditors. For example, P13 (Impl, Conslt, Drafter) mentioned that *"They need to be less interested in the gotcha game based on technicalities of the words in the standard and more interested in partnering together to achieve the security objective. Do not punish us for small things. It breaks the trust and it breaks the credibility, and it only causes people to want to hide what they are doing."*

Risk-Based Audits Offer Promise but Depend on Auditor Expertise and Judgment. Risk-based audit evaluates compliance by considering the potential impact and threat level of each asset within the power grid, according to 12 participants. This method prioritizes auditing assets whose compromise would have severe consequences on grid stability and operations, ensuring that critical vulnerabilities are addressed first. Several participants (N=12) noted that there is potential for implementing this approach in the future, and they shared its possible positive aspects. For example, P9 (Impl, Drafter) said *"If the auditors really truly understand how to do risk-based audits, I think things would move smoother, and we would get away from that whole concept of you missed this patch on this asset, therefore you have got a violation."*

However, 6 participants discussed challenges utilities might face with risk-based audits. For example, P7 (Audt, Impl, Drafter) noted how an auditor's background can influence the determination of risk, stating, *"Auditors who do not have any experience in the utility industry do not have a good concept for the level of risk. When we say this is very low risk, this is negligible; they do not really understand enough to know if that is true or not."* P22 (Audt, Impl, Conslt) noted that auditors need to check the evidence for compliance, but for a risk-based analysis, what they will consider as evidence.

6.3 Penalties & Rewards

We examine the final step of the audit process: determining the outcome, which may result in either a penalty or a reward.

Financial Penalties Raise Awareness but Vary in Deterrent Effect Across Organizations. Financial penalties are considered essential to ensure compliance by 17 participants. For instance, P10 (Impl, Conslt) discussed how a penalty of one utility could alert all community *"Duke was fined like 10 million dollars a couple of years ago for saying that they are doing something under NERC and they were not. It was gross negligence. A $10 million fine was too much or too little, I do not know, but it definitely got the industry's attention.*

So it worked for others." Some participants (N=12) discussed that penalties are not deterrent enough to ensure organizations comply with standards. P18 (Audt, Impl, Drafter) emphasized *"I think there should be more fines. I do not think fines are enough. We use the stick as much as we use the carrot in my group. I am a big believer in the stick."* Seven participants discussed that penalties' impact varied depending on the organization's size and resources. P1 (Conslt, Drafter) said, *"The smaller entities may care a little bit more than some of the bigger entities that have a little bit deeper pockets."*

Positive Observation. If the audit identifies exemplary compliance practices or achievements that exceed basic requirements, auditors make positive observations about the utility. Many participants (N=12) mentioned that without tangible benefits, positive feedback in standards compliance holds little value for organizations. For example, P5 (Impl, Drafter) said *"If there were some incentive tied to the positive performance, that would allow utilities to go beyond the standards."* emphasizing incentives can motivate organizations to exceed standards.

6.4 Improvement Suggestions

We talk about suggestions that participants directly mentioned beyond what was mentioned earlier.

Performance-Based Audits Offer Relief for High Performers and Incentivize Continuous Improvement. Several participants (N=14) discussed the transition to a more performance-based audit process, which tailors the audit frequency based on the performance of the utility during previous audits. If a utility has no violation during the audit (and maybe outperforms it), it may be granted a longer interval before the next audit, providing a form of relief. Conversely, if the audit reveals significant issues, the utility can expect another audit much sooner.

Streamlining Evidence Collection Could Reduce Audit Burden. Twelve participants considered that the process of gathering documentation and evidence for audits needs improvement, and simplifying and streamlining these processes could significantly reduce the burden on utilities. For instance, P10 (Impl, Conslt) mentioned automating the process *"If you had different ways to automatically collect your evidence, that would be a lot easier because a lot of the evidence collection is manual. A lot of the repositories are spreadsheets and Word documents and things like that."* Automating the evidence collection process could free up resources and allow to focus on more critical aspects of compliance.

Improving Auditor Training Could Enhance Audit Quality. Auditors need better training to understand the complexities of utility operations and cybersecurity, for 5 participants. P6 (Conslt) emphasized it *"You need to have that depth of understanding of the context of the organization, how they're structured, their architecture, their organizational choices, and work processes to be able to assess whether the drafted performance statement is compliant right."*

Four participants discussed that auditors also need to be trained on how to approach utilities and assess compliance. P1 (Conslt, Drafter) described inconsistent auditor behavior during audits *"Some auditors are about what we call gotcha games. They are out there to find anything they can. Other auditors are much more willing to help. They are there to collaborate to co-create solutions. So that is a problem, the different approaches between the different auditors."*

7 Standards Development

We asked participants' experience in standard development a series of questions to explore their perspectives. These questions focused on identifying the major bottlenecks and concerns in the standard development and update process, as well as gathering their suggestions for improving these processes.

7.1 Challenges About Process

Lengthy and Complex Development Process Risks Standards Becoming Outdated. Standard development within the NERC CIP involves a comprehensive regulatory process, including "Standards Authorization Request" issued by FERC, review by NERC, drafting team appointment, a rigorous voting process, further scrutiny and approval by NERC, regulatory agencies, and even provincial authorities due to the interconnected nature of the electric grid across North America. The consensus-based approach to standard development, while effective, is inherently slow due to the need for broad agreement among diverse entities (N=17). P5 (Impl, Drafter) highlighted the broad agreement process and its importance, *"If you make the wrong changes in the standard for security and if you don't understand the implications, it can create reliability issues in the power grid. For example, black start generators are small facilities...If they have to comply with these standards, the cost of complying with the standards would shut them out of business and reduce the reliability of the grid. There are a lot of unforeseen consequences that can occur. So that's why you have such a long process."*

According to five participants, the extended timelines raised concerns about the relevance and efficacy of these standards upon implementation. They questioned whether standards developed over several years would remain applicable in the face of rapidly evolving technologies. P1 (Conslt, Drafter) articulated this frustration, stating, *"It could be like 2 to 4 years before a standard actually goes live. And then how relevant really is it? And I think that is the biggest challenge. You are working on something now that may not go live for 3 years. Is it still going to be relevant in 3 years? Is virtualization gonna be the same or is the monitoring technology gonna be the same?"* This highlights a critical tension between the need for thoroughness and the rapid pace of technological change.

7.2 Challenges About Human in the Process

In this subsection, we talk about the challenges of humans in the standard development process.

Voluntary Commitment Slows Standard Development and Strains Contributors. The reliance on volunteer-based drafting teams, as highlighted by seven participants, presents a significant bottleneck in the standard development process. This model often leads to scheduling conflicts and delays due to the competing demands on volunteers' time. For example, P2's (Impl, Drafter) observation, *"One of the biggest bottlenecks that makes it slower from start to finish is just scheduling and availability of the personnel. When you have 20 people, you do need a quorum to continue for formal discussions and reviews. It just takes time to go through the process to find out if everybody is available on this date. And usually everybody out there is not available since they are all volunteers."* P4 (Impl) further emphasized the time commitment and its impact on individuals' primary jobs, stating, *"I do not understand how you*

support that if you are in a day job? I considered being on the drafting team. I looked at the time requirements and I do not understand how I can get my job done and commit to doing all these meetings as well. It just is not gonna happen." This reveals the substantial time commitment required of drafting team members.

Lack of Expertise in Drafting Teams Raise Concerns About Standards Quality. Six participants raised serious concerns about the quality and effectiveness of the standards development process by discussing that some drafting team members may lack the necessary expertise or may not be the most qualified representatives of their utilities. For example, P4 (Impl) said, *"Uncomfortable truth around the members that are on a drafting team is often these are folks that are –I do not want to say dispensable in utility–, but they in order for utilities to have been able to dedicate that much time to be on the drafting team that means that they are not doing something at their utility...Utility do not value their contributions,"* suggests a potential disconnect between standards drafters and core utility operations. Utilities may not be sending their most knowledgeable or experienced personnel to drafting teams, potentially due to the time commitment or a perceived lack of strategic importance.

Drafting Teams Lack Balanced Representation from Industry Practitioners. According to six participants, an unbalanced population in the drafting team was another concern-while there is substantial involvement from vendors, there needs to be more representation from utility professionals who deal with these standards in practice. P18 (Audt, Impl, Drafter) expressed a desire for greater industry involvement, saying, *"I have participated in the virtualization standard drafting team and the majority of folks on there were vendors. There are a lot of vendors developing standards, not necessarily that is a bad thing. I think there needs to be a mix. But there is not enough representation from the industry itself."*

Motivation of Drafting Teams Undermine Integrity of Standards Development. The potential for conflicts of interest among drafting team members, as discussed by four participants, adds another layer of complexity to the standard development process. P20 (Impl, Drafter) highlighted how team members from small utilities prioritize their interests *"I have seen this in some of the drafting teams. They literally have people who come to the drafting teams, just to make sure that lows do not get included in a standard. And those are people coming from the low impact utilities. Because it is their best interest to not have that standard for them."* This suggests that some members may prioritize their own utility interests over the broader objective of developing robust industry standards.

The transition of professionals between industry roles and standard development or auditing positions, as noted by two participants, can create peer-based conflicts and hinder the agility of the regulatory process. For example, P3 (Audt, Impl, Drafter) mentioned *"I was the vice chair of that drafting team for a year in the beginning. Then I went into the auditing field and I had a little bit of a conflict. I could not write the standards and then audit them. So that is a huge problem. That is the agility problem."* This illustrates the potential conflicts of interest when individuals switch roles, which can lead to ethical dilemmas and undermine the credibility of both the standards development and auditing processes.

7.3 Improvement Suggestions

Here, we proposed possible suggestions for improving the standard development process.

Accelerating Standard Development Could Improve Responsiveness. In response to the lengthy timelines, several participants (N=10) advocated for expediting the standard development process. For example, P22 (Audt, Impl, Conslt) discussed the potential area to speed up the process *"NERC takes a long time to review a standard, several months to review it before they rule on it. That is probably the biggest opportunity to move things quicker."* Some participants (N=8) mentioned FERC-mandated CIP-015 Internal Network Security Monitoring standard was developed in about a year, compared to the years-long process for typical standards. However, P18 (Audt, Impl, Drafter) highlighted potential challenges associated with this expedited process, *"The problem with having industry involved is that there are not the same sensitivities to the challenges we have in the utilities. CIP-015 is probably the best example of that. That is gonna pose a challenge. I am not sure people really understand the impact of it yet. It is going to be pretty substantial and pretty significant."* This highlights the potential for unintended consequences when speed is prioritized over a comprehensive understanding of the operational landscape.

As an alternative way, five participants suggested easing regulatory scrutiny and reducing the high stakes associated with audits could significantly streamline the standard development process. P9 (Impl, Drafter) exemplified this sentiment by saying, *"You'll talk to a technical person, say this is great, we can do this, it's perfect. And then you got a lawyer arguing over a single word."* indicating the intense focus on every word due to the potential for severe penalties makes consensus difficult to achieve, slowing down progress.

8 Concluding Discussion

This paper presents an in-depth, improvement-oriented examination of the cybersecurity standards lifecycle and its challenges, using NERC CIP as a case study through semi-structured interviews with implementers, auditors, and standard drafters. Our findings highlight key issues in compliance, auditing, and standard development, and reflect stakeholder-driven suggestions to make the regulation more effective, flexible, and responsive to emerging threats. These suggestions build on the regulation's strengths while addressing pain points identified by stakeholders.

These findings offer valuable insights for other critical infrastructure sectors considering similar regulatory frameworks. While adapting NERC CIP to areas like transportation or healthcare requires sector-specific adjustments, lessons from the energy sector can guide effective cybersecurity strategies and help avoid common pitfalls. Here, we synthesize the lessons learned and propose future directions, with key recommendations summarized in Figure 2.

8.1 Compliance

This stage presents challenges in balancing flexibility with prescriptiveness and managing the complex documentation. We present recommendations to address these issues to improve the process.

Adjusted Outcome-Based Standards. The balance between prescriptive and flexible standards was a major point of discussion (Section 5.1). While larger utilities with ample resources may value

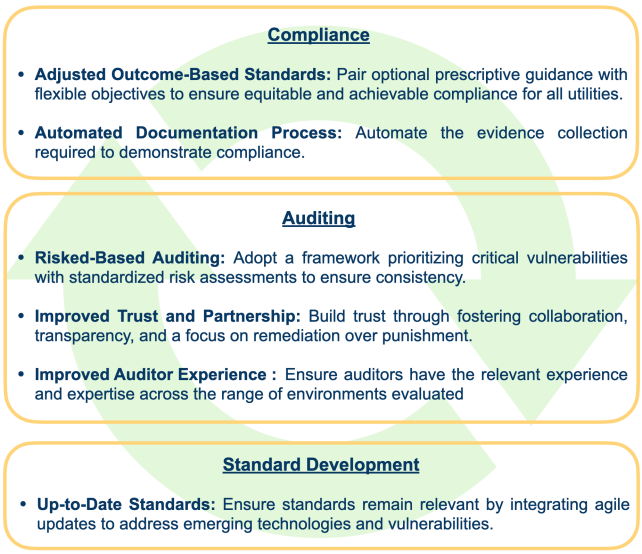

Figure 2: Our recommendations to improve cybersecurity standards throughout its lifecycle.

the flexibility of outcome-based standards, smaller utilities often struggle to fill the gaps left by these non-prescriptive guidelines (Section 5.2). Participants from smaller utilities indicated that they lack the technical resources to develop secure solutions independently, making compliance difficult and widening the gap with better-resourced peers.(Section 5.2)

To address this, we propose a dual-layered approach where prescriptive guidance serves as an optional implementation pathway. Under this model, the standards will be flexible (outcome-based), emphasizing desired security outcomes. However, a set of prescriptive steps provides a concrete roadmap to help entities, especially those with fewer resources. These prescriptive guidelines are illustrative (not mandatory) examples of how to meet flexible objectives and utilities with greater capacity may pursue alternatives if they achieve equivalent security outcomes. Auditors would evaluate compliance on outcomes, using the prescriptive path as a reference rather than a benchmark. This preserves adaptability while ensuring all utilities—regardless of size—have actionable guidance. A similar dual-layered model already exists in NIST SP 800-53 Rev. 5 [69], a widely adopted cybersecurity framework that defines high-level, outcome-based control objectives, which are paired with prescriptive implementation baselines defined in FIPS 200, the U.S. federal standard for minimum security requirements.

The potential of this dual-layered approach is reflected in NERC's recent shift toward outcome-based standards—e.g., CIP-013 (Supply Chain Risk Management), which emphasizes objectives over step-by-step controls. While not a formal dual-layered model, the existing mix of prescriptive and objective-based standards shows capacity for evolution in this direction. Our proposal builds on this foundation, pairing NERC's prescriptive elements with outcome-based flexibility to align with utilities' diverse operational contexts.

While transitioning to a dual-layered structure may increase short-term auditing complexity-requiring updated auditor training and introducing multiple evaluation paths—the long-term benefits include greater clarity for smaller utilities, flexibility for larger ones, and stronger alignment between compliance practices and actual security outcomes. This model benefits implementers seeking clearer pathways, auditors evaluating diverse utilities, and regulators aiming for more adaptive, risk-aware compliance.

Automated Documentation Process. A recurring frustration among participants was the administrative burden of compliance documentation, particularly the time and personnel required to collect and maintain audit-ready evidence (Section 5.2). Many noted this overhead detracts from substantive security efforts, creating a misalignment between compliance investments and actual risk reduction. Some utilities even hired staff primarily for documentation rather than technical security roles (Section 6.1), raising concerns about the return on compliance investments.

To address this, we recommend expanding the use of automated evidence collection and reporting. Existing tools already show the potential to automate compliance tasks [10, 18, 48], underscoring significant opportunity in this space. For example, NP-View already illustrates the promise of automating key NERC CIP activities—such as validating Electronic Security Perimeters under CIP-005. However, adoption remains limited due to cost, proprietary constraints, and scalability challenges, particularly for smaller utilities.

To address barriers, we propose leveraging collaborative development models—such as MITRE's open-source frameworks and CISA's public-private initiatives—to support the creation of modular, community-driven compliance tooling. These models offer both precedent and promise for building accessible, sector-aligned tools that reduce compliance friction without compromising rigor.

Automated documentation benefits both implementers and auditors: utilities face less manual workload and greater consistency, while auditors streamline evidence review and reduce disputes over quality or completeness. Ultimately, a broader ecosystem of open-source and cost-effective automation tools would enhance the efficiency, scalability, and equity of compliance across the sector.

8.2 Audit Process

The audit process faces key challenges: the absence of risk-based vulnerability evaluation, limited auditor expertise, and insufficient trust between regulators and utilities. Here, we recommend measures to improve audit accuracy, build trust, and better align security evaluations with operational realities.

Risk-Based Auditing. One of the critical findings from our study is the need to shift from uniform, checklist-based audits to a risk-based model (Section 6.2). Current practices give equal weight to all requirements, regardless of the actual risk posed by a system, asset, or vulnerability (e.g., patching all vulnerabilities within set timeframes without considering their relevance to core operations) (Section 5.4). This leads security teams to prioritize documentation over addressing high-risk threats that directly affect grid reliability. Instead, vulnerabilities should be prioritized by their potential impact on grid stability, guided by a threat model that accounts for different adversaries and attack goals. These findings support the shift toward more targeted, threat-informed strategies, aligning with broader industry recommendations and the Department of Energy's (DOE) cybersecurity guidelines [46].

A risk-based auditing approach would evaluate compliance by considering the potential operational impact and likelihood of exploitation, rather than applying the same scrutiny to low-risk and high-risk assets. Several participants suggested audits should prioritize issues relevant to critical operations and allow more flexibility for low-impact systems. This would help redirect attention and resources toward high-consequence vulnerabilities instead of treating minor technical issues as violations.

This model aligns with how cybersecurity risk is managed in other domains and is reinforced by existing industry frameworks. For example, the MITRE ATT&CK for ICS [4] matrix provides a structured method to map attack techniques to critical control system assets and operational impacts. Similarly, DOE has encouraged risk-based prioritization in multiple recent publications, including its Cybersecurity Capability Maturity Model (C2M2) [21] and Cyber-Informed Engineering Strategy [76], both of which emphasize aligning cybersecurity efforts with system-level risk.

Importantly, a shift toward risk-based auditing shows strong potential within NERC's oversight structure. Participants noted early momentum toward more flexible, judgment-based evaluations—especially where the standard's intent was met despite minor deviations (Section 5.1). Formalizing this approach would require additional auditor training and standardized risk assessment protocols, but builds on capabilities already in development. This model benefits implementers by focusing on high-impact systems, auditors by providing clearer priorities and more meaningful engagement with system risk, and regulators by better aligning enforcement with mission-critical objectives like grid resilience. Overall, a risk-based model offers a more adaptive, intelligence-informed regulatory process suited to the evolving threat landscape and operational complexity of critical infrastructure.

Improved Trust and Partnership. Our study found that trust between NERC and utilities is critical for effective compliance and security, as it enables more efficient audits and encourages transparent incident reporting when regulators prioritize remediation over punishment (Section 6.2,Section 5.3). Similarly, trust smooths the audit process, as utilities would feel less defensive in interactions with auditors. Models like CISA's Joint Cyber Defense Collaborative (JCDC) [17], which facilitates public-private cooperation through information sharing and joint planning, highlight the value of trusted relationships in managing cybersecurity risks.

To foster greater trust, we recommend a more collaborative auditing environment with joint working groups where utilities and regulators address issues before audits. Greater transparency—clear and constructive feedback—would strengthen relationships, while emphasizing corrective actions over penalties would encourage incident sharing and open communication. These changes hold promise within current regulatory practices; some NERC regions have already piloted pre-audit engagement or advisory roles [40], and collaborative mechanisms like JCDC demonstrate their scalability. Beneficiaries include implementers, who could engage with auditors more openly, and regulators, who would gain greater insight into evolving challenges and foster more responsive oversight.

Improved Auditor Experience. We also found the disconnect between IT and OT security expertise in compliance audits, which was a source of frustration for participants. Participants noted that auditors with IT backgrounds often ask questions that reveal a limited understanding of OT's unique challenges, which can unnecessarily extend the duration of audits. (Section 6.2)

To bridge the IT-OT disconnect, we recommend incorporating the principles from the Cyber-Informed Engineering (CIE) framework [76], which emphasizes OT-specific security practices rooted in the physical process and operational context. Regulators could improve audit effectiveness by providing OT-focused training for IT-based auditors, ensuring they are prepared to evaluate security through an operationally informed lens. Additionally, incorporating guidance from resources like the CIE implementation guide would help align cybersecurity standards with the realities of OT environments, moving beyond traditional IT security paradigms.

These suggestions are actionable because they build on existing structures—auditor training, audit protocols, and DOE-supported frameworks like CIE [76] —without requiring regulatory overhaul. Training can be integrated into existing auditor certification or continuing education efforts. CIE guidance is already publicly available and endorsed by the U.S. Department of Energy, showing promise for regulatory agencies and utilities to adopt without developing new tools from scratch. Auditors would gain a broader evaluative toolkit and greater consistency, while utilities would face fewer misinterpretations and less operational disruption during audits.

8.3 Standard Development

The standard development phase faces challenges in keeping cybersecurity regulations aligned with rapidly evolving technologies and threats, leaving critical infrastructure vulnerable. Here, we present recommendations to modernize standards and integrate emerging technologies proactively.

Up-to-Date Standards. As technology advances, current cybersecurity standards face challenges to remain relevant and effective. Our study found that current regulations often lag behind innovation, exposing critical infrastructure to new vulnerabilities that original frameworks do not address. Rigid and time-intensive processes for updating standards hinder the timely adaptation of cybersecurity policies, creating a risk that these standards will not reflect modern operational environments. Without more responsive mechanisms for updates, utilities may lack adequate guidance for addressing current and emerging cybersecurity challenges.

To address this, we propose supplementing the existing standards development process with more agile mechanisms for interim guidance, such as rotating expert panels to issue clarifications, shorter comment windows for minor updates, and formalized interpretation bulletins. These mirror NIST mechanisms—most notably, the iterative refinement of security controls in SP 800-53 and the tiered approach to guidance seen across the NIST 800-53 and FIPS 200 frameworks [68, 69]. Both NIST and NERC rely on stakeholder-driven, consensus-based development processes. However, NIST's framework is designed to support a diverse range of organizations with varying maturity levels and is supplemented by a robust infrastructure of implementation guidance, FAQs, and regular revisions. By contrast, while NERC does issue artifacts like Lessons Learned and Compliance Guidance, these documents are infrequent, advisory in nature, and lack formal standing. Applying a NIST-like model would not be a one-to-one translation, but the structural parallels—particularly in stakeholder engagement—suggest that similar

mechanisms could be adapted to NERC's domain with appropriate institutional support and oversight authority.

These enhancements could build on NERC's Compliance Guidance program, which already lets stakeholders submit guidance documents for review and endorsement. While currently advisory and infrequently updated, the program provides a foundation for a more formal process to issue interim advisories and clarifications. For example, NERC could create a streamlined review pathway for time-sensitive updates or recurring implementation questions, giving stakeholders timely and authoritative support without waiting for full standards revisions. These mechanisms would complement, not replace, the formal standards development process. A more agile guidance framework would help utilities apply CIP standards confidently to novel architectures, reduce ambiguity for auditors, and enable more responsive regulatory oversight.

8.4 Future Works

In light of the lessons learned identified across the compliance, audit, and standard development phases of the NERC CIP lifecycle, future work can focus on addressing these critical areas through targeted research and practical solutions.

Compliance. Future research should explore innovative methods to streamline compliance processes for utilities of varying sizes. Developing adaptive compliance tools, such as AI-driven reporting systems and enhanced digital portals, can further reduce administrative burdens while ensuring rigorous security measures. Additionally, studies could investigate how tailored approaches, such as tiered frameworks, affect smaller utilities' ability to meet standards effectively without compromising operational security.

Audit Process. The audit process requires continued focus on improving risk-based assessments and bridging the IT-OT expertise gap among auditors. Future efforts could involve designing comprehensive training programs for auditors that emphasize operational technology contexts and incorporating the Cyber-Informed Engineering (CIE) framework into practice. Research could also evaluate the impact of assigning dedicated risk-assessment teams on audit consistency, as well as how fostering trust between utilities and regulators improves reporting and collaboration.

Standard Development. To keep pace with technological advancements, future work should examine agile frameworks for real-time standard updates without compromising regulatory rigor. Studies could explore best practices for integrating emerging technologies, such as AI and cloud systems, into regulatory guidelines at early adoption stages. Additionally, addressing conflicts of interest within the standard development process requires research into governance models that promote transparency and accountability, such as independent oversight bodies or stricter rotation policies.

9 Acknowledgements

We thank the anonymous reviewers for their constructive feedback. This work was supported by the Department of Energy (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER). The opinions expressed in this paper do not necessarily reflect those of the research sponsors.

References

[1] Yasemin Acar, Michael Backes, Sascha Fahl, Simson Garfinkel, Doowon Kim, Michelle L Mazurek, and Christian Stransky. 2017. Comparing the Usability of Cryptographic APIs. In *IEEE Symposium on Security and Privacy (S&P)*.

[2] Yasemin Acar, Christian Stransky, Dominik Wermke, Michelle L Mazurek, and Sascha Fahl. 2017. Security Developer Studies with GitHub Users: Exploring a Convenience Sample. In *USENIX Symposium on Usable Privacy and Security (SOUPS)*.

[3] Bushra A Alahmadi, Louise Axon, and Ivan Martinovic. 2022. 99% false positives: A qualitative study of SOC analysts' perspectives on security alarms. In *USENIX Security Symposium*.

[4] Otis Alexander, Misha Belisle, and Jacob Steele. 2020. MITRE ATT&CK for industrial control systems: Design and philosophy. *The MITRE Corporation: Bedford, MA, USA* 29 (2020).

[5] Tom Alrich. 2025. Tom Alrich's Blog about Energy Sector Utilities. https://tomalrichblog.blogspot.com

[6] David Armstrong, Ann Gosling, John Weinman, and Theresa Marteau. 1997. The Place of Inter-Rater Reliability in Qualitative Research: An Empirical Study. *Sociology* 31, 3 (1997), 597–606.

[7] Miriam E Armstrong, Keith S Jones, Akbar Siami Namin, and David C Newton. 2018. The knowledge, skills, and abilities used by penetration testers: Results of interviews with cybersecurity professionals in vulnerability assessment and management. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, Vol. 62. SAGE Publications Sage CA: Los Angeles, CA, 709–713.

[8] Miriam E Armstrong, Keith S Jones, Akbar Siami Namin, and David C Newton. 2020. Knowledge, skills, and abilities for specialized curricula in cyber defense: Results from interviews with cyber professionals. *ACM Transactions on Computing Education (TOCE)* 20, 4 (2020), 1–25.

[9] Hala Assal and Sonia Chiasson. 2018. Security in the Software Development Lifecycle. In *USENIX Symposium on Usable Privacy and Security (SOUPS)*.

[10] Assurx. 2025. QUALITY AND COMPLIANCE SYSTEMS. https://www.assurx.com

[11] Rebecca Balebako, Abigail Marsh, Jialiu Lin, Jason I Hong, and Lorrie Faith Cranor. 2014. The Privacy and Security Behaviors of Smartphone App Developers. In *Usable Security and Privacy Symposium (USEC)*.

[12] Steffen Bartsch. 2011. Practitioners' Perspectives on Security in Agile Development. In *International Conference on Availability, Reliability and Security (ARES)*.

[13] Virginia Braun and Victoria Clarke. 2012. *Thematic Analysis*. American Psychological Association.

[14] Maria Christakis and Christian Bird. 2016. What Developers Want and Need from Program Analysis: An Empirical Study. In *IEEE/ACM International Conference on Automated Software Engineering (ASE)*.

[15] Aaron Clark-Ginsberg and Rebecca Slayton. 2019. Regulating risks within complex sociotechnical systems: Evidence from critical infrastructure cybersecurity standards. *Science and Public Policy* (2019).

[16] Cybersecurity and Infrastructure Security Agency (CISA). 2024. Critical Infrastructure Sectors. https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

[17] Cybersecurity and Infrastructure Security Agency (CISA). 2024. Joint Cyber Defense Collaborative (JCDC). https://www.cisa.gov/topics/partnerships-and-collaboration

[18] Industrial Defender. 2025. Compliance Software. https://www.industrialdefender.com

[19] Erik Derr, Sven Bugiel, Sascha Fahl, Yasemin Acar, and Michael Backes. 2017. Keep me Updated: An Empirical Study of Third-Party Library Updatability on Android. In *ACM Conference on Computer and Communications Security (CCS)*.

[20] Constanze Dietrich, Katharina Krombholz, Kevin Borgolte, and Tobias Fiebig. 2018. Investigating System Operators' Perspective on Security Misconfigurations. In *ACM Conference on Computer and Communications Security (CCS)*.

[21] DOE. 2022. Cybersecurity Capability Maturity Model (C2M2). https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2

[22] Pardis Emami-Naeini, Yuvraj Agarwal, Lorrie Faith Cranor, and Hanan Hibshi. 2020. Ask the experts: What should be on an IoT privacy and security label?. In *IEEE Symposium on Security and Privacy (S&P)*.

[23] EPA. 2025. Revised Guidelines on the Environmental Effectiveness of the Standards. https://www.epa.gov/sites/default/files/2014-12/documents/revguidelinessii.pdf

[24] Konstantin Fischer, Ivana Trummová, Phillip Gajland, Yasemin Acar, Sascha Fahl, and Angela Sasse. 2024. The challenges of bringing cryptography from research papers to products: results from an interview study with experts. In *USENIX Security Symposium*.

[25] Adebola Folorunso, Viqaruddin Mohammed, Ifeoluwa Wada, and Bunmi Samuel. 2024. The impact of ISO security standards on enhancing cybersecurity posture in organizations. *World Journal of Advanced Research and Reviews* (2024).

[26] Andrea Gallardo, Robert Erbes, Katya Le Blanc, Lujo Bauer, and Lorrie Faith Cranor. 2024. Interdisciplinary Approaches to Cybervulnerability Impact Assessment for Energy Critical Infrastructure. In *ACM CHI Conference on Human Factors in Computing Systems (CHI)*.

[27] Eva Gerlitz, Maximilian Häring, and Matthew Smith. 2021. Please do not use!?_ or your License Plate Number: Analyzing Password Policies in German Companies. In *USENIX Symposium on Usable Privacy and Security (SOUPS)*.

[28] Leo A Goodman. 1961. Snowball Sampling. *The Annals of Mathematical Statistics* 32, 1 (1961), 148–170.

[29] Peter Leo Gorski, Luigi Lo Iacono, Dominik Wermke, Christian Stransky, Sebastian Möller, Yasemin Acar, and Sascha Fahl. 2018. Developers Deserve Security Warnings, Too: On the Effect of Integrated Security Advice on Cryptographic API Misuse. In *USENIX Symposium on Usable Privacy and Security (SOUPS)*.

[30] Julie M Haney and Wayne G Lutters. 2018. "It's Scary...It's Confusing...It's Dull": How Cybersecurity Advocates Overcome Negative Perceptions of Security. In *USENIX Symposium on Usable Privacy and Security (SOUPS)*.

[31] Julie M Haney, Mary Theofanos, Yasemin Acar, and Sandra Spickard Prettyman. 2018. "We make it a big deal in the company": Security Mindsets in Organizations that Develop Cryptographic Products. In *USENIX Symposium on Usable Privacy and Security (SOUPS)*.

[32] Michael Hilton, Nicholas Nelson, Timothy Tunnell, Darko Marinov, and Danny Dig. 2017. Trade-Offs in Continuous Integration: Assurance, Security, and Flexibility. In *Joint Meeting on Foundations of Software Engineering (ESEC/FSE)*.

[33] Iulia Ion, Rob Reeder, and Sunny Consolvo. 2015. "... No one Can Hack My Mind": Comparing Expert and Non-Expert Security Practices. In *USENIX Symposium on Usable Privacy and Security (SOUPS)*.

[34] Fotis Kitsios, Elpiniki Chatzidimitriou, and Maria Kamariotou. 2023. The ISO/IEC 27001 information security management standard: how to extract value from data in the IT sector. *Sustainability* (2023).

[35] Lawrence L Kupper and Kerry B Hafner. 1989. On Assessing Interrater Agreement for Multiple Attribute Responses. *Biometrics* 45, 3 (1989), 957–967.

[36] Marlene Z Ladendorff. 2016. *The effect of the NERC CIP Standards on the reliability of the North American bulk electric system.* Technical Report. Idaho National Lab (INL).

[37] John Livingston. 2025. NERC CIP Standards: Safeguarding North America's Power Grid. https://verveindustrial.com/resources/blog/what-are-the-nerc-cip-standards-in-ics-security/

[38] Masike Malatji, Annlizé L Marnewick, and Suné Von Solms. 2022. Cybersecurity capabilities for critical infrastructure resilience. *Information & Computer Security* (2022).

[39] Alessandro Mantovani, Simone Aonzo, Yanick Fratantonio, and Davide Balzarotti. 2022. RE-Mind: a first look inside the mind of a reverse engineer. In *USENIX Security Symposium*.

[40] NERC. 2024. Compliance Monitoring and Enforcement Program and Organization Registration and Certification Program Mid-Year Report. https://www.nerc.com/pa/comp/CE/ReportsDL/2024%20CMEP%20and%20ORCP%20Mid-Year%20Report.pdf

[41] NERC. 2025. CIP-007-5 Systems Security Management. https://www.nerc.com/pa/Stand/Project20086CyberSecurityOrder706Version5CIPStanda/CIP-007-5_clean_20111107.pdf

[42] NERC. 2025. Critical Infrastructure Protection. https://www.nerc.com/pa/Stand/Pages/ReliabilityStandards.aspx

[43] NERC. 2025. Organization Registration and Certification Program and Compliance Monitoring and Enforcement Program Annual Report. https://www.nerc.com/pa/comp/CE/ReportsDL/2023%20CMEP%20and%20ORCP%20Annual%20Report.pdf

[44] David Nevius. 2020. *The History of the North American Electric Reliability Corporation.* NERC.

[45] Udoka Ngozi Nwizu. 2025. Securing America's Critical Infrastructure: Strengthening Compliance with NERC Cybersecurity Standards. *Journal of Technology and Systems* (2025).

[46] U.S Department of Energy. 2024. Cybersecurity Strategy. https://www.energy.gov/cio/articles/doe-cybersecurity-strategy-2024

[47] U.S. Government Accountability Office. 2025. Critical Infrastructure Protection: Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid. https://www.gao.gov/products/gao-19-332

[48] Network Perception. 2025. NERC-CIP Compliance Software. https://www.network-perception.com/solutions/nerc-cip-compliance

[49] Matteo Podrecca, Giovanna Culot, Guido Nassimbeni, and Marco Sartor. 2022. Information security and value creation: The performance implications of ISO/IEC 27001. *Computers in Industry* (2022).

[50] Andreas Poller, Laura Kocksch, Sven Türpe, Felix Anand Epp, and Katharina Kinder-Kurlanda. 2017. Can Security Become a Routine?: A Study of Organizational Change in an Agile Software Development Group.

[51] Sena Sahin. 2025. The Challenges and Opportunities with Cybersecurity Regulations: A Case Study of the US Electric Power Sector - Replication Package. https://osf.io/hyrzm/

[52] Sena Sahin, Suood Al Roomi, Tara Poteat, and Frank Li. 2023. Investigating the Password Policy Practices of Website Administrators. In *IEEE Symposium on Security and Privacy (S&P)*.

[53] Dave Schmitt. 2025. NERC CIP Compliance: What you should know. https://blogs.cisco.com/industrial-iot/nerc-cip-compliance-what-you-should-know

[54] John Shaw. 2025. NERC CIP Compliance: Headache or Opportunity? https://www.renewableenergyworld.com/energy-business/policy-and-regulation/nerc-cip-compliance-headache-or-opportunity/

[55] Brian Singer, Amritanshu Pandey, Shimiao Li, Lujo Bauer, Craig Miller, Lawrence Pileggi, and Vyas Sekar. 2023. Shedding light on inconsistencies in grid cybersecurity: Disconnects and recommendations. In *IEEE Symposium on Security and Privacy (S&P)*.

[56] Rebecca Slayton and Aaron Clark-Ginsberg. 2018. Beyond regulatory capture: Coproducing expertise for critical infrastructure protection. *Regulation & governance* (2018).

[57] Rock Stevens, Josiah Dykstra, Wendy Knox Everette, James Chapman, Garrett Bladow, Alexander Farmer, Kevin Halliday, and Michelle L Mazurek. 2020. Compliance Cautions: Investigating Security Issues Associated with US Digital-Security Standards.. In *Network and Distributed System Security Symposium (NDSS)*.

[58] Rock Stevens, Faris Bugra Kokulu, Adam Doupé, and Michelle L Mazurek. 2022. Above and Beyond: Organizational Efforts to Complement US Digital Security Compliance Mandates. In *Network and Distributed System Security Symposium (NDSS)*.

[59] Rock Stevens, Daniel Votipka, Josiah Dykstra, Fernando Tomlinson, Erin Quartararo, Colin Ahern, and Michelle L Mazurek. 2022. How ready is your ready? Assessing the usability of incident response playbook frameworks. In *ACM CHI Conference on Human Factors in Computing Systems (CHI)*.

[60] Christian Stransky, Yasemin Acar, Duc Cuong Nguyen, Dominik Wermke, Doowon Kim, Elissa M Redmiles, Michael Backes, Simson Garfinkel, Michelle L Mazurek, and Sascha Fahl. 2017. Lessons Learned from Using an Online Platform to Conduct Large-Scale, Online Controlled Security Experiments with Software Developers. In *USENIX Workshop on Cyber Security Experimentation and Test (CSET)*.

[61] Timothy Summers, Kalle J Lyytinen, Tony Lingham, and Eugene A Pierce. 2013. How hackers think: A study of cybersecurity experts and their mental models. In *Annual International Conference on Engaged Management Scholarship*.

[62] The White House. 2009. Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure. https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-044.pdf

[63] Mary Theofanos, Brian Stanton, Susanne Furman, Sandra Spickard Prettyman, and Simson Garfinkel. 2017. Be prepared: how US government experts think about cybersecurity. In *Workshop on Usable Security (USec)*.

[64] Tyler W Thomas, Madiha Tabassum, Bill Chu, and Heather Lipford. 2018. Security During Application Development: an Application Security Expert Perspective. In *ACM CHI Conference on Human Factors in Computing Systems (CHI)*.

[65] Sven Turpe, Laura Kocksch, and Andreas Poller. 2016. Penetration Tests a Turning Point in Security Practices? Organizational Challenges and Implications in a Software Development Team. In *USENIX Symposium on Usable Privacy and Security (SOUPS)*.

[66] U.S. Department of Energy. 2017. *Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector.* Technical Report. Office of Electricity Delivery and Energy Reliability.

[67] U.S. Energy Information Administration. 2025. Retail Sales. https://www.eia.gov/opendata/browser/electricity/retail-sales?frequency=annual&data=customers;price;revenue;sales;&facets=stateid;sectorid;&stateid=US;&sectorid=ALL;&start=2001&end=2024&sortColumn=period;&sortDirection=desc;

[68] US NIST. 2006. Minimum Security Requirements for Federal Information and Information Systems. https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.200.pdf

[69] US NIST. 2020. Security and Privacy Controls for Information Systems and Organizations. https://doi.org/10.6028/NIST.SP.800-53r5

[70] Artem Voronkov, Leonardo A Martucci, and Stefan Lindskog. 2019. System Administrators Prefer Command Line Interfaces, Don't They? An Exploratory Study of Firewall Interfaces. In *USENIX Symposium on Usable Privacy and Security (SOUPS)*.

[71] Daniel Votipka, Kelsey R Fulton, James Parker, Matthew Hou, Michelle L Mazurek, and Michael Hicks. 2020. Understanding security mistakes developers make: Qualitative analysis from build it, break it, fix it. In *USENIX Security Symposium*.

[72] Daniel Votipka, Rock Stevens, Elissa Redmiles, Jeremy Hu, and Michelle Mazurek. 2018. Hackers vs. testers: A comparison of software vulnerability discovery processes. In *IEEE Symposium on Security and Privacy (S&P)*.

[73] Sophie Westlake. 2023. Share of Women in Selected Energy-related Occupations. https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/enforce-password-history

[74] Michael E Whitman and Herbert J Mattord. 2007. Management of information security. (2007).

[75] Flynn Wolf, Adam J Aviv, and Ravi Kuber. 2021. Security Obstacles and Motivations for Small Businesses from a CISO's Perspective. In *USENIX Security Symposium*.

[76] Virginia L Wright et al. 2023. *Cyber-Informed Engineering Implementation Guide.* Technical Report. Idaho National Laboratory (INL).

[77] Verena Zimmermann and Karen Renaud. 2019. Moving from a 'human-as-problem" to a 'human-as-solution" cybersecurity mindset. *International Journal of Human-Computer Studies* (2019).