ESP-JETA
ESP Journal of Engineering & Technology Advancements
ISSN: 2583-2646 / Volume 1 Issue 1, September, 2021 / Page No: 273-281
Paper Id: JETA-V1I1P129 / Doi: 10.56472/25832646/JETA-V1I1P129

Original Article

A Comparative Study between NERC-CIP and NIST Compliance- Defining the Critical Framework for Building Cyberrisk Free Infrastructure

Suchismita Chatterjee
M.S. University of North, Texas / Cyber Security Specialist, USA.

Received Date: 04 July 2021 Revised Date: 03 August 2021 Accepted Date: 03 September 2021

Abstract: *This paper compares the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC-CIP) and the National Institute of Standards and Technology (NIST) cybersecurity frameworks, analysing their strengths, weaknesses, and implementation challenges. While NERC-CIP focuses on mandatory requirements for the bulk electric system, NIST provides a voluntary and adaptable framework for broader cybersecurity risk management. The study highlights the complementary nature of both frameworks and proposes a comprehensive approach to building cyber risk-free infrastructure, incorporating elements like risk-based prioritization, defense-in-depth strategies, continuous monitoring, and collaboration. It also emphasizes the limitations of relying solely on compliance and suggests additional measures such as advanced threat detection, zero-trust models, and security awareness training to enhance cybersecurity posture in critical infrastructure sectors.*

Keywords: *NERC-CIP, NIST, Cybersecurity Frameworks, Critical Infrastructure Protection, Cyber Risk Management, Compliance, Risk Assessment, Threat Detection, Security Controls, Best Practices, Case Studies, IT/OT Security, Supply Chain Risk, Resilience.*

I. INTRODUCTION

Critical infrastructure sectors, such as energy, water, transportation, healthcare, and financial services, face significant cybersecurity risks due to increasing digitalization and reliance on interconnected systems [10]. Advanced Persistent Threats (APTs) from nation-state actors pose ongoing challenges, often targeting critical systems for disruption or data theft [7]. The rise of ransomware attacks further compounds these risks, with cybercriminals encrypting systems and demanding payments, leading to potential service outages [6]. Supply chain vulnerabilities, where third-party vendors and software providers are exploited, also increase the attack surface [9]. Many organizations rely on outdated legacy systems, which are particularly susceptible to exploitation due to poor patch management and lack of modern security features [8]. Insider threats, whether intentional or accidental, can compromise sensitive systems, while the proliferation of IoT devices and integration of IT with operational technology (OT) create new vulnerabilities [12]. Compounding these challenges, inadequate preparedness and weak incident response capabilities can significantly amplify the impact of cyberattacks, threatening the continuity of essential services [14].

Compliance frameworks play a critical role in mitigating cybersecurity risks in critical infrastructure by providing structured guidelines to secure systems and processes [13]. These frameworks establish a baseline for security by defining minimum standards and controls that organizations must implement to address vulnerabilities [17]. They enhance risk management by facilitating regular assessments and enabling the deployment of effective threat mitigation measures [3]. By emphasizing the development of incident response plans, compliance frameworks improve organizational preparedness, minimizing the operational and financial impact of cyberattacks [10]. Additionally, they promote accountability by assigning roles and responsibilities, ensuring proper governance across cybersecurity programs [4]. Standardized guidelines within these frameworks encourage collaboration between industries, governments, and global partners, strengthening collective security efforts [14]. Adherence to frameworks ensures regulatory compliance, protecting organizations from penalties and building trust with stakeholders [6]. Furthermore, the evolving nature of these frameworks allows organizations to adapt to emerging threats, fostering resilience in an increasingly complex threat landscape [18]. By integrating these practices, critical infrastructure organizations can safeguard essential services while reducing cyber risk exposure [16].

Two prominent frameworks for enhancing cybersecurity in critical infrastructure are the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC-CIP) standards and the National Institute of Standards and Technology (NIST) cybersecurity framework. This report provides a comparative study of NERC-CIP and NIST compliance, highlighting their strengths and weaknesses, and proposes a comprehensive framework for building cyber risk-free infrastructure [6][9].

II. OVERVIEW OF NERC-CIP AND NIST COMPLIANCE FRAMEWORKS

A. NERC-CIP

The NERC-CIP (North American Electric Reliability Corporation Critical Infrastructure Protection) standards are mandatory cybersecurity requirements for entities that own or manage facilities within the North American Bulk Electric System (BES) [9]. These standards aim to ensure the security and reliability of the BES by establishing a baseline set of cybersecurity measures [11]. The goal is to ensure that appropriate security controls are in place to protect the BES and its users and customers from all threats that may affect its timely and effective functioning [6]. The NERC-CIP framework focuses on identifying and securing critical assets that could impact the electricity supply in the United States, Canada, and parts of Mexico [7].

The NERC-CIP standards were introduced in response to the growing need for cybersecurity in the electric grid and critical energy infrastructure [10]. Initially developed in the early 2000s, these standards gained prominence after the 2003 Northeast blackout, which highlighted vulnerabilities in grid reliability [6]. Over time, the standards have evolved through multiple versions to address emerging cyber threats and incorporate lessons learned from real-world incidents [12]. The Federal Energy Regulatory Commission (FERC) enforces NERC-CIP compliance in the United States, ensuring consistent adherence across the energy sector [8].

The primary purpose of NERC-CIP is to secure the reliability of the Bulk Electric System (BES) by safeguarding its critical cyber assets [9]. These standards focus on preventing unauthorized access, ensuring data integrity, and maintaining the operational continuity of electric grid systems [11]. NERC-CIP applies to entities involved in the generation, transmission, and distribution of electricity, specifically those that affect the BES [6]. The NERC-CIP standards are categorized into various areas, including cybersecurity, physical security, and incident response [10].

NERC-CIP standards primarily affect the energy sector, particularly organizations responsible for operating the Bulk Electric System [7]. This includes electric utilities, power generation companies, transmission operators, and related entities across North America [8].

B. NIST Compliance

The NIST Cybersecurity Framework (CSF) was first released in 2014 and updated in 2018, aiming to help organizations improve their cybersecurity posture [14]. Developed by NIST in collaboration with industry stakeholders, the framework offers a flexible, risk-based approach to managing and mitigating cyber risks [15]. It is widely regarded as a best practice for organizations seeking to enhance their cybersecurity capabilities [17].

The purpose of the NIST CSF is to provide a voluntary framework for improving cybersecurity risk management [13]. Applicable across various industries and organizations of all sizes, it helps entities identify, protect, detect, respond to, and recover from cybersecurity incidents [14]. While originally designed for critical infrastructure sectors, the NIST CSF has been widely adopted across industries such as healthcare, finance, manufacturing, government, and telecommunications [15]. Its adaptability and scalability make it suitable for organizations ranging from small businesses to large enterprises.

NIST has been pivotal in establishing robust standards for cybersecurity. Among its most influential contributions are the NIST Cybersecurity Framework (CSF), NIST Special Publication (SP) 800-53, and NIST SP 800-171 [14]. These frameworks provide comprehensive guidance for organizations to enhance their cybersecurity posture and address the evolving threat landscape [16].

The NIST CSF is organized around five core functions, each representing an essential aspect of effective cybersecurity risk management [13]:

- Identify: Develop an organizational understanding to manage cybersecurity risks to systems, assets, data, and capabilities. This includes identifying critical assets and vulnerabilities to ensure a clear risk profile [14].
- Protect: Implement appropriate safeguards to ensure the delivery of critical infrastructure services. This involves deploying security measures, such as access controls and data protection mechanisms, to mitigate identified risks [14].
- Detect: Establish activities to identify the occurrence of cybersecurity events. This includes continuous monitoring and threat detection to recognize anomalous or malicious activity promptly [17].
- Respond: Implement response actions to contain the impact of detected cybersecurity events. This encompasses incident response planning, mitigation strategies, and communication protocols to manage threats effectively [14].
- Recover: Develop plans to maintain resilience and restore any capabilities or services impaired by cybersecurity incidents. Recovery efforts focus on business continuity and the swift restoration of operations [15].

By following NIST's frameworks, entities across various sectors can strengthen their defenses and build resilience against emerging cyber threats [16]. The NIST CSF provides a structured approach for organizations to manage cybersecurity risks systematically, aligning their strategies with industry best practices [13].

III. COMPARISON OF NERC-CIP AND NIST FRAMEWORKS

While both NERC-CIP and NIST frameworks aim to enhance cybersecurity, they differ in their scope, approach, and implementation.

A. Approach and Philosophy:

NERC-CIP is more prescriptive and compliance-oriented, designed specifically for the energy sector to ensure consistent security practices and regulatory compliance. Its approach is static, which can hinder quick adaptation to new challenges outside the energy sector. In contrast, NIST's risk-based approach is more dynamic and flexible, allowing organizations to customize their cybersecurity efforts to meet their specific risk profiles. This flexibility enables NIST to be applied across diverse industries and helps organizations stay agile in the face of evolving cyber threats.[16]

Table 2: Comparison Based on Approach and Philosophy

Aspect	NERC-CIP	NIST
Philosophy	Compliance-driven, with a primary focus on regulatory adherence to ensure the reliability of the energy grid.	Risk-based, providing organizations with the flexibility to assess and manage cybersecurity risks according to their own environment and threat landscape.
Regulatory Focus	Focuses on strict compliance with predefined standards, ensuring uniform security measures across the energy sector.	Focuses on risk management, helping organizations to prioritize actions and controls based on their own risk assessments.
Flexibility	Limited flexibility due to its prescriptive nature; tailored for the energy sector with specific requirements.	Highly flexible, offering a framework that can be applied across various industries and scaled based on organizational needs.
Implementation Approach	Top-down regulatory approach that mandates adherence to specific security controls.	Bottom-up approach that encourages organizations to assess risks and implement security measures that align with their business objectives.
Focus on Adaptability	Rigid, which may limit adaptation to evolving cybersecurity threats and emerging technologies.	Adaptive, enabling organizations to continuously refine and update their cybersecurity strategies in response to changing threats and technological advances.

B. Key Components and Controls

NERC-CIP's key components and controls are heavily focused on ensuring critical infrastructure protection within the energy sector, with detailed requirements for access control, incident response, and asset management. These controls are highly prescriptive and designed to ensure compliance within the sector.

NIST, on the other hand, provides a broader, more flexible framework with key components that focus on risk management, data protection, and incident response. Its guidelines are designed to be scalable and adaptable across industries, making NIST a more versatile framework compared to the energy-specific NERC-CIP.[2]

Table 2: Comparison of NERC and NIST based on Key components

Aspect	NERC-CIP	NIST Compliance
Asset Identification	CIP-002: Identification and categorization of critical cyber assets that impact the Bulk Electric System (BES).	Identify Function: Asset management, business environment, governance, and risk assessment.
Access Control	CIP-003: Security management controls for authorized access.	NIST SP 800-53 AC (Access Control): Controls for restricting access to systems and data.

Personnel Security	CIP-004: Training and personnel requirements for managing access to critical cyber assets.	NIST SP 800-53 PS (Personnel Security): Guidelines for screening and authorizing personnel.
Perimeter Security	CIP-005: Electronic security perimeters to control network connections and communications.	Protect Function: Guidelines for securing physical and logical boundaries, including identity and access management.
System Security Management	CIP-007: Patch management, antivirus management, and system hardening requirements.	NIST SP 800-53 SI (System and Information Integrity): Standards for patching vulnerabilities and protecting systems from malware.
Physical Security	CIP-006: Physical security requirements for critical cyber assets.	NIST SP 800-53 PE (Physical and Environmental Protection): Guidelines for securing physical facilities and infrastructure.
Incident Response	CIP-008: Incident reporting, response planning, and coordination requirements.	Respond Function (SP 800-61): Incident handling, mitigation, and communication guidelines.
Recovery and Continuity	CIP-009: Recovery plans and exercises to ensure operational continuity.	Recover Function: Standards for recovery planning and improvements post-incident.
Change and Configuration Management	CIP-010: Configuration change management and regular vulnerability assessments.	NIST SP 800-128 (Configuration Management): Guidelines for monitoring, updating, and managing configurations.
Data Protection	CIP-011: Ensures confidentiality and integrity of sensitive information.	NIST SP 800-53 SC (System and Communications Protection): Data encryption, transmission security, and confidentiality guidelines.
Scope and Applicability	Focused on the energy sector and entities involved in the generation, transmission, and distribution of electricity impacting the BES.	Broadly applicable across industries, including healthcare, finance, manufacturing, and government.
Risk Assessment	Implicit in the categorization of critical assets and associated controls.	NIST SP 800-30: Comprehensive risk assessment methodology to identify and mitigate risks.

C. Implementation challenges

While both NERC-CIP and NIST present implementation challenges, the nature of these challenges differs based on the framework's approach. NERC-CIP is more prescriptive and compliance-driven, creating challenges for smaller utilities with limited resources, complex legacy systems, and the need for rigorous compliance with detailed requirements. On the other hand, NIST's flexibility is beneficial for organizations with diverse needs but introduces challenges related to organizational maturity, resource allocation, and the integration of multiple cybersecurity frameworks.[7][2]

Both frameworks require substantial investments in terms of time, resources, and personnel, but NIST's adaptability allows for more flexibility in implementation, whereas NERC-CIP demands strict compliance, particularly for critical energy infrastructure.

Table 3: Comparison of NERC and NIST on the basis Challenges

Challenge	NERC-CIP	NIST
Cost and Resource Requirements	The high cost of implementing NERC-CIP's prescriptive standards can be challenging, particularly for smaller utilities, with a significant financial burden required for both technology and workforce.	NIST also requires substantial investments for cybersecurity infrastructure and training. However, its flexibility may allow organizations

		to prioritize investments based on their risk tolerance and budget constraints.
Complexity and Rigidity	NERC-CIP's prescriptive and rigid requirements can create difficulties for organizations, especially those with diverse or evolving infrastructures. Compliance can be a complex process that requires detailed documentation and constant validation.	NIST offers flexibility but can be difficult to implement for organizations with low maturity in risk management practices. Smaller organizations may struggle to create comprehensive and effective risk management strategies.
Integration with Existing Systems	NERC-CIP's strict requirements for technology integration with legacy operational systems can cause disruptions, particularly if the systems are not designed with cybersecurity in mind.	NIST's flexibility can make integration with existing systems easier, but interoperability with other cybersecurity frameworks or technologies may still present challenges due to differing standards and controls.
Incident Response and Reporting	NERC-CIP requires detailed incident reporting and strict response timelines for BES operators. Many organizations face difficulties in developing an effective and timely response capability due to lack of resources or expertise.	NIST provides a more adaptive approach to incident response, but organizations may still struggle with the resources required to manage a dynamic incident response framework, particularly for smaller or less mature organizations.
Supply Chain Risk Management	NERC-CIP's supply chain risk management requirements are challenging due to the complexity of managing third-party vendors, particularly in the energy sector where dependencies on contractors and suppliers are high.	NIST's third-party risk management is less prescriptive but still requires organizations to assess and manage vendor-related risks. It may be more difficult to implement across diverse industries with varying supply chain structures.

IV. MAPPING BETWEEN NERC CIP AND NIST CSF

The mapping between the NERC-CIP standards and the NIST Cybersecurity Framework (CSF) plays a crucial role in helping organizations align their cybersecurity and compliance efforts. By aligning both frameworks, organizations can enhance their cyber risk management strategies and improve their overall compliance maturity [6]. The mapping process provides a clear view of how NIST's cybersecurity principles can support achieving NERC CIP compliance requirements, offering valuable insights into how organizations can improve their cybersecurity posture across critical infrastructure sectors [13].

The relationship between NIST CSF Subcategories and NERC CIP standards provides a detailed understanding of the similarities, overlaps, and gaps between the two frameworks. This mapping process helps organizations ensure that their compliance programs cover the necessary cybersecurity areas while maintaining flexibility in implementation [6][14].

The mapping relationships for each informative reference in the NIST CSF to NERC CIP include:

Table 4: Mapping Relationship

Mapping Relationship	**Description**
Subset of	The language used in the NIST CSF element is a subset of the language used in the NERC CIP element. This indicates that NIST CSF can help address some specific CIP requirements.

Intersects with	The NIST CSF Subcategory and the NERC CIP Reliability Standard share some concepts in common. While they may not be identical, their goals align in promoting better cybersecurity practices.
Superset of	The NIST CSF element is a broader or more comprehensive version of the corresponding NERC CIP element. This shows that NIST CSF offers a more detailed or inclusive approach to addressing cybersecurity.
Equal to	The concepts in both the NIST CSF Subcategory and the NERC CIP Reliability Standard are identical. This indicates that the two frameworks fully align in terms of their language and requirements.
Not related to	There is no overlap or connection between the NIST CSF element and the NERC CIP element. These elements address completely different aspects of cybersecurity and risk management.

This detailed mapping helps organizations evaluate where NIST CSF can support the implementation of NERC CIP standards and identify areas for improvement or enhancement. It also allows organizations to streamline their compliance processes, reducing duplication of efforts and aligning their cybersecurity objectives more effectively.

V. CHALLENGES AND BEST PRACTICES IN IMPLEMENTING NERC-CIP AND NIST FRAMEWORKS

Implementing NERC-CIP and NIST frameworks can be challenging due to various factors, including the complexity of the standards and the evolving threat landscape. Resource constraints, including personnel, budget, and technology, are a common challenge for both frameworks and can hinder effective implementation [6][13].

One of the key challenges in implementing NERC-CIP is balancing security with operational efficiency. Organizations must find a way to implement stringent security protocols without compromising the performance of their operations. The rapidly evolving threat landscape also presents a challenge, as it necessitates continuous updates and adaptations to security measures to stay ahead of potential threats. Additionally, maintaining comprehensive documentation of compliance efforts can be burdensome for organizations, requiring significant time and resources [7].

A. Best Practices for NERC-CIP Compliance Include

- Conducting regular risk assessments: Identifying and prioritizing risks to inform security measures, ensuring that resources are focused on the most critical areas [12].
- Cultivating a culture of security: Promoting cybersecurity awareness and responsibility among employees to ensure that security is embedded into the organizational culture [6].
- Providing regular training: Ensuring that personnel are continuously trained on cybersecurity policies, procedures, and best practices, helping to mitigate human error [13].
- Automating where possible: Leveraging automation for tasks such as monitoring, reporting, and compliance management to improve efficiency and reduce the risk of oversight [7].
- Conducting incident response drills: Regularly testing incident response plans to ensure that personnel are prepared to respond effectively to security events and minimize damage during a real incident [12].

In addition to resource constraints, challenges in implementing the NIST framework include the complexity of the framework, which requires a deep understanding of cybersecurity principles, as well as potential resistance to change from staff when introducing new processes and procedures. The framework's comprehensive nature demands significant effort to fully implement, and organizational buy-in is critical for successful adoption [6][14].

B. Best Practices for NIST Implementation Include:

- Prioritizing high-impact areas: Focus on areas that have the most significant effect on the security posture, ensuring that resources are directed toward the most critical risks [13].
- Leveraging existing resources: Utilize existing tools, processes, and expertise within the organization to streamline implementation and avoid duplication of efforts [6].
- Fostering a cybersecurity culture: Promote cybersecurity awareness across the organization and encourage employees

to take ownership of security practices, creating a security-conscious workforce [7].

- Engaging stakeholders: Involve stakeholders from various departments to ensure a coordinated approach and to align the cybersecurity strategy with broader organizational goals [14].

By following these best practices, organizations can navigate the complexities of NIST framework implementation and enhance their overall cybersecurity resilience.

Table 5: Challenges and Best Practices Summary

Aspect	NERC-CIP	NIST
Key Challenges	- Balancing security with operational efficiency	- Complexity of the framework requiring deep understanding of cybersecurity principles
	- Evolving threat landscape requiring continuous updates and adaptations	- Potential resistance to change from staff when implementing new processes and procedures
	- Maintaining comprehensive documentation of compliance efforts	- Resource constraints (personnel, budget, and technology)
Best Practices	- Conducting regular risk assessments to identify and prioritize risks	- Prioritizing high-impact areas that significantly affect security posture
	- Cultivating a culture of security by promoting awareness and responsibility among employees	- Leveraging existing resources (tools, processes, and expertise)
	- Providing regular training to ensure personnel are up-to-date with cybersecurity policies	- Fostering a cybersecurity culture by promoting awareness and encouraging employee ownership of security
	- Automating tasks where possible to improve monitoring, reporting, and compliance management	- Engaging stakeholders across the organization for a coordinated approach
	- Conducting incident response drills to test preparedness and response plans	

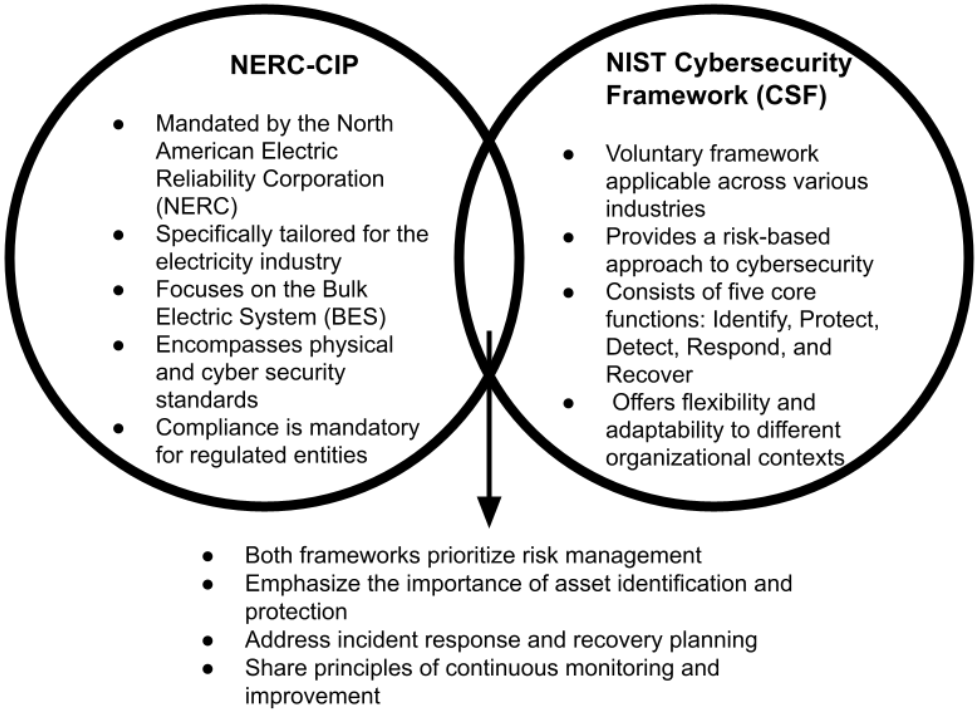

Figure 1: Differences and Similarity of NERC and NIST

Also, the NIST website provides a collection of success stories from organizations that have implemented the NIST Cybersecurity Framework. These case studies span various sectors, including international organizations, state and local

governments, academia, and the private sector. For example, the University of Kansas Medical Center successfully implemented the NIST framework to enhance its cybersecurity posture and better protect sensitive patient data. By adopting the NIST framework, the institution strengthened its security measures and ensured compliance with relevant regulations, safeguarding critical healthcare information.

In the case of Sacramento Municipal Utility District (SMUD), the organization successfully transitioned to NERC CIP Version 5 to enhance its cybersecurity protocols, while another utility company has partnered with NST for over a decade to achieve and maintain NERC CIP compliance. This long-term collaboration involved various aspects of the compliance program, including vulnerability assessments, staff augmentation, and ongoing support to ensure continuous alignment with NERC standards.

V. A Comprehensive Framework for Building Cyber Risk-Free Infrastructure

A comprehensive framework for building cyber risk-free infrastructure begins with identifying critical infrastructure, focusing on systems vital to organizational or national operations. Once identified, the next step is to assess regulatory oversight. If the infrastructure falls under the jurisdiction of the North American Electric Reliability Corporation (NERC), organizations must adhere to NERC-CIP standards, which emphasize access control, incident response, and system monitoring. For infrastructure not regulated by NERC, the NIST Cybersecurity Framework (CSF) is recommended. This framework provides a flexible, risk-based approach encompassing five core functions: identify, protect, detect, respond, and recover. Regardless of the chosen standard, implementing tailored security controls is essential. These measures should include technical solutions like firewalls, administrative policies, and physical safeguards. Continuous monitoring and improvement complete the framework, ensuring systems are audited, threats are addressed, and controls are updated in response to evolving risks. The decision-making process, as depicted in the diagram, guides organizations to adopt the appropriate standards, ensuring robust security controls and fostering resilience against cyber threats.

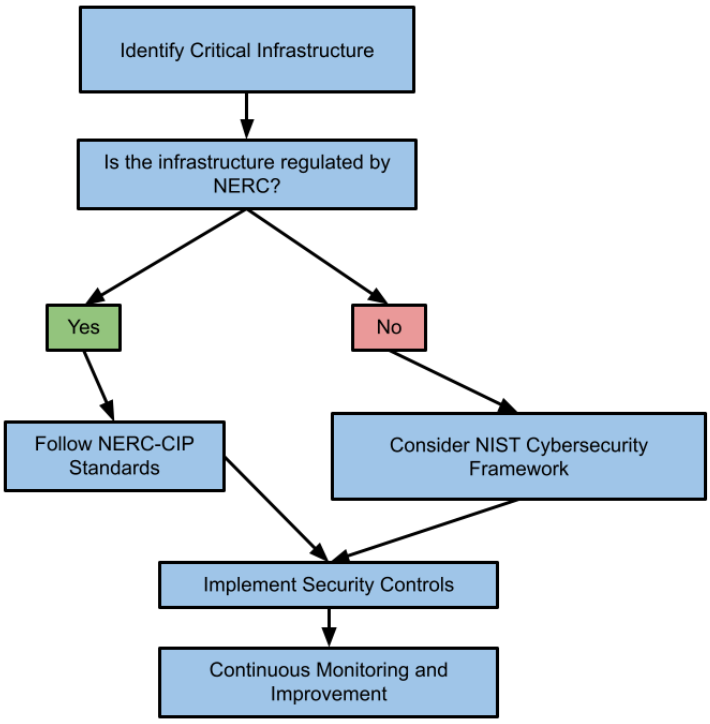

Figure 2: Framework for Building Cyber Risk-Free Infrastructure

While compliance with NERC-CIP and NIST frameworks is essential, it is crucial to recognize that compliance alone does not guarantee complete cybersecurity. These frameworks provide a foundation for cybersecurity but may not address all emerging threats or specific organizational needs. One limitation of both frameworks is that a focus on compliance may lead to a "check-the-box" mentality rather than fostering a proactive approach to risk management.

Limitations specific to NERC-CIP include its narrow scope, as it primarily addresses the bulk electric system and may not adequately cover cybersecurity risks in other critical infrastructure sectors. Additionally, integrating NERC-CIP

requirements with legacy systems can be complex and costly. On the other hand, limitations of the NIST Cybersecurity Framework include its voluntary nature, which may not provide sufficient incentives for effective implementation. The lack of specific requirements can be a weakness for organizations with limited cybersecurity expertise, and measuring the framework's effectiveness in reducing cybersecurity risk can be challenging.

VI. CONCLUSION

Protecting critical infrastructure from cyber threats requires a comprehensive and multi-layered approach. NERC-CIP and NIST frameworks provide valuable guidance and a foundation for cybersecurity risk management in critical infrastructure sectors. NERC-CIP offers a prescriptive and mandatory set of standards specifically designed for the bulk electric system, while NIST provides a more flexible and adaptable framework applicable to organizations across all sectors. By understanding the strengths and weaknesses of each framework, organizations can develop a tailored approach to cybersecurity that meets their specific needs and risk profiles. However, it is crucial to recognize that compliance with these frameworks alone does not guarantee complete cybersecurity. Organizations should go beyond compliance and implement additional measures and strategies to address the evolving threat landscape and their specific needs. This includes employing advanced threat detection and response technologies, adopting a zero trust security model, conducting regular security awareness training, implementing robust vulnerability management programs, developing and testing incident response plans, and considering cybersecurity insurance. By adopting a proactive and holistic approach to cybersecurity, critical infrastructure sectors can enhance their resilience and ensure the continuous delivery of essential services. This requires a commitment to continuous monitoring and improvement, collaboration and information sharing among stakeholders, and a culture of cybersecurity awareness and responsibility throughout the organization. By integrating these elements into their cybersecurity strategy, critical infrastructure organizations can effectively mitigate cyber risks and safeguard their vital systems.

VII. REFERENCES

[1] Proctor, Matt, and Terry Smith. "Lessons learned from NERC CIP applied to the industrial world." 2017 70th Annual Conference for Protective Relay Engineers (CPRE). IEEE, 2017.

[2] Dolezilek, David, and Laura Hussey. "Requirements or recommendations? Sorting out NERC CIP, NIST, and DOE cybersecurity." 2011 64th Annual Conference for Protective Relay Engineers. IEEE, 2011.

[3] Christensen, Dane, et al. "Risk assessment at the edge: Applying NERC CIP to aggregated grid-edge resources." The Electricity Journal 32.2 (2019): 50-57.

[4] Zafirovic-Vukotic, Mira, et al. "Secure Scada network supporting NERC CIP." 2009 IEEE Power & Energy Society General Meeting. IEEE, 2009.

[5] Mertz, Mike. "NERC CIP compliance: We've identified our critical assets, now what?"." 2008 IEEE Power and Energy Society General Meeting-Conversion and Delivery of Electrical Energy in the 21st Century. IEEE, 2008.

[6] Marron, Jeffrey, Avi Gopstein, and Daniel Bogle. "Benefits of an Updated Mapping between the NIST Cybersecurity Framework and the NERC Critical Infrastructure Protection Standards." National Institute of Standards and Technology: Gaithersburg, MD, USA (2021): 9.

[7] Weiss, Joseph M., and CISM PE. "Control systems cyber security—the need for appropriate regulations to assure the cyber security of the electric grid." US Congress Testimony. 2007.

[8] Abrams, Marshall. "Applying NIST SP 800-53 to Industrial Control Systems."

[9] Zhang, Zhen. "NERC's Cyber Security Standards: Fulfilling Its Reliability Day Job and Moonlighting as a Cyber Security Model." Environmental Practice, Journal of the National Association of Environmental Professionals, DePaul University (2011).

[10] Hilt, David W. "Critical infrastructure protection required on electric grid continually changing." Natural Gas & Electricity 34.8 (2018): 9-15.

[11] Zhang, Zhen. "ENVIRONMENTAL REVIEW & CASE STUDY: NERC's cybersecurity standards for the electric grid: Fulfilling its reliability day job and moonlighting as a cybersecurity model." Environmental Practice 13.3 (2011): 250-264.

[12] Pollet, Jonathan. "The past, present, and future of securing electric power systems." 2009 42nd Hawaii International Conference on System Sciences. IEEE, 2009.

[13] Krumay, Barbara, Edward WN Bernroider, and Roman Walser. "Evaluation of cybersecurity management controls and metrics of critical infrastructures: A literature review considering the NIST cybersecurity framework." Secure IT Systems: 23rd Nordic Conference, NordSec 2018, Oslo, Norway, November 28-30, 2018, Proceedings 23. Springer International Publishing, 2018.

[14] Cybersecurity, Critical Infrastructure. "Framework for improving critical infrastructure cybersecurity." URL: https://nvlpubs. nist. gov/nistpubs/CSWP/NIST. CSWP 4162018 (2018): 7.

[15] Plan, NIST Public Access. "National Institute of Standards and Technology (NIST)."

[16] Cauffman, Stephen A., Maria K. Dillard, and Jennifer Helgeson. Implementation of the NIST community resilience planning guide for buildings and infrastructure systems. US Department of Commerce, National Institute of Standards and Technology, 2018.

[17] Scofield, Meg. "Benefiting from the NIST cybersecurity framework." Information Management 50.2 (2016): 25.

[18] Hiller, Janine S., and Roberta S. Russell. "Privacy in crises: The NIST privacy framework." Journal of Contingencies and Crisis Management 25.1 (2017): 31-38. [17] Pan, Ya, et al. "A systematic literature review of android malware detection using static analysis." IEEE Access 8 (2020): 116363-116379.