Political Implications: NIST Cybersecurity Framework 2.0

CYSE 425W

Danny Choi

May 16, 2025

The NIST Cybersecurity Framework 2.0 (CSF) is a framework for organizations, public and private, to voluntarily follow to mitigate any adverse cybersecurity risks. It is a byproduct of the National Institute of Standards and Technology (NIST) and was meant to be universally applicable as an industry standard. In terms of political aspects, it does not have any affiliation, but due to the rise in cyber-attacks and cybersecurity concerns, the political implications of different industry frameworks, like the CSF, are being implemented. This paper will look at the political implications, specifically the CSF, and how politicians or policymakers have addressed the CSF, why they came to these conclusions, and the ramifications of their decisions.

Politicians and policymakers have begun to understand the importance of cybersecurity and have begun to undertake the position of supporting implementation of different frameworks. In the case of CSF, many policymakers have widely supported the framework due to its nature of flexibility and adaptability on all different fronts, without the need for oversight and regulatory burden. The NIST collaborates with government and private sectors to establish a baseline with generational updates to manage cybersecurity risks. “While adherence to the CSF is voluntary… policymakers have looked to the Framework as one of the ways to assess whether an organization has implemented reasonable security” (Gesser et al., 2023). The CSF is held in high regard, but in politics, the debate goes on about what the industry standard should be. The need for regulatory oversight in areas such as mandatory standards, as opposed to freedom of regulatory to create competition and innovation, is a political debate that will shape how the CSF gets implemented throughout the industry (Gesser et al., 2023).

With the growing amounts of cyberattacks crippling different factions of the industry, politicians and policymakers are escalating the notion of threats that are detrimental or harmful to national security. Even though there isn’t an industry standard, CSF is still held in high regard,

and “there is a fundamental tension between NIST’s flexible, intentionally non-regulatory approach to the CSF and establishing it as a regulatory baseline” (Brown et al., 2023). The issue that arises without an industry standard is how to protect national security and what should be mandated or regulated. Private sectors, governments, and other affiliates all have different agendas and needs, but the rising urgency to protect national security, the stability of the economy, and the trust of the public is something that is at the forefront of policymakers and politicians alike.

The political adoption of a framework like the CSF would have ramifications and consequences that would affect the industry. The CSF has always been a flexible and elective framework, and the incorporation as the industry standard would highlight the gaps in security resources of small to big organizations. The uneven adaptation and implementation disparity could highlight even bigger issues such as government funding and resource allocations (Oluomachi et al., 2024). However, even though there would be challenges, there are stories of success. “The implementation of the NIST Cybersecurity Framework has positively impacted organizations across various sectors… like Microsoft…[and demonstrates]… its effectiveness” (Oluomachi et al., 2024).

Cyberspace is a new domain, and the urgency for a regulatory standard is growing more prominent every day. Cyberthreats are becoming increasingly common and not only affect organizations and companies but also national security and the stability of the nation. Organizations and companies need to incorporate frameworks, like the CSF, and have security readiness. In conclusion, this paper has examined the political implications of the CSF, how politicians or policymakers addressed it, why they came to these decisions, and the consequences of their decisions.

References:

Brown, J., Brown, M., Scott, K., Waldman, J., & White, S. (2023). *NIST cybersecurity framework 2.0 reveals major shifts in federal guidance*. JD Supra. https://www.jdsupra.com/legalnews/nist-cybersecurity-framework-2-0-1207953/

Gesser, A., Liebermann, E., & Roberts, M. R. (2023). *Takeaways from proposed changes to the NIST Cybersecurity Framework*. Harvard Law School Forum on Corporate Governance. https://corpgov.law.harvard.edu/2023/04/01/takeaways-from-proposed-changes-to-the-nist-cybersecurity-framework/

Oluomachi, E., Ahmed, A., Ahmed, W., & Samson, E. (2024). *Assessing the effectiveness of current cybersecurity regulations and policies in the US*. arXiv. https://arxiv.org/abs/2404.11473