

Analysis of NIST Cybersecurity Framework (CSF)

As the technology continues to advance, more and more organizations rely on it for essential operations and services. From healthcare systems to emergency services, almost every sector leverages technology to some extent. Additionally, the internet itself has significantly impacted our everyday lives by making communication and access to information faster and more efficient than ever. As a result, vast amounts of information are now stored, transferred, and accessed through digital platforms, creating increasingly large databases. This data often includes sensitive information such as personal identification, health records, and even nation's critical and highly sensitive information. And when such information falls into the wrong hands, the consequences can be severe. This raises important questions: Are these systems that handle such data properly secured? And what are the organizations doing to safeguard and protect their systems and network against potential cyber threats? This highlights the need for effective cybersecurity strategies and policies to address the increasing cyber threats across the nation.

Cybersecurity has become an essential component across nearly every field. This growing need led to the development of the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), a widely adopted standard used by organizations to manage and reduce cybersecurity risk. This essay examines the factors that led to the development of the NIST framework, explains how this framework is applied in a specific setting, and further discusses how it fits into broader national cybersecurity policy.

The NIST Cybersecurity Framework (CSF) is a widely accepted security standard used to identify, assess, and manage cyber risk. It is most commonly used in the United States; however, it has inspired other nations to develop and adapt similar frameworks (Cockcroft, 2020). Almost every organization, including both government and private sectors, uses this framework as a

basic standard for managing cyber risks. It was developed and released in February 2013 by the National Institute of Standards and Technology. Several factors led to its development, including an executive order and the need for a flexible, repeatable, and standardized approach to protect the nation's critical infrastructure.

As mentioned above, one of the key factors behind the development of this framework was Executive Order 13636, which was primarily issued by President Obama to protect critical infrastructures such as healthcare systems, power grids, water treatment facilities, and transportation systems. Another crucial factor was the need for a standardized approach that could serve as a common language for cybersecurity risk management across different organizations and sectors. Prior to its development, organizations relied on a wide range of standards, making it very difficult to follow, communicate, and compare cyber risks across organizations. The NIST framework addressed this issue by offering a standardized structure built around six core functions: Govern, Identify, Protect, Detect, Respond, and Recover, which comes under the CSF Core component. Additionally, CSF Organizational Profiles and CSF Tiers are the other two main components of the NIST framework. Furthermore, this framework is repeatable, flexible, and technically neutral, enabling organizations of all sizes and industries to adopt and implement it effectively.

For the purpose of this essay, now let's explore one of the most crucial sectors, the healthcare sector, and examine how the NIST framework is applied in this specific setting. The NIST Cybersecurity framework can be effectively applied in all kinds of organizations and sectors, including healthcare organizations. Healthcare organizations usually deal with highly sensitive patients' data and rely heavily on digital medical equipment, emphasizing the need for better protection against potential cyber threats. The Health Insurance Portability and

Accountability Act (HIPPA), a federal law that provides national standards to protect patient health information against unauthorized access (Chipeta, 2025). In order to comply with HIPPA, organizations may leverage the NIST cybersecurity framework to strengthen the cybersecurity posture. For example, the six functions can be applied as follows: **Identify** critical assets such as, patients' health records, medical equipment etc., and **Protect** them through access controls, encryption, and employee training, **Detect** threats using continuous monitoring systems or Intrusion Detection Systems (IDS), **Respond** to cyber attacks with incident response plans, and **Recover** to restore systems as quickly as possible. Finally, the **Govern** function focuses on guiding and prioritizing the outcomes of the other five functions (NIST CSF 2.0).

As discussed earlier, the NIST Cybersecurity Framework was developed to enhance the protection of the nation's critical infrastructure, thereby strengthening overall national security. Moreover, it aligns closely with the U.S. National Cyber Strategy by supporting its objective of securing the nation's digital ecosystem and safeguarding critical infrastructure from cyber threats.

In conclusion, the NIST Cybersecurity Framework serves as an effective and widely recognized tool for organizations seeking to strengthen their cybersecurity posture. Although adoption is not mandatory, it is found highly effective when implemented properly. This proactive approach strengthens organizational resilience and acts as a preventive measure, helping organizations to anticipate and mitigate evolving cyber threats.

References:

Compliance Guide: NIST CSF and the Healthcare Industry | UpGuard. (n.d.).

Www.upguard.com.

<https://www.upguard.com/blog/compliance-guide-nist-csf-healthcare-industry>

GovFacts. (2025, December 5). *GovFacts*. GovFacts.

<https://govfacts.org/government/federal/agencies/commerce/nist/the-nist-cybersecurity-framework-a-guide-for-u-s-businesses/>

How to Map Healthcare Risks to NIST Framework. (2025, December 24). Censinet.com;

Censinet. <https://censinet.com/perspectives/how-to-map-healthcare-risks-to-nist-framework>

NIST. (2025). *Cybersecurity Framework*. National Institute of Standards and Technology.

<https://www.nist.gov/cyberframework>

NIST. (2024). The NIST cybersecurity framework (CSF) 2.0. *The NIST Cybersecurity*

Framework (CSF) 2.0, 2.0(29). <https://doi.org/10.6028/nist.cswp.29>

National Cyber Security Strategies: The Past, Present, and Future. (2025, July 29). USENIX.

<https://www.usenix.org/publications/loginonline/national-cyber-security-strategies-past-present-and-future>