

Political Implications of NIST Cybersecurity Framework

The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) was originally developed in 2013 to support the nation's critical mission of safeguarding critical infrastructure. Due to its flexible, repeatable, and technology-neutral nature, it has been widely adopted by many organizations as a benchmark for identifying, assessing, and managing cyber risks. While many federal agencies are required to adopt NIST standards, it is primarily a voluntary risk management guide that organizations can leverage to strengthen their cybersecurity posture. Despite its widespread popularity, the framework also carries significant political implications at both the national and international levels. This essay examines the political implications of the NIST Cybersecurity Framework in depth.

The NIST cybersecurity framework has emerged as one of the most influential tools in the field of cybersecurity, carrying several significant political and strategic implications. Although the framework was introduced as a voluntary framework, it raises serious considerations about whether it should be made mandatory across all organizations, including private and government sectors. Interestingly, even though the framework provides substantial benefits, it has not been made mandatory because of several advantages it provides; for example, it supports organizational autonomy, allowing entities to tailor their cybersecurity practices to their specific needs and risk profiles.

Moreover, policy makers have treated this framework as a mechanism to influence private institutions' cybersecurity practices and to support strengthening national security. Its voluntary nature, rather than formal legislation, has contributed to its widespread adoption across diverse sectors, enabling broad implementation without the constraints of formal legislation. The

reasons policymakers reached this conclusion involve several factors and considerations, from the framework's development to its implementation, which we will discuss further.

The NIST cybersecurity framework was created to address the growing concerns about cyber threats to critical infrastructure. During its development, the National Institute of Standard and Technology (NIST) collaborated with industry stakeholders, academic experts, along with government agencies to address the common issues of cyber attacks. Policymakers recognized that a vast amount of critical infrastructure is privately owned, making such policy documents highly reliable upon 'public-private partnership' a key mechanism to mitigate threats (Carr, 2016). Therefore, rather than imposing strict mandatory rules, policymakers chose a collaborative, risk-based approach that encouraged voluntary adoption and allowed for greater flexibility. Carr (2016) argued that this decision reflects previous negative experiences with regulatory models, which often led to lower compliance rather than meaningful improvements in security.

"Soft regulation" is another major political implication that emerged from this framework. Although the framework is voluntary, federal agencies are required to comply with NIST standards under the Federal Information Security Modernization Act (FISMA). In addition, organizations that handle or process sensitive federal information often adopt the NIST standard to demonstrate due diligence in order to receive federal grants or contracts. Due to this indirect regulatory influence, policymakers are able to shape flexible cybersecurity practices without imposing strict regulations, ultimately making it favorable for both private and federal institutions. As a result, this led to the policymakers ultimately arriving at their conclusions through a combination of economic analysis, stakeholder engagement, and crisis responses.

Since the cyber vulnerabilities can be exploited in both private and public systems, this outcome-based approach is beneficial and highly adaptable across various sectors.

In conclusion, the NIST cybersecurity framework represents a significant evolution in cybersecurity governance. Although voluntary in nature, it operates as a powerful policy shaping federal compliance as well as private sector behavior in protecting their cyber landscape. As cyber threats continue to rise, affecting both private and public institutions, political debates over whether this framework should be made mandatory or remain voluntary will continue to be a central focus for policymakers in shaping effective cybersecurity policies and strategies.

References

- Bernardo, L., Malta, S., & Magalhães, J. (2025). An Evaluation Framework for Cybersecurity Maturity Aligned with the NIST CSF. *Electronics*, 14(7), 1364.
<https://doi.org/10.3390/electronics14071364>
- Carr, M. (2016). Public-private partnerships in national cyber-security strategies. *International Affairs*, 92(1), 43–62. <https://doi.org/10.1111/1468-2346.12504>
- Federal Information Security Modernization Act (FISMA)*. CMS Information Security and Privacy Program. (n.d.).
<https://security.cms.gov/learn/federal-information-security-modernization-act-fisma>
- History and creation of the CSF 1.1*. NIST. (2024, February 26).
<https://www.nist.gov/cyberframework/history-and-creation-framework>
- Ibrahim, A., Valli, C., McAteer, I., & Chaudhry, J. (2018). A security review of local government using NIST CSF: A case study. *The Journal of Supercomputing*, 74(10).
<https://doi.org/10.1007/s11227-018-2479-2>
- Stoltz, M. (2024, May 11). *The road to compliance: Executive Federal agencies and the NIST Risk Management Framework*. arXiv.org. <https://arxiv.org/abs/2405.07094>
- Tsarynny, I. (2025, April 25). *Who must comply with NIST? A compliance guide*. Feroot Security.
<https://www.feroot.com/blog/who-must-comply-with-nist-guide/>