International Journal of Latest Research in Engineering and Technology (IJLRET)
ISSN: 2454-5031
www.ijlret.com || Volume 11 - Issue 07 || July 2025 || PP. 47-52

NIST Regulatory Requirements in Ensuring National Cybersecurity

Elshad Neymatov
MBA and MS in IT Management student, Webster University
IT Specialist, Advent Health Company
Denver, Colorado, USA

Abstract: The study focuses on conducting an analysis of the regulatory mandates of the National Institute of Standards and Technology of the United States (NIST) as an element in constructing a comprehensive national cybersecurity system. The objective of the article is to systematize and evaluate the effectiveness of implementing the NIST Cybersecurity Framework (CSF) for the protection of strategically significant sectors: healthcare, energy, and transport complex.

The methodological basis consisted of a retrospective system-synthetic analysis of current scientific publications for 2021–2025, relevant regulatory acts, and statistical reports reflecting practices of NIST standards implementation.

As a result of the study, the main advantages and bottlenecks in adapting NIST CSF in various sectors were identified, and recommendations for further improvement of the framework model were formulated.

In particular, with regard to the protection of electronic medical records (EHR), it is proposed to implement a multi-level approach combining AES-256 encryption, role-based access control (RBAC), and continuous monitoring for strict compliance with HIPAA requirements.

The scientific novelty lies in reconceiving NIST CSF not as a static set of prescriptions, but as a dynamic, adaptive system capable of integrating sectoral specificity and timely responding to new technological challenges.

The practical significance of the obtained conclusions is determined by their value for cybersecurity specialists, representatives of regulatory authorities, and leaders of critical infrastructure organizations responsible for developing strategic measures for the protection of information assets.

Keywords: cybersecurity, NIST, cybersecurity framework, critical infrastructure, national security, data protection, healthcare, energy, transport, risk management

Introduction

In the context of the continuous process of digital transformation and the rapid complication of cyber threats, the issues of protecting national critical infrastructure acquire key importance for maintaining state resilience and economic well-being. Vulnerabilities in such strategic sectors as healthcare, energy and transportation are capable of provoking destructive consequences, undermining social stability and threatening national security. According to the IBM report, the average cost of a data breach in 2024 was 4.9 million US dollars [1]. This statistic clearly indicates the need to implement comprehensive and reliable cybersecurity measures.

The relevance of the study is dictated by the necessity of forming a comprehensive framework model to ensure the security of critically important services. The subject of the research encompasses the mechanisms for protecting sensitive infrastructure from cyber-attacks capable of disrupting the functioning of vital public systems, while guaranteeing their availability, integrity and reliability.

The scientific gap lies in the insufficient systematization of practical experience in adapting the universal NIST standards to industry-specific requirements against the backdrop of the rapidly evolving threat landscape.

The aim of the article is to systematize and evaluate the effectiveness of the implementation of the NIST Cybersecurity Framework (CSF) for the protection of strategically significant sectors: healthcare, energy and the transportation complex.

The scientific novelty consists in substantiating an approach in which the NIST cybersecurity framework (CSF) should be regarded not as a rigid set of prescriptions, but as a flexible and adaptive tool for constructing multi-layered protection of critical infrastructure.

The author's hypothesis is based on the assumption that the effective implementation of the NIST CSF requires not only compliance with technical criteria, but also deep integration with corporate risk management processes and the security culture of each organization, which ultimately transforms regulatory requirements into an effective mechanism for enhancing systems' resilience to cyber-attacks.

Materials and Methods

Studies devoted to ensuring national cybersecurity in the context of NIST requirements demonstrate a diversity of methodological approaches and practical models. In the literature, four main thematic clusters can be identified: the development and adaptation of maturity frameworks and conceptual models, the evaluation of the effectiveness of regulatory frameworks and policies in specific industries, the systematization of risk management methods and cyber-threat taxonomies, and the economic assessment of incident consequences and protection costs.

The first cluster includes works dedicated to the creation of generalized and applied security maturity models. Almomani I., Ahmed M., Maglaras L. [2] propose a framework model (maturity assessment framework) for Saudi Arabian higher education institutions, based on the NIST CSF and ISO 27001 standards, with detailed elaboration of the domains of identity management, data protection and incident response. Reyes-Acosta R. E. et al. [3] describe a conceptual model for edge computing and Internet of Things environments, emphasizing the specificity of distributed architectures and the need to adapt NIST SP 800-53 controls for IoT devices. Toussaint M., Krima S., Panetto H. [7] conduct a review of Industry 4.0 frameworks, examining approaches to integrating NIST CSF, ISA/IEC 62443 and European recommendations ENISA to ensure the security of digital manufacturing systems.

The second cluster comprises studies assessing the effectiveness of existing regulatory requirements and policies in specific sectors. Sani M. [4] analyzes the resilience of personal data protection measures in healthcare, comparing the HIPAA, GDPR and NIST 800-66 requirements and noting the lack of unification of backup and encryption approaches at the level of medical institutions. Alghassab M. [5] investigates the impact of cybersecurity on monitoring and control systems for energy networks, highlighting compatibility issues between SCADA protocols and NIST recommendations and the vulnerability of obsolete equipment.

The third thematic block is represented by systematic reviews and taxonomies. Sánchez-García I. D., Mejía J., San Feliu Gilabert T. [6] carry out a mapping of research on risk assessment, identifying more than 50 analysis methods (quantitative, qualitative and hybrid) and proposing their own validation of the methodology based on NIST SP 800-30. Rahman M. H., Wuest T., Shafae M. [8] focus on industrial manufacturing: they propose a meta-taxonomy of cyber attacks and countermeasures, classifying incidents by vector of intrusion (network, physical, software) and the corresponding NIST 800-82 recommendations for each category.

Finally, economic studies occupy a separate place. The annual IBM Security Cost of a Data Breach Report 2023 provides empirical data on average costs of data breaches, analyzing the relationship between NIST CSF compliance and the magnitude of losses [1].

Despite the wealth of proposed models, the literature reveals a number of contradictions. First, different sectors (education, healthcare, energy, manufacturing) use approaches adapted to their specifics, which complicates the development of a unified set of maturity assessment metrics. Second, there is a gap between the NIST-recommended controls and the capabilities of small and medium-sized enterprises to implement them due to limited resources and staff qualifications. In addition, the economic studies (Cost of a Data Breach Report) provide aggregated data without taking into account sectoral differences and the scale of infrastructural investments. Finally, the issues of interaction between NIST frameworks and international standards (for example, ISO and ENISA), as well as the problems of assessing the effectiveness of implemented measures in real time, including automated monitoring and continuous validation of controls, are insufficiently covered. These gaps indicate promising directions for further research in the unification of maturity metrics, adaptive models for resource-constrained organizations and the integration of NIST approaches with international cybersecurity initiatives.

Results and Discussion

The use of NIST regulatory mandates as the foundation of the national cybersecurity system requires careful concretization of their practical implementation in critical sectors. The Cybersecurity Framework (CSF) with its five core functions — identification, protection, detection, response and recovery — represents not a list of disparate measures but an integrated risk-management methodology spanning the full threat lifecycle. This study focuses on the design and deployment of a comprehensive cyber-defense system to ensure continuity and security of key services in healthcare, energy and transportation, with each sector requiring adaptations dictated by its specific threat profile, regulatory environment and technological architecture.

In healthcare the priority is to preserve confidentiality, integrity and availability of sensitive patient data, where electronic health records (EHR) form the core of the information landscape. Resilience of these systems to unauthorized access and cyberattacks, as well as compliance with HIPAA and related standards, is achieved through a combination of technical and organizational measures structured according to NIST CSF logic. Foremost, end-to-end encryption of data at rest and in transit is applied. The use of robust algorithms (for example AES-256) protects records stored in databases, file systems and backup media, while mandatory

implementation of SSL/TLS secures EHR exchange channels among healthcare providers, patients and partners. A strict role-based access-control model is then implemented, limiting staff privileges in accordance with job responsibilities and thereby reducing the risk of insider breaches [2, 6]. The system is complemented by continuous monitoring and auditing. Persistent logging of read, modify and delete operations on data, together with intrusion-detection and prevention tools, enables prompt identification and neutralization of network-traffic anomalies (port scanning, credential stuffing). Machine-learning-based advanced threat protection technologies detect zero-day attacks targeting the EHR infrastructure, and a pre-established incident-response plan ensures rapid localization and mitigation of consequences (fig.1).

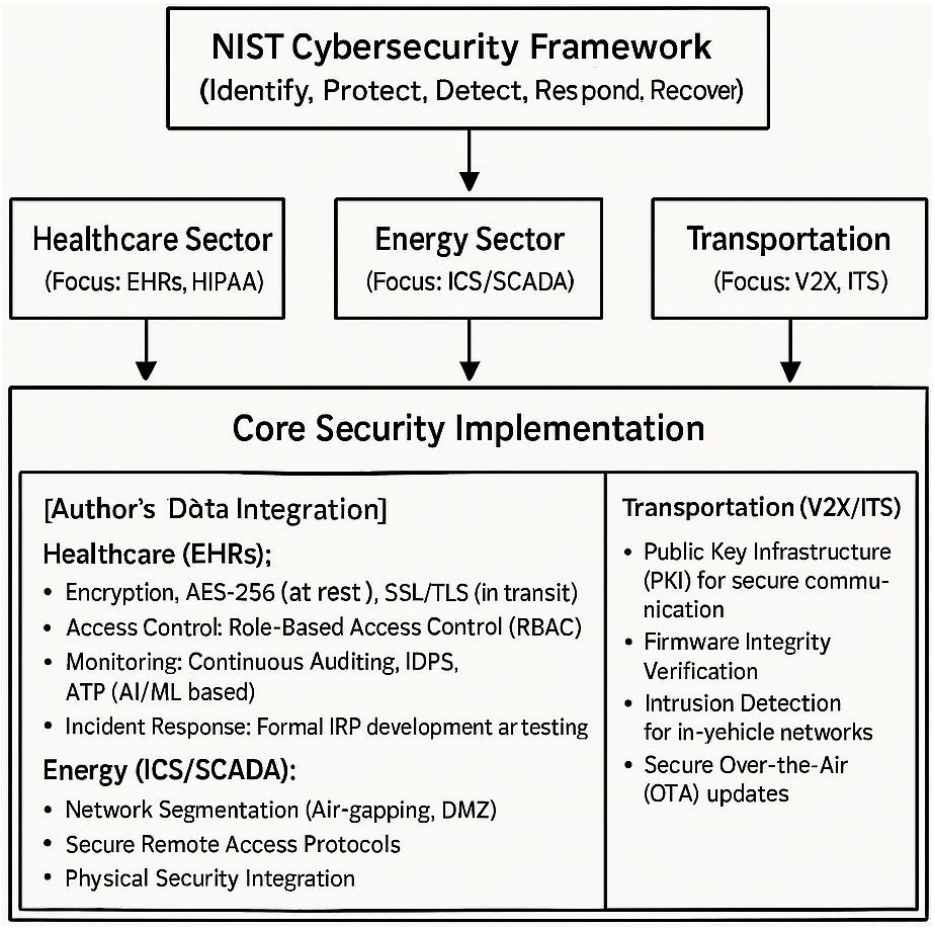

Fig.1: Multi-layered security model for electronic health records (EHR) based on NIST CSF [2, 3, 6]

The energy sector operating ICS and SCADA infrastructure is under threat of attacks capable of causing large-scale blackouts and cascading failures in adjacent sectors. Within the framework of the NIST CSF priority is given to strict isolation of critical network segments and timely anomaly detection. The baseline defense is constituted by deep network segmentation with the establishment of air gaps and demilitarized zones (DMZ), thereby eliminating direct communication between corporate IT environments and industrial control loops. Additionally, monitoring systems based on behavioral analysis are employed to register any deviations of equipment from reference operating modes, thus enabling the detection of cyberattacks at early stages [5] (table 1).

Table 1: Comparative characteristics of implementing NIST CSF in critical sectors [4, 5]

Criterion	**Healthcare**	**Energy**	**Transportation**
Key asset	Electronic health records (EHR), patient data	Industrial control systems (ICS/SCADA)	Vehicle-to-everything (V2X) communication systems, intelligent transportation systems (ITS)
Primary risk	Confidential data leakage, service availability disruption	Physical destruction, large-scale outages	Traffic safety disruption, logistical failures
Priority NIST function	Protect	Detect	Identify
Key technologies	Encryption (AES-256), RBAC, IDPS/ATP, SIEM	Network segmentation, anomaly monitoring, ICS endpoint protection	PKI, software integrity verification, secure OTA updates
Regulatory environment	HIPAA, HITECH	NERC CIP, C2M2	SAE standards, ISO/SAE 21434

Development of vehicle-to-everything (V2X) (fig.2) communication technologies and intelligent transportation systems (ITS) has greatly expanded the attack surface in the transportation sector. Compromise of such systems can disrupt road traffic and directly threaten human lives. Within the framework of the NIST CSF priority is given to preserving the integrity and authenticity of transmitted data. An indispensable security requirement is the deployment of a public key infrastructure (PKI) providing encryption and digital signing of messages exchanged between vehicles and road infrastructure. Additionally secure over-the-air (OTA) software update mechanisms and firmware integrity verification of onboard modules are implemented to block any unauthorized code modifications.

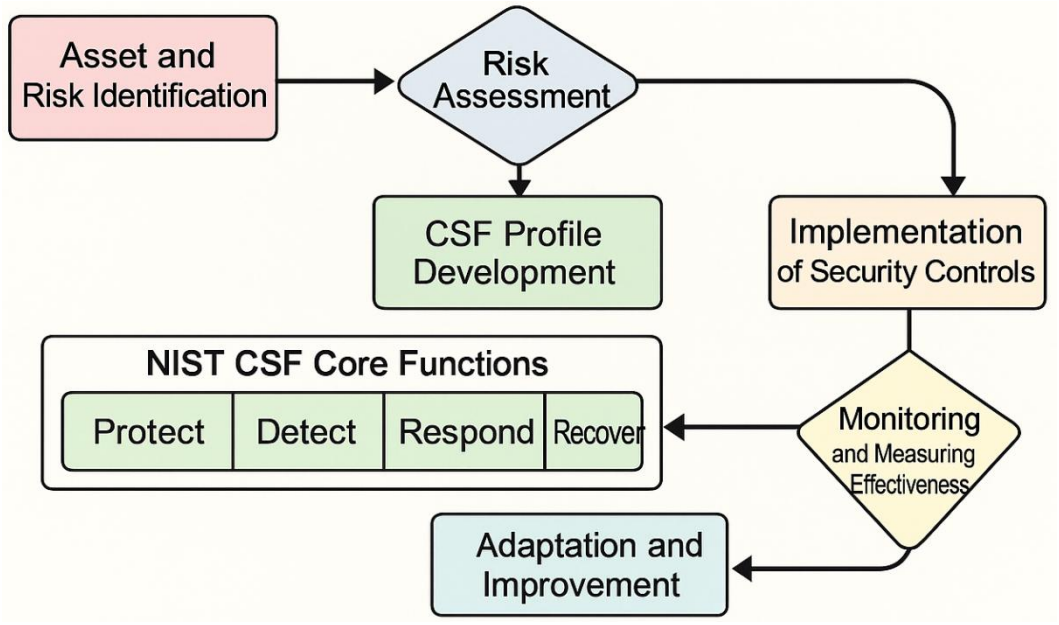

Fig.2: Critical Infrastructure Cyber Risk Management Process Based on NIST CSF [4, 7]

Therefore, although the fundamental principles of the NIST CSF are universal in nature, their effective implementation is impossible without deep industry-specific adaptation. A critically important tool is the development of specialized profiles that map the core functions and categories of the CSF to the unique threats, risks, and regulatory requirements of each sector. This approach takes an organization beyond mere formal compliance, creating a truly layered and agile cyber-defense system capable of evolving alongside the threat landscape.

Recommendations are subsequently provided for its flexible configuration and effective implementation in the critical sectors of the national economy

Special attention is devoted to the development of sector-specific CSF profiles that explicitly map the functions, categories and subcategories of the framework to the actual assets, vulnerabilities and regulatory

requirements of healthcare, energy and transportation. It is recommended to formalize maturity metrics, KPI targets and implementation roadmaps, which will enable a transition from mere compliance to controlled risk management

To enhance cyber resilience it is advisable to integrate the requirements of the NIST CSF into the organizational risk management and information security culture. Such integration involves the participation of senior management, information security and risk management specialists, as well as legal and human resources divisions, thereby ensuring a unified vision of priorities and consistent funding of cyber resilience initiatives

In the healthcare sector it is recommended to strengthen the protection of electronic medical records using a multilayered approach: symmetric AES-256 encryption for data at rest and TLS 1.3 for transmission channels, strict RBAC with periodic access-rights audits, as well as automated SIEM/IDPS systems and machine-learning modules for anomaly and zero-day detection. Regular penetration testing and incident response exercises will ensure verification of process fault tolerance

For energy facilities it is critically important to segment the industrial network at micro- and macro-levels: establishment of DMZs and air gaps, minimization of direct channels between corporate and operational segments, along with a full vulnerability management cycle (patch management) and scheduled replacement of obsolete controllers

In the transportation sector special emphasis is placed on maintaining the integrity and authenticity of messages in V2X and ITS systems through a robust PKI infrastructure for encryption and digital signing, secure OTA update mechanisms with embedded software verification, and continuous monitoring of firmware changes, which enables prompt detection of attempts to manipulate vehicle location and status data

Given the limited resources of small and medium-sized enterprises, it is advisable to develop simplified maturity models that allow for the phased implementation of the most critical controls. It is also important to harmonize NIST approaches with the international ISO/IEC and ENISA standards, and to organize regular validation through automated testing, audits and personnel training programs [3, 8]

In the end, the NIST normative-methodological framework demonstrates significant potential as a universal and flexible instrument for shaping a national cybersecurity system. At the same time, the actual return on its application directly depends on the ability to adapt abstract principles to the specific risk profile and threats of each critical-infrastructure sector. Achieving a sustainable outcome implies not just the implementation of technical control measures, but the construction of an integrated model in which technologies, regulated processes, and personnel competencies function within a single, proactive cyber-risk management strategy.

Conclusion

The conducted research reveals the significance of NIST standards in shaping the modern national cybersecurity architecture. It has been determined that the cybersecurity framework NIST CSF represents not merely a set of recommendations but an integrated methodology enabling critical infrastructure organizations to systematically manage cyber risks. The analysis demonstrated that, despite the universal nature of the five fundamental CSF functions, their practical implementation is impossible without detailed sector-specific adaptation. In healthcare, ensuring the confidentiality of EHR through encryption and strict access control in accordance with HIPAA remains paramount. For the energy sector, segmentation of industrial networks ICS/SCADA and real-time anomaly detection are critical, whereas the transportation sector focuses on preserving the integrity of V2X communications via cryptographic mechanisms. The proposed measures, including the implementation of AES-256 encryption, RBAC and proactive monitoring, illustrate the practical embodiment of this model in healthcare. Thus, NIST regulatory requirements establish a reliable foundation for constructing a multilayered and resilient protection system for national critical infrastructure.

References

[1]. *IBM Security. (2023). Cost of a data breach report 2023.* https://www.ibm.com/reports/data-breach (date of request: 05.05.2025).
[2]. Almomani, I., Ahmed, M., & Maglaras, L. (2021). Cybersecurity maturity assessment framework for higher education institutions in Saudi Arabia. PeerJ Computer Science, 7,1-26. https://doi.org/10.7717/peerj-cs.703
[3]. Reyes-Acosta, R. E., García-Alcaraz, J. L., Martínez-González, A., Acevedo-Chedid, J. A., & Rodríguez-Borbon, M. I. (2025). Cybersecurity conceptual framework applied to edge computing and Internet of Things environments. Electronics, 14(11), 10–35. https://doi.org/10.3390/electronics14112109
[4]. Sani, M. (2024). Assessing the effectiveness of current cybersecurity regulations and policies for resilience in healthcare data protection,1-9.

[5]. Alghassab, M. (2021). Analyzing the impact of cybersecurity on monitoring and control systems in the energy sector. Energies, 15(1), 1–21. https://doi.org/10.3390/en15010218

[6]. Sánchez-García, I. D., Mejía, J., & San Feliu Gilabert, T. (2022). Cybersecurity risk assessment: A systematic mapping review, proposal, and validation. Applied Sciences, 13(1), 1–29. https://doi.org/10.3390/app13010395

[7]. Toussaint, M., Krima, S., & Panetto, H. (2024). Industry 4.0 data security: A cybersecurity frameworks review. Journal of Industrial Information Integration. https://doi.org/10.1016/j.jii.2024.100604

[8]. Rahman, M. H., Wuest, T., & Shafae, M. (2023). Manufacturing cybersecurity threat attributes and countermeasures: Review, meta-taxonomy, and use cases of cyberattack taxonomies. Journal of Manufacturing Systems, 68, 196–208. https://doi.org/10.1016/j.jmsy.2023.03.009