# Implications of NIST Cybersecurity Framework Version 2.0

**Jack C. Gubasta**

**School of Information, University of South Florida**

**LIS4934: BSIS Senior Capstone**

**Dr. Alicia K. Long**

**February 29, 2024**

**Implications of NIST Cybersecurity Framework Version 2.0**

The National Institute of Standards and Technology (NIST) is a government agency under the US Department of Commerce. The NIST is tasked with developing standards and guidelines for a broad range of technological industries including cybersecurity, IT, manufacturing, and more. In cybersecurity, they are commonly known for developing the NIST Cybersecurity Framework and their special 800 series publications which provide guidelines and procedures for information security. The first version of the NIST Cybersecurity Framework was produced in 2014 and was widely accepted by the cybersecurity community and implemented by countless organizations across the US. 10 years later, the NIST has released version 2 of their cybersecurity framework. This essay will cover what has been updated as well as what this could mean for stakeholders, and any legislative implications version of the NIST Cybersecurity Framework might pose.

Every year, new vulnerabilities and exploits are discovered, giving cybercriminals a consistent flow of new attack vectors and challenges that will eventually be exploited at the cost of their target. The first version of the NIST Cybersecurity Framework is extremely technical and can be very confusing for smaller organizations that may not have any cybersecurity professionals on hand. Version 2 attempts to fix this by making the document more accessible to less tech-savvy individuals, according to Chad Boutin, an employee of the NIST "The new 2.0 edition is designed for all audiences, industry sectors, and organization types, from the smallest schools and nonprofits to the largest agencies and corporations — regardless of their degree of cybersecurity sophistication" (Boutin C.,

2024). This new level of readability makes it more accessible to lesser educated individuals than the first version. This allows for stakeholders to better understand the more technical aspects of cybersecurity in a much easier-to-read document.

Another major change to the NIST framework is the addition of the “Govern” function to its core functions. Previously known as the “5 pillars of Cybersecurity,” according to Laura French “NIST conceptualizes the “Govern” function as being central to the rest of the pillars, symbolizing its holistic connection to all other CFS functions” (French L., 2024). Meaning governance is a key aspect that helps control the other 5 pillars allowing for more well-informed, and better communicated policies.

Since the original NIST Cybersecurity Framework has been referenced in countless federal legislation, we can expect version 2 to have a similar impact on our laws and regulations. For example, NIST standards may be incorporated into laws requiring specific security measures for government agencies or critical infrastructure sectors. Legislators are likely to use this new framework when drafting bills aimed at enhancing cybersecurity standards across various industries. Industries regulated by the federal government will most likely need to make changes in their security postures to meet the newer standards of NIST 2. This would require businesses and organizations under the umbrella of said industry to comply with NIST 2 which would allow for a more standardized approach to cybersecurity. At the state level, if multiple states implement NIST 2 as a standard this could create better consistency for a state's cybersecurity posture.

Although consistency within cybersecurity may make things easier for those tasked with protecting them, it could also pose the threat of systems being easier to exploit. A strict level of uniformity could allow multiple different systems to be exploited in the same way at different times. That is why a layered defense is always your best friend and part of the reason why businesses might take liberty with the Framework. As it states, this is a *framework* and not an explicit law or regulation.

As you can see, the release of version 2 of the NIST Cybersecurity Framework marks a significant evolution in cybersecurity standards and guidelines. The latest version of the NIST Cybersecurity Framework was written with accessibility in mind, allowing for a broader audience of professionals to have a greater level of understanding of how best to protect their organization and mitigate cyber-attacks from happening in the first place. NIST 2 has also added the “Govern” function as a central part of the 5 pillars of cybersecurity emphasizing the importance of governance in guiding and coordinating cybersecurity efforts. Lastly, we discussed the legislative impact we can expect to see as a result of the latest NIST Cybersecurity Framework. Overall, NIST 2 represents a crucial step forward in addressing evolving cybersecurity challenges and promoting a more standardized approach to cybersecurity across sectors.

# Works Cited

Boutin, C. (2024, February 26). *NIST releases version 2.0 of Landmark Cybersecurity Framework*. NIST. https://www.nist.gov/news-events/news/2024/02/nist-releases-version-20-landmark-cybersecurity-framework.

French, L. (2024, February 28). *Top 3 NIST cybersecurity framework 2.0 takeaways*. SC Media. https://www.scmagazine.com/news/nist-publishes-cybersecurity-framework-2-0-3-key-takeaways.