Political Implications of the NIST Cybersecurity Framework

Akela Villegas

Old Dominion University School of Cybersecurity

CYSE 425W: Cyber Strategy and Policy

Dr. Shideh Yavary Mehr

June 30, 2025

Abstract

This paper analyzes the political implications of the NIST Cybersecurity Framework (CSF), a widely adopted but voluntary policy tool developed by the National Institute of Standards and Technology. Even though the CSF is technical, it has become politically significant due to its influence on federal regulatory debates, public and private partnerships, governmental relations, and policy concerns. This paper also examines how U.S. policymakers, including legislators and federal agencies, have addressed the CSF, the political motivations behind their actions, and the consequences of those decisions. Using a political science lens, this analysis draws from scholarly literature to demonstrate how the CSF's flexible design intersects with civil liberties, regulatory governance, and federalism, shaping the broader national cybersecurity agenda.

Overview

The NIST Framework was developed through an inclusive process including federal agencies, small to large businesses, and academia. While it is technical nature is clear, the CSF's political implications extend well beyond cybersecurity operations, influencing many areas.

Regulatory Authority and Partisanship

Although voluntary, the CSF has become a political instrument shaping discussions on the extent of federal regulatory power. Legislators who are wary of government overreach argue that the CSF's voluntary nature respects autonomy, while others seek to make it a binding standard. These debates reflect a broader political tension between proponents of strong federal oversight and defenders of autonomy. Scholars note that such tension frequently slows

cybersecurity progress, as competing policy priorities must be balanced alongside national cybersecurity goals (Khan).

Incentives and Federal Resource Allocation

Federal support for CSF adoption via funding, technical assistance, and acquisition preferences signals political prioritization. For example, grants from institutions like the Department of Homeland Security and incentives for CSF alignment in federal contracts show an evolving policy landscape where adherence to the CSF translates into benefits. This creates political power dynamics. Organizations that implement CSF-aligned cybersecurity are favored by policymakers, reinforcing the framework's adoption without regulation. However, budget politics also matter: research shows that policy attention and controversy heighten the science content, such as CSF usage, within regulatory justification documents, suggesting that politically prominent cybersecurity rules draw more evidence and gain stronger legitimization (Costa, 2015).

Public-Private Information Sharing Dynamics

A central political dimension of the CSF is its role in facilitating or constraining information sharing between private entities and the government. Policies like the Cybersecurity Information Sharing Act (CISA) of 2015 encourage data exchange, yet pose challenges around trust, liability, and privacy. Scholars Elaine Sedenberg and James Dempsey observe that governance of these sharing networks reflects a web of political negotiations. How much control should government have, what liabilities are assigned to private partners, and which privacy protections are guaranteed? They stress that implicit trust among sectors underpins effective

cybersecurity policy but also generates political trade-offs regarding oversight and civil liberties (Sedenberg, 2018).

Civil Liberties and Privacy Concerns

Even though the CSF itself doesn't directly regulate individual behavior, its governance and threat-reporting mechanisms intersect heavily with privacy norms. Privacy advocates fear that more standardization of CSF-linked monitoring and data exchange into private networks may erode safeguards. Politicians sympathetic to such concerns argue for built-in privacy protections and transparency mechanisms. The governance politics around CSF, therefore, center on embedding civil liberties, often invoking broader debates about state surveillance versus public safety.

Federalism and Government Coordination

Finally, the CSF's deployment highlights the complex interplay of federalism. Initially aimed at critical infrastructure oversight at the federal level, the CSF is now being endorsed—though not mandated—by state and local governments. This diffusion expands its influence but introduces policy fragmentation, where adoption varies by jurisdiction. While some states integrate CSF into procurement and government cybersecurity policies, others resist, citing local autonomy. This creates an uneven national cybersecurity environment shaped as much by local politics as by federal incentives.

References

Costa, M., Desmarais, B. A., & Hird, J. A. (2015, December 1). *Science use in regulatory impact analysis: The effects of political attention and controversy*. arXiv.org. https://arxiv.org/abs/1512.00448

Khan, M. M. (n.d.). JSAER. https://jsaer.com/download/vol-10-iss-8-2023/JSAER2023-10-8 150-157.pdf

Sedenberg, E. M., & Dempsey, J. X. (2018, May 31). *Cybersecurity Information Sharing Governance Structures: An ecosystem of diversity, trust, and tradeoffs*. arXiv.org. https://arxiv.org/abs/1805.12266