Journal of Crime and Criminal Behavior
Vol. 5, No. 1, 2025, pp. 103-144

URL: www.arfjournals.com
https://doi.org/10.47509/JCCB.2025.v05i01.06

Cyber Security Laws, Regulation, and Policy Frameworks for SCADA Systems and Mitigating Threats to Critical Infrastructures

Tiffany Weitoish
Capitol Technology University. E-mail: ttoish@gmail.com

TO CITE THIS ARTICLE

Tiffany Weitoish (2025). Cyber Security Laws, Regulation, and Policy Frameworks for SCADA Systems and Mitigating Threats to Critical Infrastructures. *Journal of Crime and Criminal Behavior,* 5: 1, pp. 103-144. *https://doi.org/10.47509/JCCB.2025.v05i01.06*

Abstract: Supervisory Control and Data Acquisition (SCADA) systems are the backbone of critical infrastructures, including energy, water, transportation, and manufacturing. However, the increasing interconnectedness and reliance on SCADA systems have exposed them to cyber threats, ranging from unauthorized access to system manipulation and sabotage. This research delves into the laws, regulations, and policy frameworks designed to address these vulnerabilities and safeguard critical infrastructures. It explores the evolving landscape of SCADA security, highlighting the importance of comprehensive risk management strategies and proactive measures. This chapter aims to provide insights into the challenges faced by policymakers, industry stakeholders, and cybersecurity experts in ensuring the resilience of SCADA systems against emerging threats. The research discusses the need for collaboration between government agencies, private sector entities, and international partners to develop robust frameworks that promote information sharing, threat intelligence, and incident response capabilities. Through a multidisciplinary approach, this chapter underscores the urgency of adopting adaptive strategies to mitigate the evolving risks posed by cyber threats to critical infrastructures that rely on SCADA systems.

Keywords: Supervisory Control and Data Acquisition (SCADA), Risk Management, Cybersecurity Framework, Threat Landscape, and Regulatory Compliance

Introduction

Supervisory Control and Data Acquisition (SCADA) systems play a pivotal role in modern society, providing real-time monitoring and control of critical infrastructures

Received : 20 April 2025 • **Revised :** 18 May 2025 • **Accepted :** 23 May 2025 • **Published :** 1 June 2025

such as energy, water, transportation, and manufacturing. However, increasing reliance on interconnected digital systems has introduced unprecedented cybersecurity challenges, exposing SCADA systems to diverse threats. From malicious actors seeking to disrupt operations to state-sponsored cyberattacks aiming to undermine national security, the vulnerabilities inherent in SCADA systems have become a focal point for policymakers, industry stakeholders, and cybersecurity experts. This research delves into the complex landscape of cybersecurity law, regulations, and policy frameworks that are instrumental in safeguarding SCADA systems against evolving cybersecurity threats.

Historically, SCADA systems have been susceptible to cybersecurity threats due to their critical role and inherent vulnerabilities. In response to these evolving threats, policymakers and regulatory bodies have been tasked with developing comprehensive frameworks to safeguard SCADA systems and protect critical infrastructures from potential disruptions. Despite significant advancements in cybersecurity measures, there remain pressing concerns about the adequacy of existing frameworks to deter and withstand cybersecurity violations effectively. The rapid technological advancements and sophisticated nature of modern cyber threats frequently outpace current regulations, challenging their efficacy and enforcement, which requires continuous updates and adaptations. In addition, the enforcement of these frameworks varies widely across sectors and organizations, contributing to inconsistent levels of security in SCADA systems across different domains. This inconsistency can undermine the overall effectiveness of national cybersecurity strategies, leaving certain areas more vulnerable than others. Therefore, while the current regulatory frameworks have laid a critical foundation for protecting SCADA systems, ongoing assessment, revision, and enforcement of these policies are essential. It is only through a dynamic, responsive regulatory approach that cybersecurity professionals, lawmakers, and researchers keep pace with the evolving cybersecurity threats and provide a true deterrent to violations that jeopardize critical infrastructure.

This research sets the stage for a deeper exploration of the cybersecurity laws, regulations, and policy measures and frameworks implemented to address these challenges and enhance the resilience of these systems. This study examines the contributions of cybersecurity frameworks, focusing on laws, regulations, policies, and the National Institute of Standards and Technology (NIST) related to

SCADA systems and critical infrastructures. For instance, the National Institute of Standards and Technology (NIST) promotes innovation by advancing measurement science, standards, and technology, which has also been instrumental in defining cybersecurity standards that are pivotal for SCADA systems. In addition, the NIST guidelines, such as NIST SP 800-53 Rev 5, provide updated security and privacy controls for federal information systems and organizations, which are critical for protecting SCADA systems against evolving cyber threats (NIST, 2020). The NIST Cybersecurity Framework (CSF) 2.0 also outlines standards, guidelines, and best practices to manage cybersecurity risks at a sector-specific level, including those pertinent to SCADA systems (NIST, 2024). These guidelines offer a structured approach to managing cybersecurity risks tailored to SCADA systems, which promotes resilience and robust security measures.

The U.S. government has also played a proactive role through executive orders to strengthen the cybersecurity of federal networks and critical infrastructures, directly affecting SCADA systems within government operations. Executive Order 13800 and Executive Order 14028 highlight initiatives to enhance the cybersecurity of federal networks and critical infrastructures, which directly impact SCADA systems within government operations (The White House, 2017; The White House, 2021). Establishing robust and comprehensive cybersecurity frameworks and issuing targeted executive orders demonstrate a proactive governmental approach to securing SCADA systems. These initiatives are crucial given the vulnerabilities inherent in SCADA systems, which have been historically focused more on operational efficiency than on security. The frameworks and policies guide the technical measures needed to protect these systems and foster a collaborative environment among government agencies, industry partners, and international bodies to address cybersecurity threats collectively.

The integration of NIST guidelines and federal directives underscores a comprehensive approach to SCADA system security, ensuring that these critical systems are equipped to handle the sophisticated landscape of cyber threats. By examining the policy development and the implementation through technical, legal, and operational lenses, it becomes clear that securing SCADA systems against cyber threats is a dynamic and multifaceted endeavor requiring ongoing adaptation and cooperation across various sectors. This paper seeks to elucidate the key issues, debates, and considerations surrounding the development and implementation of

policies and regulations governing SCADA systems. This research will provide insights into gaps related to SCADA systems in the current cybersecurity landscape through a detailed exploration of laws, regulations, and policies. This paper seeks to propose actionable strategies and recommendations for policymakers, industry leaders, and cybersecurity professionals to improve the security and resilience of critical infrastructures, ensuring they are equipped to face the challenges of an increasingly digitalized world.

Problem Statement

The escalating reliance on SCADA systems across critical infrastructures such as energy, water, and transportation has intensified the exposure of these vital sectors to cybersecurity threats. This exposure highlights the urgency for enhanced protective measures and robust regulatory frameworks to effectively counteract threats ranging from cyber espionage and sabotage to ransomware attacks and insider threats, which pose a significant risk to the stability, resilience, and security of vital sectors such as energy, water, transportation, and manufacturing. Despite persistent efforts to fortify security, significant gaps and vulnerabilities persist, often exacerbated by outdated infrastructures, increased interconnectivity, and the swift evolution of technology.

The burgeoning problem revolves around the need for robust laws, regulations, and policy frameworks to effectively mitigate these threats and safeguard critical infrastructures against potential disruptions. Initiatives such as NIST SP 800-53 Rev 5 provide crucial security and privacy controls for federal information systems, including SCADA systems (NIST, 2020). In addition, executive orders like EO 13800 and EO 14028 have been pivotal in strengthening the cybersecurity framework that affects SCADA systems directly (The White House, 2017; The White House, 2021). However, despite these advancements, current regulatory measures often fail to offer comprehensive guidance and robust enforcement mechanisms necessary to counteract cyber threats' dynamic and complex nature.

In addition, the inconsistency in regulatory regimes, disparate levels of cybersecurity maturity across different sectors, and the limited scope of information sharing pose additional challenges. These issues complicate the development of unified and effective strategies to enhance resilience and bolster response capabilities against cyber threats. Therefore, there are critical challenges for policymakers, industry stakeholders, and cybersecurity experts in finding the optimal balance

between fostering innovation and ensuring security, all while maintaining the uninterrupted operation of essential services amid evolving cyber threats.

This study aims to elucidate the complexities of this problem and identify key significant gaps and deficiencies within existing laws, regulations, and policy frameworks. By critically analyzing these frameworks and identifying areas needing improvement, this research endeavors to inform and guide efforts to enhance the security and resilience of SCADA systems. The ultimate goal is to contribute to developing more robust cybersecurity measures that address current threats and are adaptable to future challenges, thus ensuring the protection and stability of critical infrastructures in an increasingly digital world.

Purpose and Nature of the Study

This study aims to critically examine the existing laws, regulations, and policy frameworks governing Supervisory Control and Data Acquisition (SCADA) systems, aiming to mitigate cybersecurity threats to critical infrastructures. The study seeks to explore the current landscape of SCADA security, identify key challenges and gaps within existing laws, regulations, and policies, and propose recommendations to enhance the resilience and security of critical infrastructures. Furthermore, it proposes strategic recommendations aimed at bolstering the resilience and security of critical infrastructures, thereby enhancing their capacity to withstand and respond to cyber threats.

By adopting an interdisciplinary approach, this study draws on insights from legal, technical, and operational perspectives to provide a holistic understanding of the complex issues surrounding SCADA security. Essential regulatory guidelines such as the NIST SP 800-53 Rev 5 provide a baseline for evaluating the adequacy of security and privacy controls essential for protecting SCADA systems against evolving cyber threats (NIST, 2020). Similarly, executive orders such as EO 13800 and EO 14028 highlight governmental efforts to strengthen the cybersecurity of federal networks and critical infrastructures, directly impacting the security practices around SCADA systems (The White House, 2017; The White House, 2021).

By synthesizing existing literature, analyzing regulatory documents, and incorporating insights from industry experts, the study identifies a critical need for updates and enhancements to address the complex nature of modern cyber threats while elucidating the interplay between laws, regulations, and policies,

and cybersecurity in the context of critical infrastructure protection. Through a combination of qualitative analysis and evidence-based research, this research aims to bridge the knowledge gap in SCADA security by offering actionable insights and forward-thinking recommendations to the ongoing discourse on SCADA for policymakers, regulatory bodies, industry stakeholders, and cybersecurity professionals. By fostering dialogue and collaboration among policymakers, regulatory bodies, and industry stakeholders, the study seeks to spur innovation and strategic action to enhance the security postures of critical infrastructure sectors reliant on SCADA systems.

Significance of the Study

The significance of this study in examining SCADA systems' security extends across multiple domains, including influencing policymakers, regulatory bodies, industry stakeholders, and the broader society. By emphasizing and enhancing resilience, this research delineates critical gaps and deficiencies within current legal, regulatory, and policy frameworks governing SCADA systems. These frameworks play a pivotal role in safeguarding critical infrastructures, as outlined by the Federal Information Security Modernization Act (FISMA) of 2014 (113th Congress, 2014). The study focuses on enhancing resilience, informing policy development, strengthening collaboration, mitigating risks, and safeguarding societal well-being, thereby playing a crucial role in enhancing the security posture of critical infrastructures. These facets are integral to bolstering the security posture of critical infrastructures.

The study serves as a crucial resource for informing policy development, providing a comprehensive overview of the current policy landscape surrounding SCADA security. This is critical for regulatory bodies tasked with developing and implementing security measures, as emphasized by the Cybersecurity & Infrastructure Security Agency's efforts in establishing governance frameworks and industrial control systems security measures (CISA, 2024a; 2024b). By fostering collaboration among various stakeholders, including government agencies, industry partners, and international entities, the study promotes a unified approach to addressing SCADA security challenges.

This research enhances policy frameworks and focuses on mitigating risks by equipping cybersecurity professionals with actionable recommendations to enhance the security of SCADA systems. This proactive approach contributes to the

infrastructure's stability, reliability, and security, which are crucial for society's well-being. The NIST SP 800-53 Rev. 5 guidelines and the Cybersecurity Framework (CSF) 2.0 provide foundational security controls and best practices (NIST, 2020; 2024a).

By highlighting the gaps in existing policies and suggesting areas for enhancement, the study catalyzes the development of more resilient infrastructures, encouraging a collaborative approach among various stakeholders to share knowledge and coordinate efforts against cyber threats. This collaborative impact is vital for evolving cybersecurity measures, ensuring they are comprehensive and proactive in addressing both current and emerging threats. The research contributes to academic debate and plays a crucial role in shaping future policy formulations and strategic decisions in cybersecurity practices, supporting societal stability and economic continuity. By mitigating the risks posed by cyber threats to essential services such as energy, water, transportation, and manufacturing, the study helps ensure the uninterrupted delivery of vital services that protect against potential disruptions that could have far-reaching consequences for society.

The research is supported by robust guidelines and frameworks, such as the NIST SP 800-53 Rev 5, which provides a comprehensive set of security controls for information systems and organizations that include SCADA systems (NIST, 2020). In addition, executive orders like EO 13636 and EO 14028 illustrate government efforts to bolster the cybersecurity framework affecting SCADA systems (The White House, 2013; The White House, 2021). By highlighting the gaps in the current policies and suggesting areas for enhancement, the study aids in developing more resilient infrastructures. It encourages a collaborative approach among various stakeholders to share knowledge and coordinate efforts against cyber threats. This collaborative impact is crucial for evolving cybersecurity measures and ensuring they are comprehensive and proactive, addressing both current and potential threats. The study is a cornerstone for future policy formulations and strategic decisions in cybersecurity practices, emphasizing the need for forward-thinking strategies.

Literature Review

The literature on cybersecurity laws, regulations, and policy frameworks for mitigating threats to critical infrastructures, particularly those related to Supervisory Control and Data Acquisition (SCADA) systems, encompasses diverse perspectives,

methodologies, and findings. This review synthesizes key themes, trends, and insights from existing research to provide a comprehensive understanding of the current state of knowledge in cybersecurity, such as the evolution of SCADA systems from isolated entities to highly interconnected frameworks susceptible to various cyber threats, necessitating robust security measures (NIST, 2024).

The "Historical Context and Evolution of SCADA Security" discusses the literature on SCADA security and often begins with exploring the historical context and evolution of cyber threats targeting critical infrastructures. Early studies highlight the transition from isolated, proprietary SCADA systems to interconnected, internet-enabled networks, which has increased the attack surface and exposed vulnerabilities to a broader range of threats. Studies like those by Ross and Pillitteri (2024) discuss the importance of safeguarding sensitive information across nonfederal systems, while executive orders detail governmental efforts to strengthen the cybersecurity framework affecting SCADA systems (The White House, 2021). Reviewing historical SCADA security to the current threat landscape allows for analyzing prevalent risks while evaluating the robustness of existing security frameworks in mitigating threats.

The "Threat Landscape and Vulnerability Analysis" provides research and an examination of the threat landscape facing SCADA systems, identifying common attack vectors, threat actors, and tactics used to exploit vulnerabilities. Researchers assess the effectiveness of these frameworks in addressing emerging cyber threats and propose recommendations for improvement with the analysis of attack vectors, identifying the methods and tactics used by threat actors to exploit system weaknesses. This is crucial in understanding the security posture of SCADA systems, which are often highlighted as points of vulnerability in network architecture, software design, and configuration practices. Reviewing the effectiveness of current frameworks in threat mitigation will determine how legislation and regulatory guidelines shape security practices for SCADA systems. This analysis is crucial for assessing existing regulations' adequacy and identifying potential areas where policy might be strengthened to better protect critical infrastructures from evolving cybersecurity challenges.

The "Policy and Regulation Frameworks" focuses on analyzing existing policies and regulation frameworks governing SCADA security. This comprehensive review examines key legislation, such as the Federal Information Security Modernization

Act (FISMA) of 2014, which mandates ongoing federal agency evaluations of information security programs to protect critical information infrastructure, including SCADA systems (113th Congress, 2014). The analysis extends to cybersecurity governance frameworks established by authoritative bodies like the National Institute of Standards and Technology (NIST) such as NIST SP 800-53 Rev. 5 and NIST SP 800-82, aimed at securing operation technology environments (NIST, 2020; Stouffer *et al*., 2023).

The "Legal Framework of Cybersecurity Laws" refers to the collection of statutes, regulations, and case law that governs how organizations, individuals, and governments handle cybersecurity. This framework protects information systems and data from unauthorized access, attacks, theft, or damage. It covers various aspects such as data privacy, critical infrastructure protection, cybercrime, and incident reporting. The U.S. legal framework of cybersecurity laws concerning SCADA systems and critical infrastructure is composed of a variety of federal regulations and standards designed to protect these essential systems from cyber threats. SCADA systems are crucial for managing operations in critical infrastructure sectors such as water treatment, power generation and distribution, oil and gas refining, and transportation. The following are key components of the U.S. legal framework related to cybersecurity for SCADA systems and critical infrastructures and encompasses a variety of statutes, regulations, and directives designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access.

Federal Laws and Regulations

National Security Laws refer to the legal frameworks designed to protect a nation from potential threats, including espionage, terrorism, sabotage, and warfare. These laws typically focus on safeguarding national interests, maintaining the security of the people, and preserving critical infrastructures and essential resources. The national security laws specifically address cybersecurity, SCADA systems, and critical infrastructures and are designed to protect vital systems from cyber threats, espionage, and terrorist activities. These laws help safeguard systems that control essential services such as electricity, water, transportation, and communication. Essential national security laws and regulations in the United States explicitly target the enhancement of cybersecurity and protecting critical infrastructure. Among these, the Cybersecurity Information Sharing Act (CISA) of 2015 stands

out by promoting the exchange of cybersecurity threat information between the government and private sectors, a move that crucially bolsters the defenses of critical infrastructures, including SCADA systems. Additionally, the Patriot Act, primarily focused on anti-terrorism efforts, incorporates provisions aimed at augmenting the capabilities of government agencies to monitor and counteract cyber threats, thereby reinforcing national security measures. Complementing these acts, Homeland Security Presidential Directive 7 (HSPD-7) delineates a national policy that mandates Federal departments and agencies to identify and prioritize critical infrastructure and key resources for protection against terrorist attacks.

Furthermore, the Federal Information Security Management Act (FISMA) plays a pivotal role by requiring federal agencies to develop, document, and implement comprehensive information security and protection programs. Although directly applicable to federal entities, FISMA's principles extend their influence on the security protocols governing critical infrastructures, including those involving SCADA systems. Moreover, the National Defense Authorization Act (NDAA) continually integrates provisions that address cybersecurity defenses, reflecting a dynamic legislative approach to the evolving spectrum of threats. Together, these laws form a cohesive structure that not only addresses immediate cybersecurity concerns but also fosters a resilient infrastructure capable of withstanding future challenges.

The Homeland Security Act of 2002 and the Critical Infrastructure Protection (CIP) Standards were established by the Department of Homeland Security (DHS) and that led to the creation of the Cybersecurity and Infrastructure Security Agency (CISA), which focuses on enhancing the security, resilience, and reliability of the nation's cybersecurity and communications infrastructure. The Cybersecurity Infrastructure Security Agency (CISA) is recognized as America's Cyber Defense Agency, which provides extensive resources and guidance on industrial control systems (ICS), including SCADA systems, that are critical to the nation's infrastructure. CISA emphasizes the strategic importance of protecting these systems due to their critical role in various sectors, such as energy, water, and transportation (CISA, 2024). CISA's resources are designed to assist stakeholders in enhancing the resilience and security of these systems against potential cyber threats. CISA's offerings include risk assessment tools, best practices for cybersecurity, and real-time monitoring and incident response capabilities. This guidance is essential

for ensuring the operational continuity and security of critical infrastructures that rely heavily on SCADA systems, addressing the evolving nature of cybersecurity threats and the specific vulnerabilities associated with industrial control systems.

The Computer Fraud and Abuse Act (CFAA) was initially enacted in 1986 and is a critical piece of legislation in the United States that addresses cybercrime, specifically targeting unauthorized access and damage to computer systems, including those integral to SCADA systems and critical infrastructure. As outlined by the Congressional Research Service (2020) and the U.S. Department of Justice (2015), the CFAA serves as the primary federal law to combat computer-related offenses, offering a legal framework to protect computer networks against various forms of cyber intrusion and attacks. The CFAA is especially pertinent to the security of SCADA systems, which operate within critical infrastructure sectors such as energy, water, and transportation. Under the CFAA, activities such as accessing a computer without authorization, exceeding authorized access, and transmitting harmful programs or information are deemed illegal (CRS, 2020; DOJ, 2015). This legislation not only helps prosecute cybercriminals but also acts as a deterrent against potential threats to the nation's critical operational frameworks. The relevance of the CFAA in the context of national security is underscored by its application in protecting systems that maintain essential public and economic functions, thus ensuring the stability and security of critical infrastructure against evolving cyber threats.

The Federal Information Security Modernization Act (FISMA) of 2014, enacted by the 113th Congress, represents a significant legislative step in evolving national cybersecurity strategies, particularly impacting SCADA systems and critical infrastructures. As outlined in Public Law 113-283, FISMA 2014 updates the federal government's approach to cybersecurity, emphasizing a continuous monitoring and risk management framework. This act is crucial for enhancing the security of information systems that underpin the nation's critical infrastructures, including power grids, water treatment facilities, and transportation systems, which often rely on SCADA systems for operational control. FISMA mandates federal agencies to develop, document, and implement an agency-wide program to secure their information and systems, which includes requirements for periodic assessments of risk, policies for information security, and plans for action based on risk assessments (113th Congress, 2014). The importance of FISMA lies in its

requirement for agencies to report compliance annually, ensuring ongoing oversight and adaptation of security practices in line with current threats, thereby reinforcing the resilience and security of essential services against cyber threats.

Sector-Specific Regulations

Different sectors of critical infrastructures are overseen by specific federal agencies. For example, the Environmental Protection Agency (EPA) is responsible for water systems and has recognized the importance of cybersecurity within the water sector, emphasizing the necessity to protect SCADA systems that operate critical water infrastructure. The document titled "EPA Cybersecurity for the Water Sector" outlines a strategic approach adopted on December 23, 2020, to enhance the resilience and security of water systems against potential cyber threats. The EPA underscores the implementation of robust cybersecurity practices as essential to safeguarding the water sector's infrastructure, which is vital for public health and safety. The guidance provided by the EPA includes recommendations for risk assessment, response strategies, and the adoption of best practices in cybersecurity (EPA, 2020). These measures are aimed at helping water utilities detect vulnerabilities, mitigate risks, and respond to incidents effectively, thereby ensuring the continued safety and reliability of water services across the nation. This initiative reflects a broader commitment to securing critical infrastructure from cyber threats, aligning with national security objectives, and protecting public welfare (EPA, 2020).

The Department of Energy (DOE) oversees the energy sector and has played a pivotal role in enhancing the cybersecurity of SCADA networks, which are integral to critical infrastructure operations. On September 9, 2002, the DOE released a foundational document titled "21 Steps to Improve Cyber Security of SCADA Networks," which serves as a comprehensive guide for securing these systems. This document outlines a structured approach to safeguarding SCADA networks from cyber threats. It provides a detailed set of actionable recommendations that organizations can implement to enhance their cybersecurity measures. These steps include assessing risks, securing remote access points, implementing robust authentication and authorization practices, and ensuring physical security (DOE, 2002). The guide emphasizes the importance of a layered security approach to protect the integrity, availability, and confidentiality of critical operational data. By following these steps, entities involved in critical infrastructure sectors can significantly

mitigate their exposure to cyberattacks, thereby strengthening national security and the reliability of essential services (DOE, 2002). The DOE's initiative highlights its commitment to leading national efforts in securing critical infrastructure from evolving cyber threats, ensuring a resilient energy framework for the United States.

The Health Insurance Portability and Accountability Act (HIPAA) sets the standard for protecting sensitive patient data. Any company that deals with protected health information (PHI) must ensure that all the required physical, network, and process security measures are in place and followed (NIST, 2024). The National Institute of Standards and Technology (NIST) has provided vital resources for entities regulated by the Health Insurance Portability and Accountability Act (HIPAA), particularly those managing SCADA systems within critical infrastructures. The "NIST SP 800-66 Rev 2: Cybersecurity Resources for HIPAA-Regulated Entities" offers comprehensive guidelines to enhance the cybersecurity posture of these entities. This publication underscores the integration of cybersecurity measures with HIPAA compliance, emphasizing the protection of electronic protected health information (ePHI) within SCADA environments that are increasingly connected to healthcare networks (NIST, 2024). NIST's recommendations include adopting a risk management framework, ensuring adequate access controls, and monitoring systems for potential cybersecurity threats. The document advocates for a proactive approach to securing systems by aligning HIPAA's administrative, physical, and technical safeguards with modern cybersecurity practices (NIST, 2024). This alignment is crucial for entities operating at the intersection of healthcare and critical infrastructure, ensuring that they not only comply with legal requirements but also strengthen their defenses against evolving cyber threats (NIST, 2024).

The Gramm-Leach-Bliley Act (GLBA) requires financial institutions to explain their information-sharing practices to their customers and to safeguard sensitive data. The Congressional Research Service's report on "Banking, Data Privacy, and Cybersecurity Regulation," released on March 13, 2023, which provides a detailed analysis of the Gramm-Leach-Bliley Act (GLBA) and its implications for cybersecurity within the banking sector and critical infrastructures including SCADA systems. This document emphasizes the importance of safeguarding financial data through stringent cybersecurity measures as mandated by the GLBA. It highlights how financial institutions and related entities, which may include operators of SCADA systems involved in financial operations, must implement

comprehensive security programs to protect customer information (CRS, 2023). The report discusses the evolving nature of cyber threats and the corresponding need for robust cybersecurity protocols that align with both GLBA requirements and the broader regulatory landscape. This includes a focus on ensuring the integrity and security of SCADA systems that might handle financial data or connect to financial networks, underscoring the act's relevance beyond traditional banking environments to include other critical infrastructure sectors (CRS, 2023). The synthesis of data privacy and cybersecurity in this context underscores the necessity for a multidimensional approach to compliance and security strategy formulation within and beyond the financial industry.

The Federal Energy Regulatory Commission (FERC) emphasizes the critical importance of cybersecurity within the energy sector, particularly concerning SCADA systems and other critical infrastructure components, through its dedicated resource on "Cyber and Grid Security." This resource outlines FERC's regulatory and oversight activities aimed at enhancing the security and resilience of the national electric grid (FERC, 2023). The document details the commission's ongoing efforts to enforce rigorous cybersecurity standards, monitor compliance, and respond to emerging threats that could compromise the integrity and functionality of SCADA systems. FERC's proactive approach includes collaborations with other federal agencies and private sector partners to fortify cybersecurity measures across the energy landscape (FERC, 2023). This effort is vital for maintaining system reliability and protecting against potential disruptions caused by cyber-attacks. The summary encapsulates FERC's commitment to safeguarding the United States' energy infrastructure through enhanced security protocols, continuous oversight, and adaptive regulatory frameworks that address the dynamic nature of cyber threats.

North American Electric Reliability Corporation (NERC) regulates the cybersecurity standards for the U.S. power grid. The North American Electric Reliability Corporation (NERC) plays a pivotal role in ensuring the stability and security of the electrical grid across North America, particularly emphasizing the oversight of SCADA systems and other critical infrastructure components. The NERC's "Reliability Standards" provides comprehensive guidelines designed to uphold and enhance the reliability of the power system. These standards are critical for preventing and mitigating system disturbances resulting from cyber

threats and other vulnerabilities (NERC, 2024). The document elaborates on various requirements that system operators, utilities, and other stakeholders must adhere to, encompassing areas such as system protection, control, and incident reporting. By establishing a rigorous compliance framework, NERC seeks to foster a secure, resilient, and reliable energy infrastructure. This effort is crucial in the context of increasing cyber threats targeting critical infrastructures, highlighting the significance of NERC's standards in the ongoing battle to protect national security and public safety. The NERC standards underscore the importance of a proactive and enforced approach to enhancing electrical grid reliability through comprehensive standards and continuous adaptation to the evolving landscape of threats and technological advancements.

The National Institute of Standards and Technology (NIST) Guidelines

The National Institute of Standards and Technology (NIST) Cybersecurity Framework provides a policy framework of computer security guidance for how private sector organizations in the U.S. can assess and improve their ability to prevent, detect, and respond to cyber-attacks. NIST has developed several special publications that are particularly relevant to the cybersecurity of SCADA systems within critical infrastructures. The integration of applicable NIST regulations within the United States policies and regulation frameworks underscores a systematic approach to enhancing cybersecurity across various sectors. The NIST Cybersecurity Framework (CSF) provides a voluntary, risk-based approach for organizations to manage and improve their cybersecurity posture through comprehensive guidelines and best practices. It offers a set of guidelines, standards, and best practices for identifying, protecting, detecting, responding to, and recovering from cyber threats. Organizations can use the CSF to develop customized cybersecurity programs tailored to their specific needs and priorities, including those related to securing SCADA systems and critical infrastructures (NIST, 2024).

The NIST Special Publication 800-82 Rev 3: Guide to Operational Technology (OT) Security provides guidance for securing industrial control systems (ICS), including SCADA systems, within critical infrastructure sectors. It offers recommendations for assessing ICS security risks, implementing security controls, and managing ICS security programs. The publication addresses topics such as network architecture, access control, incident response, and security

awareness training relevant to SCADA systems security. The publication is crucial for enhancing network architecture and ensuring effective incident response within critical infrastructure sectors (Stouffer *et al.*, 2023).

The NIST Special Publication 800-53 Rev 5: Security and Privacy Controls for Information Systems and Organizations provides a comprehensive catalog of security and privacy controls for federal information systems and organizations. While primarily intended for federal agencies, these controls can be adapted by private sector organizations, including those operating critical infrastructures, to enhance their cybersecurity posture. The publication aids organizations operating critical infrastructures in adopting stringent security measures such as access control, authentication, encryption, and incident response to protect against potential cyber threats (NIST, 2020).

The NIST Special Publication 800-171 Rev 3: Protecting Controlled Unclassified Information (CUI) in Nonfederal Systems and Organizations outlines requirements for protecting controlled unclassified information (CUI) in nonfederal systems and organizations. While initially designed for contractors and subcontractors working with the federal government, these requirements can also be relevant to organizations operating critical infrastructures that handle sensitive information. The publication includes security requirements related to access control, data protection, and incident response that apply to SCADA systems security (Ross & Pillitteri, 2024). By adhering to these NIST regulations and publications, organizations in the United States can enhance the security and resilience of their SCADA systems and critical infrastructures against cyber threats. These frameworks provide valuable guidance and best practices for implementing effective cybersecurity measures tailored to industrial control systems' unique needs and challenges.

The NIST SP 800-82 Rev. 2 "Guide to Industrial Control Systems (ICS) Security" provides recommendations for securing Industrial Control Systems, including SCADA systems, distributed control systems (DCS), and other control system configurations such as programmable logic controllers (PLC). It discusses typical system topologies, identifies potential targets, suggests security countermeasures, and provides leading practices (NIST, 2023). The NIST SP 800-82 Rev. 2 is an invaluable resource for cybersecurity professionals tasked with protecting ICS environments from evolving threats, ensuring that these systems

remain robust against intrusion and operational disruptions.

The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0 represents a significant update designed to enhance cybersecurity measures across various sectors, including SCADA systems and critical infrastructures. The framework serves as a comprehensive guideline for organizations aiming to improve their cybersecurity practices and resilience against cyber threats. It emphasizes the importance of understanding cybersecurity risks, implementing appropriate safeguards, and continually assessing and adapting security measures to mitigate potential vulnerabilities (NIST, 2024a). The CSF 2.0 extends its applicability to SCADA systems by providing tailored recommendations that address the unique security needs of these systems, which are integral to national critical infrastructures (NIST, 2024a). As industries increasingly rely on automated and interconnected technologies, while CSF 2.0 offers strategic guidance to help secure these essential systems against evolving cyber threats. By integrating the framework's updated practices, organizations can enhance their security posture and contribute to the broader goal of national security and resilience (NIST, 2024a).

NIST guidelines are generally voluntary and do not carry direct legal penalties for non-compliance. These guidelines are widely regarded as best practices and are often used as benchmarks for setting industry standards in cybersecurity. However, while there may not be direct penalties for not following NIST guidelines, there can be indirect consequences such as:

- **Regulatory Compliance** – federal agencies and contractors working with the federal government often need to comply with NIST guidelines under laws such as the Federal Information Security Modernization Act (FISMA). Non-compliance in such cases can lead to penalties under those specific regulatory frameworks (113th Congress, 2014).
- **Legal and Financial Risks** – Organizations that experience data breaches or cybersecurity incidents may face legal action or financial liabilities if they are found not to have adhered to industry best practices, including NIST standards. Compliance with NIST guidelines can be seen as part of due diligence to protect sensitive information and systems.
- **Insurance Claims** – Organizations that file cybersecurity insurance claims may be affected by non-compliance with recognized standards like NIST,

and may lead to higher premiums. Insurers may require adherence to specific standards as part of the policy agreement. "The global market for cybersecurity insurance was $7.60 billion and is expected to grow to $20.43 billion by 2027" (Network Assured *et al.*, 2024). In 2022, only 19% of organizations claimed in a survey to have coverage for cyber events beyond $600,000, and only 55% of organizations claimed to have cybersecurity insurance.

- **Contractual Obligations** – Contracts involving IT services or partnerships may include clauses requiring adherence to specific security standards, including NIST guidelines. Non-compliance could result in contractual penalties or termination of contracts.

While there are no direct penalties from NIST itself for non-compliance, following these standards is crucial to minimizing cybersecurity risks and aligning with broader regulatory and industry expectations.

Executive Orders and Directives

- Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," was issued in 2013, which aimed to enhance the security and resilience of the nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties. Executive Order 13636 also helps secure infrastructure by increasing information sharing and by collaboratively developing and implementing risk-based standards.
- Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," was issued in 2017 and calls for government agencies to adopt the NIST Cybersecurity Framework and requires a review of the nation's cybersecurity policies and practices.
- Executive Order 13920, "Securing the United States Bulk-Power System," sought to secure the United States bulk-power system (BPS) against foreign adversaries' exploitation. It prohibited the acquisition, importation, transfer, or installation of bulk-power system electric equipment that poses an undue risk to national security, including SCADA systems components. The executive order

aimed to safeguard critical infrastructure assets from potential exploitation by foreign adversaries (The White House, 2020).

- Executive Order 14028, "Improving the Nation's Cybersecurity," aimed to enhance the cybersecurity of federal government networks and critical infrastructure. It called for the adoption of the NIST Cybersecurity Framework and other best practices to improve cyber threat detection, incident response, and information sharing. The executive order directed federal agencies to modernize and secure their systems, including SCADA systems, to better protect against cyber threats (The White House, 2021).
- Presidential Policy Directive 21 (PPD-21) aims to strengthen and secure the country's critical infrastructure by directing federal agencies to coordinate their efforts according to specific sector-specific agencies (The White House, 2013b).
- Data Breach Notification Laws currently have no single federal law overseeing data breach notifications across every state; several states have their own law requiring notification of security breaches involving personal information.
- Cyber Incident Reporting was enacted in 2021. An Executive Order on Improving the Nation's Cybersecurity has further emphasized the importance of enhancing software supply chain security and has mandated baseline security standards for developing software sold to the government, including requiring developers to maintain greater visibility into their software and making security data publicly available (The White House, 2024).
- The Cybersecurity Act of 2015 encourages the sharing of cybersecurity threat information among private sector companies and between the private sector and government in a protected manner to enhance the security of critical infrastructure (DHS & DOJ, 2018).

These executive orders and directives collectively strengthen the policy framework for cybersecurity, delineating clear pathways for the implementation of robust security measures across critical infrastructures, including SCADA systems. By adhering to these directives, federal agencies and industry stakeholders are better equipped to secure vital operational technologies from cyber threats, ensuring sustained national security and infrastructure resilience. Compliance with these cybersecurity laws and regulations is essential for organizations operating critical

infrastructures, as they help ensure the resilience, reliability, and security of SCADA systems and other essential services.

U.S. Criminal Codes and Statutes Related to Cybersecurity Violations

Cybersecurity violations specifically affecting SCADA systems and critical infrastructures in the United States have several applicable key statutes and sections of the U.S. Criminal Code. These legal provisions are designed to address unauthorized access, sabotage, and other malicious activities targeting the systems that manage, monitor, and control critical infrastructures such as power grids, water treatment facilities, and transportation networks. Here are some relevant sections and their implications:

- Computer Fraud and Abuse Act (CFAA) - 18 U.S.C. § 1030 is the primary statute that addresses cybercrimes against computers, including those that manage SCADA systems. It criminalizes unauthorized access or exceeding authorized access to computers and networks, and it is often applied to protect critical infrastructures from cyber threats. Penalties under the CFAA vary widely depending on the nature and consequences of the unauthorized actions. For offenses involving unauthorized access that leads to damage or obtaining valuable information, penalties can include significant fines and imprisonment of up to 10 years for a first offense and up to 20 years for subsequent offenses (FindLaw, 2024).
- Patriot Act - 18 U.S.C. § 2332b law includes provisions for combating acts of terrorism against computers and networks that affect interstate or foreign commerce, which would include SCADA systems critical to national security and economic stability. The Patriot Act addresses acts of terrorism and includes severe penalties for offenses impacting national security, including life imprisonment or, if the offense results in death, potential capital punishment. This can apply to cyber-terrorism activities that significantly disrupt SCADA systems (FindLaw, 2024a).
- Critical Infrastructures Protection Act of 2001 - Part of the USA PATRIOT Act enhances protections for systems deemed critical to the nation's infrastructure, offering additional resources and support to safeguard these assets from cyber threats. While this act itself primarily focuses on

enhancing protective measures and does not specify penalties, violations likely fall under broader federal statutes such as the CFAA or specific anti-terrorism laws, carrying severe penalties depending on the impact of the breach.

- National Information Infrastructure Protection Act - 18 U.S.C. § 1030 amended the CFAA to include specific enhancements in penalties for attacks against computers used by the Federal Government or used in interstate or foreign commerce or communication, including those involved in critical infrastructure sectors. As an amendment to the CFAA, this act reinforces the penalties mentioned under the CFAA, emphasizing enhanced penalties for attacks against federal interest computers and those affecting interstate or foreign commerce (FindLaw, 2024).
- Homeland Security Act of 2002 - 6 U.S.C. §§ 101 et seq. established the Department of Homeland Security (DHS) and provisions related to the security of critical infrastructures, including cyber threats against SCADA systems. This act primarily establishes the framework for the Department of Homeland Security and does not specify criminal penalties but mandates the protection of critical infrastructures, implying that violations could lead to serious legal actions under related cybersecurity laws (FindLaw, 2024c).
- Federal Information Security Management Act (FISMA) - 44 U.S.C. § 3541 et seq. requires federal agencies, and by extension contractors and other entities handling federal data or critical infrastructure systems, to protect information systems from cybersecurity risks. FISMA does not specify criminal penalties but sets forth requirements for information security that, if not followed, could lead to administrative actions, loss of federal funding, or other civil penalties.
- Sabotage Act - 18 U.S.C. § 2155 criminalizes the destruction of national defense materials, national defense premises, or national defense utilities, which can include SCADA systems of critical infrastructure. The Sabotage Act imposes severe penalties for the destruction of national defense materials, premises, or utilities. Convictions can lead to fines and imprisonment of up to 20 years, and if the sabotage results in death, the penalties can be more severe, including life imprisonment (FindLaw, 2024c).

These laws are enforced by various federal entities, including the FBI's Cyber Division, DHS's Cybersecurity and Infrastructure Security Agency (CISA), and the Department of Justice. Violations can result in severe penalties, including fines and imprisonment, reflecting the high stakes involved in protecting the nation's critical infrastructures from cyber threats.

The "Compliance and Enforcement" framework examines compliance and enforcement mechanisms related to SCADA security and often explores issues such as regulatory oversight, accountability, and enforcement actions. Researchers assess the extent to which organizations adhere to regulatory requirements, identify barriers to compliance, and evaluate the effectiveness of enforcement measures in deterring cyber threats.

A significant challenge identified is the lack of explicit policies or procedures within many organizations that delineate consequences for non-compliance with cybersecurity mandates. This gap often leads to a lax adherence environment where employees may not fully comply with essential cybersecurity laws, regulations, policies, procedures, and software updates. The absence of stringent enforcement and clear penalties not only diminishes the overall security posture but also amplifies the risk posed by insider threats and disgruntled employees.

The need for more rigorous research is evident, particularly in enhancing the language within Executive Orders, CISA directives, NIST guidelines, and other regulatory frameworks. Such enhancements should aim to close gaps in compliance protocols by clearly defining and implementing consequences for violations. By strengthening these aspects of the compliance and enforcement framework, policymakers can foster a more secure and resilient environment for SCADA systems, ensuring that organizations are not only aware of their security obligations but are also held accountable for fulfilling them. This approach will be crucial in building a more robust defense against the evolving landscape of cyber threats. An example of "Failure to Comply with Cybersecurity" in a policy is:

- Example of Failure to Comply with Cybersecurity Statement: "Failure to comply with Cybersecurity laws, regulations, policies, procedures, and mandated software constitutes a serious breach of security protocols and can result in disciplinary action. Non-compliance may compromise the integrity, confidentiality, and availability of sensitive information, putting personal data and critical operations at risk. Such actions can

lead to immediate corrective measures, including but not limited to fines, suspension of network access, mandatory retraining, or other disciplinary actions as deemed necessary by the Office of Information Technology and federal laws. Adherence to these laws, regulations, policies, and procedures are essential to maintaining a secure and resilient cybersecurity posture."

The "Public-Private Partnerships and Collaboration" literature highlights the importance of public-private partnerships and collaboration in addressing SCADA security challenges. Researchers examine initiatives aimed at fostering information sharing, threat intelligence collaboration, and joint cybersecurity exercises between government agencies, industry stakeholders, and international partners.

The "Emerging Technologies and Trends" provides literature on SCADA security and often explores emerging technologies and trends that have the potential to shape the future of critical infrastructure protection. This includes studies of advanced threat detection techniques, secure software development practices, and the integration of artificial intelligence and machine learning into SCADA security operations.

Overall, the literature on policies and regulation frameworks for mitigating threats to critical infrastructures offers valuable insights into the complexities of SCADA security and the multifaceted challenges facing policymakers, regulatory bodies, industry stakeholders, and cybersecurity professionals. By synthesizing and building upon existing research, this study aims to contribute to the ongoing discourse on enhancing the resilience and security of critical infrastructures against cyber threats.

Financial Issues for United States Businesses

United States businesses face significant financial challenges when implementing and maintaining security frameworks for SCADA systems. These challenges encompass initial investment costs, ongoing maintenance, compliance expenses, and the broader management of cybersecurity risks. The implementation of SCADA systems security requires substantial initial investments in technology and personnel (NIST, 2020). This includes acquiring and deploying security tools and technologies, upgrading legacy systems, and hiring cybersecurity experts to assess vulnerabilities and develop mitigation strategies. Furthermore, adherence to regulatory standards, such as those specified in the NIST guidelines, mandates

ongoing financial commitments for maintenance and system updates. Businesses must allocate resources for regular security assessments, software updates, patch management, and system upgrades to address emerging threats and vulnerabilities (Ross & Pillitteri, 2024; Stouffer *et al.*, 2023).

Due to their limited resources, the financial requirements can be burdensome for small and medium-sized enterprises (SMEs). The compliance costs with regulatory requirements, such as those outlined in the NERC CIP standards, may incur additional costs related to documentation, reporting, audits, and assessments. Businesses must allocate resources for compliance activities, including staff training, external audits, and regulatory filings, to demonstrate adherence to security standards.

The risk management expenses for managing cybersecurity risks associated with SCADA systems require investment in risk assessment tools, threat intelligence services, and incident response capabilities. Businesses may need to budget for cybersecurity insurance premiums, legal fees, and crisis management expenses to mitigate the financial impact of cyber incidents.

Small and medium-sized businesses (SMBs) may face resource constraints, including limited budgets, personnel, and expertise when implementing policies and regulation frameworks for SCADA systems security. These businesses may struggle to allocate sufficient resources to cybersecurity initiatives, leading to gaps in security controls and increased vulnerability to cyber threats. Businesses that rely on third-party vendors and suppliers for SCADA system components and services may incur additional costs associated with assessing and managing supply chain risks. This includes conducting vendor assessments, implementing contractual security requirements, and monitoring vendor compliance with security standards.

Investing in business continuity planning and disaster recovery measures is essential for mitigating the financial impact of cyber incidents on critical infrastructures. Businesses must allocate resources to develop and test response plans, establish redundant systems, and ensure operational resilience to minimize downtime and financial losses. Overall, businesses in the United States must carefully consider the financial implications of implementing policies and regulation frameworks for SCADA systems security and allocate resources accordingly to effectively mitigate threats to critical infrastructures.

Theories for Policies and Regulation Frameworks for SCADA Systems

Integrating diverse theoretical perspectives enhances the formulation of effective policies and regulatory frameworks for SCADA systems. Understanding the theoretical underpinnings of these frameworks is crucial for enhancing cybersecurity measures in critical infrastructures. The following theories apply to SCADA systems:

- Risk Management Theory - Risk management theory posits that effective cybersecurity policies and regulation frameworks should be grounded in a comprehensive understanding of the risks facing SCADA systems and critical infrastructures (Kure *et al.*, 2022). This theory emphasizes the importance of systematically identifying, assessing, and mitigating risks, and incorporating elements such as threat intelligence, vulnerability analysis, and risk prioritization (NIST, 2020). Risk management theory, as outlined in guidelines such as NIST SP 800-53 Rev 5, stresses the importance of establishing robust security controls and continuous monitoring to preempt cyber threats.
- Regulatory Compliance Theory - Regulatory compliance theory suggests that policies and regulation frameworks play a crucial role in shaping the behavior of organizations and individuals responsible for securing SCADA systems. This theory emphasizes the need for clear, enforceable regulations that establish minimum security standards, compliance requirements, and accountability mechanisms to ensure adherence to cybersecurity best practices (Ross & Pillitteri, 2024). This approach is evident in implementing the NIST Cybersecurity Framework, which provides a structured methodology for managing cybersecurity risks across various sectors.
- Institutional Theory - Institutional theory highlights the role of social norms, organizational structures, and institutional pressures in shaping the development and implementation of cybersecurity policies and regulation frameworks. This theory posits that factors such as industry standards, regulatory mandates, and stakeholder expectations influence the adoption of specific security practices and compliance behaviors within organizations. Institutional theory can be seen through integrating cybersecurity into the corporate culture by adopting frameworks such as NIST SP 800-82 that guide operational technology security (Stouffer *et al.*, 2023).

- Systems Theory - Systems theory offers a holistic perspective on the interconnectedness of SCADA systems, critical infrastructures, and the socio-technical environment in which they operate. This theory highlights the need for policies and regulation frameworks that account for the complex interactions between technical, organizational, and human factors in mitigating cyber threats and ensuring the resilience of critical infrastructures (The White House, 2013).
- Cybersecurity Governance Theory - focuses on the structures, processes, and mechanisms by which cybersecurity policies and regulations are developed, implemented, and enforced (CISA, 2024; MITRE *et al.*, 2010). This theory emphasizes the role of governance frameworks, regulatory authorities, and multi-stakeholder collaborations in promoting cybersecurity resilience and fostering trust in critical infrastructure systems. Effective governance involves multiple stakeholders and robust processes to ensure cybersecurity measures are comprehensive, well-coordinated, and sustainable, as highlighted in various guidelines and executive orders (The White House, 2017).

These theories underscore the complexity of developing and implementing effective cybersecurity policies for SCADA systems. They highlight the need for an integrated approach that combines understanding risks, enforcing compliance, leveraging institutional structure, engaging stakeholders, considering systemic interconnections, and establishing robust governance practices to protect critical infrastructures effectively. By drawing on these theories, policymakers, regulatory bodies, industry stakeholders, and cybersecurity professionals can develop informed strategies for designing, implementing, and evaluating policies and regulation frameworks to mitigate threats to SCADA systems and safeguard critical infrastructures against cyberattacks.

Cybersecurity Laws and Regulations in the United States for Policies and Regulation Frameworks

In the United States, the development and enforcement of cybersecurity laws and regulations have been strategically structured to protect critical infrastructures, particularly those utilizing SCADA systems. The Critical Infrastructure Protection (CIP) Standards are at the forefront of these efforts and are enforced by the North

American Electric Reliability Corporation (NERC). These standards are crucial in setting cybersecurity requirements for the electric power industry, focusing on safeguarding essential assets such as SCADA systems against potential cyber threats. They address vital areas like access control, incident response, and security awareness training, ensuring that the electric power industry maintains robust defenses and is prepared to respond effectively to emerging cyber threats (The White House, 2020).

The Cybersecurity and Infrastructure Security Agency (CISA) is integral to the Department of Homeland Security (DHS). It is also instrumental in enhancing the cybersecurity resilience of critical infrastructure sectors, including those that depend on SCADA systems. CISA offers guidance, resources, and support to organizations to help them strengthen their cybersecurity defenses. By providing these tools and resources, CISA helps organizations to better protect themselves against cyber threats, thereby contributing to a stronger overall national cybersecurity posture (CISA, 2024).

Another significant resource in this effort is the Cybersecurity Framework developed by the National Institute of Standards and Technology (NIST). This framework offers voluntary guidelines and best practices for improving cybersecurity risk management across various critical infrastructure sectors. It is particularly valuable for those sectors utilizing SCADA systems because it provides a flexible, risk-based approach to cybersecurity that can be customized to address the specific needs and challenges of SCADA and other industrial control systems (NIST, 2024). These structured frameworks and guidelines collectively represent a robust approach to securing the United States' critical infrastructures against the increasing magnitude of cyber threats, ensuring a comprehensive strategy that integrates both regulatory requirements and voluntary best practices into a resilient national cybersecurity posture, helping to protect against the increasing complexity and frequency of cyber threats.

Discussion

In cybersecurity, particularly in protecting SCADA systems and critical infrastructures, the United States has established a foundational legal framework that, while comprehensive, has shown signs of aging as technology rapidly evolves. Notably, the Computer Fraud and Abuse Act (CFAA), enacted in 1986, was an early legislative response to cybercrime and computer-related offenses but has

struggled to keep pace with the rapid advancements in technology and the growing complexity of cyber threats. Similarly, the Patriot Act of 2001, developed in response to the 9/11 terrorist attacks, along with the Critical Infrastructures Protection Act of 2001, the National Information Infrastructure Protection Act of 1996, and the Homeland Security Act of 2002 collectively outline a broad security framework. However, these laws reflect security concerns from decades past, leaving gaps in addressing present or future cybercrime and cybersecurity threats.

Furthermore, the Federal Information Security Management Act (FISMA) of 2002 and the provisions under the Sabotage Act were originally part of the Espionage Act of 1917, showing the historical context of these legislations, which were drafted in response to specific threats of their times. These acts, while foundational, necessitate updates to address the current cyber threat landscapes effectively, which is characterized by increasingly advanced technological threats to critical infrastructures.

Modern challenges require updating existing laws and creating new regulations that address the complexities of modern cyber threats and cybercrimes targeting SCADA systems. Currently, no specific law prevents the sale of critical infrastructures to foreign countries or individuals. However, the Committee on Foreign Investment in the United States (CFIUS) regulates foreign investments in U.S. companies, especially those involving critical infrastructures. CFIUS reviews, investigates, and has the authority to block transactions that might result in a foreign entity gaining control of U.S. companies if such control could pose a risk to national security (U.S. Department of the Treasury, 2024). This includes critical infrastructure transactions across various sectors, such as telecommunications, utilities, and transportation. In addition, the Foreign Investment Risk Review Modernization Act (FIRRMA) of 2018 addresses national security concerns related to foreign investments in critical technologies, critical infrastructures, and sensitive personal data of U.S. citizens (U.S. Department of the Treasury, 2024). CFIUS and FIRRMA illustrate a contemporary approach to regulating investments that might impact national security related to critical infrastructures. These laws and regulations are not outright bans but mechanisms to review and potentially prohibit foreign acquisitions that pose security risks.

Despite these efforts, a significant gap remains in the overarching cybersecurity mandate across all sectors, emphasizing the lack of uniform compliance requirements.

This gap often leads to inconsistent cybersecurity practices. No comprehensive laws, regulations, or policies mandating uniform cybersecurity compliance across U.S. federal, state, local, and private organizations exist. The lack of explicit policies or procedures often creates an environment of lax adherence, where employees may not fully comply with essential cybersecurity laws, regulations, policies, procedures, or software updates. The lack of stringent enforcement and clear penalties for non-compliance weakens the overall security posture and exacerbates the risks posed by insider threats and disgruntled employees. Urgent action is needed to update laws and enforce compliance to mitigate these risks.

Addressing these issues requires updating existing laws with explicit penalties to enhance deterrence against cybercrime and cybersecurity violations. Additionally, developing clear, enforceable policies that span all levels of government and the private sector is critical for establishing a resilient national cybersecurity framework capable of adapting to current and emerging threats. Finally, expanding research and implementing recommendations for future cybersecurity measures for SCADA systems and critical infrastructures is essential to safeguarding national security and economic stability in the face of ever-evolving cyber threats. By strengthening existing laws, enacting more robust penalties for cybersecurity violations, and fostering greater collaboration across government and private sectors, the U.S. can build a more secure and resilient infrastructure capable of withstanding the threats posed by cybercrime and other cybersecurity risks.

Recommendations for Future Research

Recommendations for Policies and Regulation Frameworks in the United States

Enhance collaboration and information sharing by fostering greater collaboration and information sharing among government agencies, industry stakeholders, and international partners to facilitate the exchange of threat intelligence, best practices, and lessons learned in SCADA security. This collaboration can help improve situational awareness, enhance incident response capabilities, and strengthen the overall resilience of critical infrastructures.

Strengthen regulatory oversight and enforcement by enhancing regulatory oversight and enforcement mechanisms to ensure compliance with cybersecurity standards and regulations, such as the NERC CIP standards. This may include

conducting regular audits, assessments, and inspections to verify adherence to security requirements and imposing penalties for non-compliance to incentivize organizations to prioritize cybersecurity.

Promote the adoption of best practices and standards by encouraging the adoption of industry best practices and cybersecurity standards, such as the NIST Cybersecurity Framework and ISA/IEC 62443 standards, to establish baseline security controls and guidelines for securing SCADA systems. Provide resources, incentives, and technical assistance to support organizations in implementing these practices effectively.

Invest in cybersecurity education and training programs will help build a skilled workforce capable of addressing the unique challenges associated with securing SCADA systems and critical infrastructures. Offer incentives for cybersecurity professional development, certification, and workforce development initiatives to attract and retain cybersecurity talent.

Promote research and development by supporting efforts to advance SCADA security technologies, techniques, and methodologies. Invest in innovation initiatives, public-private partnerships, and collaborative research projects to develop and deploy next-generation cybersecurity solutions tailored to the needs of critical infrastructure sectors.

Enhance resilience and incident response capabilities by strengthening the resilience of critical infrastructures by promoting the adoption of robust incident response plans, business continuity measures, and disaster recovery strategies. Regular exercises, simulations, and drills should be conducted to test response capabilities and improve readiness to mitigate cyber incidents affecting SCADA systems.

Stay abreast of emerging cyber threats, vulnerabilities, and technological trends that may impact the security of SCADA systems and critical infrastructures. Continuously assess and update policies and regulation frameworks to address evolving risks and challenges such as ransomware, supply chain vulnerabilities, and the Internet of Things (IoT).

Enhance the language within Executive Orders, CISA directives, NIST guidelines, and other regulator frameworks to close the gaps in compliance protocols by clearly defining and implementing consequences for violations.

Create laws and regulations to prevent critical infrastructures from being sold and acquired by foreign countries and foreign people. Critical infrastructures are

not for sale in the United States. United States companies and government entities must monitor, regulate, and preserve critical infrastructures appropriately.

Future research on Lean Six Sigma within cybersecurity policies and regulation frameworks in the United States should emphasize a multi-faceted approach. Conducting comprehensive studies to identify the areas where Lean Six Sigma methodologies can be most effectively integrated into cybersecurity practices is crucial. This entails a detailed analysis of existing security protocols and identifying inefficiencies and areas susceptible to improvement through streamlining processes. Such research would benefit from adopting case study methodologies to provide practical insights and real-world applicability (Farahbod *et al.*, 2022; Fitzsimmons, 2023; 6sigmastudy, 2024). Moreover, there is a need to develop policy recommendations that explicitly incorporate Lean Six Sigma principles. Researchers should explore the potential for these methodologies to enhance regulatory compliance and operational efficiency in cybersecurity. This could involve the creation of guidelines or frameworks that outline how Lean Six Sigma tools can be used to measure and improve compliance with established cybersecurity standards, such as those set forth by the National Institute of Standards and Technology (NIST) (Farahbod *et al.*, 2022; Fitzsimmons, 2023; 6sigmastudy, 2024). Additionally, future research should focus on the training and development of cybersecurity personnel using Lean Six Sigma methodologies. Investigating the outcomes of such training on cybersecurity readiness and incident response times could provide valuable data to support the implementation of these practices at a broader scale. Empirical research examining the correlation between Lean Six Sigma training and improved security outcomes in various sectors could substantiate the efficacy of this approach (NIST, 2024). Lastly, there is a substantial opportunity for cross-disciplinary research leveraging insights from process improvement and cybersecurity. Such studies could examine the synergistic effects of integrating Lean Six Sigma methodologies with cutting-edge cybersecurity technologies, potentially leading to threat detection and response mechanism innovations. Collaborative research projects involving both cybersecurity and process improvement experts could yield robust frameworks and tools that align with both operational efficiency and security objectives (NIST, 2024; Farahbod *et al.*, 2022; Fitzsimmons, 2023; 6sigmastudy, 2024). Integrating Lean Six Sigma into cybersecurity policies and regulation frameworks holds promise for enhancing security measures' effectiveness

and efficiency. Future research should aim to systematically explore and document the specific benefits, challenges, and best practices associated with this integration to guide policymakers and practitioners in the evolving landscape of cybersecurity.

By implementing these recommendations, the United States can strengthen its policies and regulation frameworks for mitigating threats to SCADA systems and critical infrastructures, thereby enhancing national security, economic resilience, and public safety.

Future Recommendations for Enhancing Cybersecurity in SCADA Systems and Critical Infrastructures

The rapid advancement of emerging technologies presents unique challenges and opportunities for the United States cybersecurity policies and regulatory frameworks such as artificial intelligence (AI), machine learning (ML), and the Internet of Things (IoT) on SCADA systems security. Research should explore how these technologies can be leveraged to enhance critical infrastructures' threat detection, anomaly detection, and incident response capabilities. The National Institute of Standards and Technology (NIST) continually updates guidelines such as NIST SP 800-53 Rev 5 and the Cybersecurity Framework (CSF) 2.0 to incorporate considerations for new technological developments, emphasizing the importance of security and privacy controls in the evolving digital landscape (NIST, 2020; NIST, 2024). Further research is essential to evaluate the impact of these emerging technologies on critical infrastructure, particularly in areas governed by executive orders aimed at strengthening the nation's cybersecurity posture (The White House, 2013; 2017; 2021). Studies should also explore the intersection of technology and policy, assessing how advanced threat detection technologies can be integrated within national cybersecurity strategies, as evidenced by recent guidance from NIST and efforts by the Cybersecurity and Infrastructure Security Agency (CISA) to improve public safety security measures (CISA, 2024).

The intersection of technological advancements and security within supply chain management has become increasingly critical in the United States, as highlighted by recent frameworks and directives (NIST, 2020; The White House, 2021). As SCADA systems become more integral to critical infrastructures, understanding the implications of supply chain vulnerabilities on their security and overall resilience is crucial. Research should focus on assessing risks within

the supply chain, developing strategies to mitigate attacks, and improving visibility and resilience through enhanced vendor management practices. The interconnected nature of supply chains underscores the importance of securing these networks against potential cyber threats. This is particularly pressing as the U.S. continues to advance its regulatory framework to bolster supply chain security. Ongoing research is vital to ensure these frameworks remain adaptive and effective in the face of evolving threats. By systematically analyzing the impact of emerging technologies and integrating perspectives from various sectors and international partners, policymakers can craft measures that address current security needs and anticipate future challenges. This proactive approach will be instrumental in safeguarding the nation's critical infrastructure and ensuring its resilience against cyber threats (113th Congress, 2014; Congressional Research Service, 2023; CISA, 2024a). Furthermore, collaborative efforts among government agencies and private sector organizations are necessary to develop robust frameworks that promote information sharing, threat intelligence, and incident response capabilities. Implementing best practices, such as those outlined in the NIST Cybersecurity Framework and Lean Six Sigma methodologies, can enhance the effectiveness of these initiatives (Farahbod *et al.*, 2022; NIST, 2020). As the U.S. strengthens its regulatory approach to supply chain security, addressing vulnerabilities and enhancing resilience in SCADA systems is critical in maintaining the security of essential services (DOE, 2022; FERC, 2023; U.S. Department of Treasury, 2024). This comprehensive strategy must encompass regulatory requirements and best practices to form a resilient national cybersecurity posture that can effectively protect critical infrastructures against the growing sophistication of cyber threats (NIST, 2024b).

Regulatory compliance and enforcement in cybersecurity are pivotal areas that require ongoing research to ensure United States policies and regulation frameworks remain effective and adaptive to emerging threats. The NIST SP 800-53 Rev 5 and various executive orders on cybersecurity from the White House have laid a robust foundation for security and privacy controls across information systems and organizations (NIST, 2020; The White House, 2021). These documents provide a comprehensive set of guidelines as the baseline for future regulatory developments. Future research should focus on evaluating the effectiveness of these regulations in practical application by having studies to examine how organizations implement these standards and the challenges they face, which will provide a feedback loop

to refine and enhance regulatory frameworks. In addition, with the rapid evolution of technology and the corresponding security threats, there is a crucial need to continuously update and adapt these frameworks. Research could also explore innovative enforcement mechanisms that are flexible and scalable to the pace of technological change and the sophistication of cyber threats. Research should assess the impact of regulatory frameworks such as the NERC CIP standards on organizational behavior, security posture, and incident response capabilities. As the digital landscape evolves, the regulatory frameworks that govern SCADA systems must also evolve.

Fostering strong public-private partnerships (PPPs) to bolster cybersecurity within the United States is paramount, particularly in national security and safeguarding critical infrastructures. Notably, foundational documents such as NIST 800-53 Rev 5 and Executive Order 14028 highlight the essential role of collaboration between the public and private sectors in tackling the multifaceted cybersecurity challenges that surpass the capacity of individual organizations (NIST, 2020; The White House, 2021). Future research should, therefore, explore the mechanisms through which these partnerships can be optimized to enhance cybersecurity resilience and response capabilities. By examining the effectiveness of existing collaborative efforts and identifying areas for improvement, scholars can provide actionable recommendations that guide policy enhancements and foster more robust defensive strategies against cyber threats. This approach will be crucial in developing comprehensive frameworks that address current cybersecurity needs and anticipate and mitigate future vulnerabilities. Future research should emphasize developing models that quantify the effectiveness of PPPs in cybersecurity, specifically how these collaborations can be structured to optimize resource sharing and threat intelligence between government entities and private corporations. Studies could examine the dynamics of information sharing and the barriers that currently hinder effective collaboration by referencing directives like NIST SP 800-171 and the Cybersecurity Framework (CSF) 2.0, which advocate for enhanced and streamlined cybersecurity practices across all sectors (Ross & Pillitteri, 2024; NIST, 2024). In addition, investigative research could explore innovative governance models that leverage the strengths of both sectors to improve cyber incident response times and mitigation strategies. This could include the evaluation of joint task forces and their roles in quick response to cybersecurity incidents, as highlighted in recent

governmental strategies and NIST publications aimed at fortifying the security of operational technology systems (Stouffer *et al.*, 2023; The White House, 2020). As cybersecurity threats continue to evolve with increasing complexity, the strategic importance of reinforcing public-private partnerships becomes paramount to align toward a resilient cybersecurity posture for the nation. This approach will be essential for adapting to and mitigating future cybersecurity challenges.

The critical importance of addressing human factors and insider threats in cybersecurity cannot be overstated, particularly within the framework of United States policies and regulations. The updated guidelines provided by the NIST SP 800-53 Rev 5 emphasize the need for robust security and privacy controls that specifically address these human elements, suggesting a focus on comprehensive user education and behavioral monitoring (NIST, 2020). Future research should explore the development of advanced predictive models that integrate psychological and behavioral data to anticipate and mitigate insider threats effectively. This approach could be further enriched by insights from the NIST Cybersecurity Framework (CSF) 2.0, which provides a structured approach to managing cybersecurity risks associated with human factors (NIST, 2024). In addition, there is a compelling need for empirical research that evaluates the impact of training programs designed to increase cybersecurity awareness among employees at all levels. This research could assess the correlation between training and a decrease in incidents related to human error, drawing on frameworks such as those outlined in NIST SP 800-171 Rev 3, which stresses the protection of controlled unclassified information in nonfederal systems (Ross & Pillitteri, 2024). As the cybersecurity landscape continues to evolve, integrating human factors into the policy-making process remains a critical area of focus. Future research should strive to create a body of evidence that supports the development of policies that address the technical aspects of cybersecurity and the human elements that significantly contribute to the overall security posture of organizations within the United States.

The evolving landscape of global cybersecurity necessitates a focused approach towards international cooperation and standards harmonization, particularly for the United States, which can leverage frameworks such as the NIST Cybersecurity Framework (CSF) 2.0 and NIST SP 800-52 Rev 5. These frameworks provide comprehensive guidelines on security and privacy controls that could serve as a baseline for international cybersecurity standards (NIST, 2020; 2024).

Recommendations for future research should include a systematic analysis of how international cybersecurity policies can be aligned with these standards, ensuring that U.S. policies are not only compliant with international norms but also promote a unified security posture globally. In addition, it is crucial to examine the role of diplomatic engagement in facilitating these partnerships, potentially through the creation of bilateral or multilateral agreements that standardize cybersecurity practices across borders. This approach will ensure that the United States and its partners are equipped to handle the increasingly sophisticated cyber threats that are no longer confined by geographic boundaries. Integrating U.S. cybersecurity standards with international regulations enhances global security infrastructure and positions the U.S. as a leader in shaping global cybersecurity norms. By fostering international cooperation and harmonizing standards, the U.S. can effectively protect its interests while promoting a stable, secure, and resilient cyberspace.

The importance of resilience and continuity planning in cybersecurity cannot be overstated, particularly in safeguarding United States policies and regulatory frameworks. Future research should build upon the National Institute of Standards and Technology (NIST), such as NIST SP 800-53 Rev 5 and NIST SP 800-82 Rev 3, to create comprehensive continuity plans that address the dynamic nature of cyber threats. Research could explore the integration of resilience planning into the cybersecurity strategies outlined by the White House through various executive orders, emphasizing the importance of improving the nation's cybersecurity infrastructure (The White House, 2013; 2021). It is recommended that studies examine the effectiveness of current resilience measures in real-world scenarios, drawing from recent cybersecurity incidents. Strengthening the resilience and continuity planning within U.S. cybersecurity policies requires a concerted effort to apply and test the guidelines by NIST and other regulations. By focusing on the practical application and continuous improvement of these frameworks, future research can contribute significantly to the security and stability of national cyberinfrastructure.

Lastly, integrating Lean Six Sigma methodologies into cybersecurity policies and frameworks in the United States offers a promising avenue for enhancing the effectiveness and efficiency of security measures. According to the National Institute of Standards and Technology (NIST), continuous improvement processes such as those outlined in NIST SP 800-53 Rev 5 and the Cybersecurity Framework (CSF)

2.0 are critical for maintaining robust security and privacy controls in information systems (NIST, 2020; NIST, 2024). It is necessary to align these frameworks with Lean Six Sigma principles to streamline process improvements and reduce redundancies in cybersecurity practices.

Lean Six Sigma can assist in assessing and mitigating vulnerabilities, especially in operational technology (OT) security, as detailed in NIST SP 800-82 Rev. 3 (Stouffer *et al.*, 2023). Organizations can identify critical inefficiencies by applying Lean tools and techniques and enhance their response strategies to cybersecurity incidents. The recent Executive Orders, including EO 14028, emphasize the importance of adopting comprehensive frameworks incorporating risk management and resilience (The White House, 2021). This approach suggests a strategic alignment with Lean Six Sigma's focus on minimizing waste and optimizing process capability.

Moreover, future research should explore the impact of Lean Six Sigma on the cybersecurity maturity model while analyzing how iterative process improvements could align with evolving threats and technologies. Researchers can examine case studies of organizations that have successfully integrated these methodologies to develop best practices that could inform policy adjustment and framework enhancements. This research would provide valuable insights into the practical challenges and benefits of such integrations, supporting the ongoing evolution of national cybersecurity policies.

The application of Lean Six Sigma in cybersecurity policy and regulation offers a structured approach to enhancing the resilience and effectiveness of security measures. By focusing on continuous improvement and efficiency, U.S. regulatory bodies can better equip themselves against the increasing sophistication of cyber threats, fostering a more secure and resilient digital infrastructure.

Addressing the multifaceted challenges of cybersecurity within United States laws, regulations, and policy frameworks necessitates a multi-pronged research approach that transcends traditional methods. Integrating emerging technologies such as AI, ML, and IoT into the security measures of SCADA systems, as recommended by the NIST and mandated by various executive orders, offers significant potential to advance the nation's cybersecurity capabilities (NIST, 2020; The White House, 2021). However, further research is imperative to optimize the efficacy of these technologies in real-world applications, ensuring that cybersecurity frameworks not only keep pace with technological advancements but also effectively

mitigate emerging threats. In addition, the crucial role of public-private partnerships in this endeavor cannot be overstated. These collaborations are essential for pooling resources, sharing critical threat intelligence, and co-developing strategic solutions that enhance the collective cybersecurity posture of both sectors. Future studies should focus on identifying the barriers to effective partnerships and proposing innovative solutions to enhance cooperation between government and industry. By consolidating efforts across government, private sector, and academia, the United States can fortify its defenses against an increasingly complex cyber threat landscape, ensuring the security and resilience of its critical infrastructure. Lastly, by addressing these research gaps, future studies can contribute to developing more effective policies and regulation frameworks for mitigating threats to SCADA systems and critical infrastructures in the United States, thereby enhancing national security, economic resilience, and public safety.

References

113th Congress. (2014, December 18). *Public Law 113–283 Federal Information Security Modernization Act (FISMA) of 2014* [PDF]. Govinfo.gov. Retrieved August 24, 2024, from https://www.govinfo.gov/content/pkg/PLAW-113publ283/pdf/PLAW-113publ283.pdf

6sigmastudy. (2024, February 16). *Lean Six Sigma methodology in cyber security operations*. Retrieved September 2, 2024, from https://www.6sigmastudy.com/article?title=Lean-Six-Sigma-Methodology-in-Cyber-Security-Operations

Congressional Research Service. (2020, September 21). *Cybercrime and the Law: Computer Fraud and Abuse Act (CFAA) and the 116th Congress*. CRS Reports. Retrieved August 23, 2024, from https://crsreports.congress.gov/product/pdf/R/R46536

Congressional Research Service. (2023, March 13). *Banking, Data Privacy, and Cybersecurity Regulation*. Retrieved August 25, 2024, from https://crsreports.congress.gov/product/pdf/R/R47434

Cybersecurity & Infrastructure Security Agency. (2024a). *Cybersecurity governance*. Cybersecurity and Infrastructure Security Agency CISA. Retrieved September 2, 2024, from https://www.cisa.gov/topics/cybersecurity-best-practices/cybersecurity-governance

Cybersecurity & Infrastructure Security Agency. (2024b). *Industrial control systems*. CISA America's Cyber Defense Agency. Retrieved August 24, 2024, from https://www.cisa.gov/topics/industrial-control-systems

Department of Energy. (2002, September 9). *21 steps to improve cyber security of SCADA networks* [PDF]. Retrieved August 24, 2024, from https://www.oe.netl.doe.gov/docs/prepare/21stepsbooklet.pdf

Department of Homeland Security & Department of Justice. (2018, June 15). *Privacy and Civil Liberties Final Guidelines: Cybersecurity Information Sharing Act of 2015*. CISA.gov. Retrieved September 2, 2024, from https://www.cisa.gov/sites/default/files/publications/Privacy%2520and%2520Civil%2520Liberties%2520Guidelines%2520under%2520the%2520Cybersecurity%2520Information%2520Sharing%2520Act%2520of%25202015.pdf#:~:text=On%20December%2018%2C%202015%2C%20the%20President%20signed%20CISA,sources% 20and%20methods%2C%20and% 20privacy%20and% 20civil%20liberties.

Environmental Protection Agency. (2020, December 23). *Epa cybersecurity for the water sector*. US EPA. Retrieved August 24, 2024, from https://www.epa.gov/waterresilience/epa-cybersecurity-water-sector

Farahbod, K., Shayo, C., & Varzandeh, J. (2022). Six Sigma and Lean Operations in Cybersecurity Management. *Journal of Business and Behavioral Science*, *34*(1), 99–109. Retrieved September 2, 2024, from https://www-proquest-com.captechu.idm.oclc.org/scholarly-journals/six-sigma-lean-operations-cybersecurity/docview/2667274873/se-2

Federal Energy Regulatory Commission. (2023, December 12). *Cyber and grid security*. Retrieved August 25, 2024, from https://www.ferc.gov/industries-data/electric/industry-activities/cyber-and-grid-security

FindLaw. (2024a, January 1). *18 U.S.C. § 2332b - U.S. Code - Unannotated Title 18. Crimes and Criminal Procedure § 2332b. Acts of terrorism transcending national boundaries*. Retrieved August 30, 2024, from https://codes.findlaw.com/us/title-18-crimes-and-criminal-procedure/18-usc-sect-2332b/

FindLaw. (2024b, January 1). *18 U.S.C. § 1030 - U.S. Code - Unannotated Title 18. Crimes and Criminal Procedure § 1030. Fraud and related activity in connection with computers*. FindLaw.com. Retrieved August 30, 2024, from https://codes.findlaw.com/us/title-18-crimes-and-criminal-procedure/18-usc-sect-1030/

FindLaw. (2024c, January 1). *18 U.S.C. § 2155 - U.S. Code - Unannotated Title 18. Crimes and Criminal Procedure § 2155. Destruction of national-defense materials, national-defense premises, or national-defense utilities*. Retrieved August 30, 2024, from 18 U.S.C. § 2155

FindLaw. (2024d, January 1). *6 U.S.C. § 101 - U.S. Code - Unannotated Title 6. Domestic Security § 101. Definitions*. Retrieved August 30, 2024, from https://codes.findlaw.com/us/title-6-domestic-security/6-usc-sect-101/

Fitzsimmons, M. (2023, May 25). *Strengthening cybersecurity with lean six sigma: eliminating human behaviors that jeopardize systems*. 360 Degrees Mngt. Retrieved September 2, 2024, from https://www.360degreesconsultants.org/post/strengthening-cybersecurity-with-leansixsigma-eliminating-human-behaviors-that-jeopardize-systems

Kure, H., Islam, S., & Mouratidis, H. (2022). An integrated cyber security risk management framework and risk predication for the critical infrastructure protection. *Neural Computing and Applications*, *34*(18), 15241–15271. Retrieved September 2, 2024, from https://doi.org/10.1007/s00521-022-06959-2

MITRE, Bodeau, D., Boyle, S., Fabius-Greene, J., & Graubart, R. (2010, September). *Cyber Security Governance* [PDF]. mitre.org. Retrieved September 2, 2024, from https://www.mitre.org/sites/default/files/pdf/10_3710.pdf

National Institute of Standards and Technology. (2020). NIST SP 800-53 Rev 5: Security and Privacy Controls for Information Systems and Organizations. Retrieved May 3, 2024, from https://doi.org/10.6028/NIST.SP.800-53r5

National Institute of Standards and Technology. (2024b, February 14). *NIST SP 800-66 Rev 2: Cybersecurity resources for hipaa-regulated entities* [PDF]. Cybersecurity Resources. Retrieved August 24, 2024, from https://csrc.nist.gov/files/pubs/sp/800/66/r2/final/docs/sp800-66r2-cybersecurity-resources.pdf

National Institute of Standards and Technology. (2024a). The NIST Cybersecurity Framework (CSF) 2.0. Retrieved July 6, 2024, from https://doi.org/10.6028/NIST.CSWP.29

National Institute of Standards and Technology. (2024c, February 26). *The NIST cybersecurity framework (csf) 2.0* [PDF]. Retrieved August 27, 2024, from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

National Institute of Standards & Technology, Nelson, A., Rekhi, S., Souppaya, M., & Scarfone, K. (2024, April). *NIST SP 800-61r3 incident response recommendations and considerations for cybersecurity risk management: A csf 2.0 community profile* [PDF]. National Institute of Standards. Retrieved September 2, 2024, from https://doi.org/10.6028/NIST.SP.800-61r3.ipd

Network Assured & Cole, N. (2024, August 7). *23 eye-opening cybersecurity insurance statistics*. Network Assured. Retrieved September 2, 2024, from https://networkassured.com/security/cybersecurity-insurance-statistics/

North American Electric Reliability Corporation. (2024). *NERC Reliability Standards*. Retrieved August 27, 2024, from https://www.nerc.com/pa/Stand/Pages/default.aspx

Olafuyi, B. A. (2023). Cyber threats to national security: An in-depth analysis of the United States landscape. *International Journal of Scientific and Research Publications*, *13*(12), 134–139. Retrieved July 24, 2024, from https://doi.org/10.29322/ijsrp.13.12.2023.p14415

Ross, R., & Pillitteri, V. (2024). NIST SP 800-171 Rev 3: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. Retrieved May 3, 2024, from https://doi.org/10.6028/NIST.SP.800-171r3

Stouffer, K., Pease, M., Tang, C., Zimmerman, T., Pillitteri, V., Lightman, S., Hahn, A., Saravia, S., Sherule, A., & Thompson, M. (2023). NIST SP 800-82 Rev. 3: Guide to Operational Technology (OT) Security. *National Institute of Standards and Technology*. Retrieved October 28, 2023, from https://doi.org/10.6028/NIST.SP.800-82r3

The White House. (2013a, February 12). *Executive Order 13636 - Improving Critical Infrastructure Cybersecurity*. Retrieved May 5, 2024, from https://obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity/eo-13636

The White House. (2013b, February 12). *Presidential policy directive/ppd-21: Critical infrastructure security and resilience* [PDF]. Retrieved February 23, 2024, from https://www.cisa.gov/sites/default/files/2023-01/ppd-21-critical-infrastructure-and-resilience-508_0.pdf

The White House. (2017, May 11). *Executive Order 13800 - Strengthening the cybersecurity of federal networks and critical infrastructure – the white house*. Retrieved May 5, 2024, from https://trumpwhitehouse.archives.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/

The White House. (2020, May 1). *Executive Order 13920 - Securing the United States bulk-power system – the white house*. Retrieved May 7, 2024, from https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-securing-united-states-bulk-power-system/

The White House. (2021, May 12). *Executive Order 14028 - Improving the nation's cybersecurity*. Retrieved May 7, 2024, from https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

U.S. Department of the Treasury. (2024). *The committee on foreign investment in the United States (cfius)*. Retrieved September 2, 2024, from https://home.treasury.gov/policy-

issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius

U.S. Department of Justice. (2015, February 19). *9-48.000 - computer fraud and abuse act*. U.S. Department of Justice: Justice Manual Title 9: Criminal. Retrieved August 24, 2024, from https://www.justice.gov/jm/jm-9-48000-computer-fraud.