Sutter Health

[redacted]

November 6, 2023

SUBMITTED ELECTRONICALLY VIA cyberframework@nist.gov
Cherilyn Pascoe
NIST Cybersecurity Framework Program Lead
National Institute of Standards and Technology

RE: Discussion Draft: The NIST Cybersecurity Framework 2.0 Core with Implementation Examples

Dear Ms. Pascoe:

Sutter Health was founded in 1921 and is a non-profit, integrated health delivery system that encompasses more than twenty-three hospitals, thirty-three ambulatory surgery centers, and over thirty other health care centers and facilities serving northern California. The Sutter Health workforce includes more than 53,000 dedicated team members, 12,000 physicians, nurse practitioners and physician assistants providing services in support of more than three million patients.

At Sutter Health, we hold a steadfast commitment to patient safety by recognizing the paramount importance of safeguarding patient privacy within the ever-evolving healthcare landscape. Sutter is appreciative of NIST providing the opportunity to submit comments on the NIST Cybersecurity Framework (CSF) and all that your organization does in sharing resources, guidance, and strategy in cybersecurity governance. Sutter's comments relate to the following areas: (1) How Sutter currently integrates the CSF into its operations and (2) Improvements to the CSF to consider moving forward.

HOW SUTTER HEALTH USES NIST CYBERSECURITY FRAMEWORK (CSF)

As a critical infrastructure organization, Sutter Health currently integrates the NIST CSF into its privacy and information security program by adopting many of the capabilities identified within the CSF. Sutter Health integrates concepts from the CSF in policies, procedures, processes, controls and operational requirements to help manage and monitor cybersecurity risks. The CSF framework provides clear insight into identifying risk, informing our vulnerability management strategy, and helping provide the quality metrics necessary for managing risk.

However, in the years since the last update, new cybersecurity risks, vulnerabilities, and concerns have emerged for health systems that the prior version of the CSF did not adequately address.

A growing reliance on third party vendors and the growing importance of IoT devices in health care have made it increasingly difficult for health systems to protect critical data. Systems are more and more reliant on the security of these vendors and IoT device manufacturers, but often have little to no recourse when these organizations neglect their security. The cost of health care data breaches has risen 53 percent since 2020[1]. This is reflected in the cybersecurity insurance industry, which is the fastest-growing segment of the market[2] and saw a year-on-year

[1] Average Cost of Healthcare Data Breach Reaches $11M (healthitsecurity.com)

[2] Cyber insurance market growing with rising cyber threats - Insurance News | InsuranceNewsNet

price increase of 48% in the third quarter of 2022[3]. Hospital systems' vulnerabilities are now spread out across an increasing number of organizations but the ability to share knowledge across organizations has not improved. We applaud NIST for releasing an updated CSF draft that addresses emergent vulnerabilities in cybersecurity and look forward to seeing additional guidance on these areas in the final draft.

Supply Chain Risk Management

While Sutter Health appreciates the addition of a Cybersecurity Supply Chain Risk Management category, we believe that this topic is important enough to merit its own classification. One of the greatest strengths of the CSF is how it incorporates industry feedback to respond to the rapidly changing landscape of cybersecurity. Supply chain risks are a large and ever-growing threat, and mitigating these risks requires more and more resources from organizations. A 2022 survey by BlueVoyant found that in the last year, 98 percent of respondents had been negatively impacted by cybersecurity breaches in their supply chain and 85 percent increased their supply chain risk budget, with 20 percent reporting an increase of over 100 percent. Organizations are often at the mercy of the vendors they employ. For example, if a pacemaker or patient monitoring system manufacturer is late in patching their software, potentially impacting patient safety, hospital systems have limited recourse to resolve this issue. The BlueVoyant survey found that 40 percent of respondents had no way of knowing when or if suppliers had security issues, and 42 percent said that when suppliers did report issues, the organization could not verify if the matter was resolved.

Given how vulnerable organizations are to vendor security breaches, it is critical that they receive guidance on how to establish vendor partnerships. This guidance should include templates for how to conduct assessments of third-party vendors, self-assessment templates for vendors to examine their own security posture, when to advise vendors to acquire cybersecurity insurance, and vendor education templates to ensure their employees are trained. It is also recommended to include guidance on the minimum cyber hygiene that vendors must adhere to including guidelines on encryption, access control, multi-factor authentication, data handling procedures, data storage, data retention, data destruction, disaster recovery, incident response, and security incident notification procedures. Organizations can benefit from guidance on best practices for continuous vendor monitoring, when to conduct deeper assessments such as onsite audits, architecture reviews or penetration testing, and the needed capabilities to safeguard organizations using multiple layers of protection. We applaud all that NIST has done to address this issue in the latest draft and encourage the organization to go even further in its final product.

Internet of Things (IoT)

Similar to supply chain risk management, IoT devices represent a growing cybersecurity concern. At Sutter, we have numerous devices across our network that are connected to patients or delivering care, and the number will continue to grow. IoT devices offer incredible possibilities to transform patient care and improve safety at hospitals. Remote monitoring allows constant tracking of blood pressure, heart rate, glucose levels, and other critical signals, and can send out alerts to physicians and family members when these signals indicate an emergency. At hospitals, IoT use cases range from humidity and temperature controls to robotic surgery devices. As IoT

[3] The Cost of Cyber Insurance Just Keeps on Rising (tech.co)

use cases grow in the medical sector, so does the need for consistent guidance on how to properly deploy these devices. Hospitals depend on manufacturers to provide adequate protection for their devices, and when they do not, the hospital must develop costly corrective measures to mitigate vulnerabilities. For example, the recent Log4Shell vulnerability forced healthcare providers to analyze and triage the impacts of the vulnerability for each connected medical device and implement mitigation measures, while some vendors took more than six months to implement a patch.

Understanding the risks posed by IoT devices is an expensive and time-consuming undertaking for hospital systems and will only become more burdensome as these devices become more integrated into care. Accordingly, NIST should integrate an IoT template for standards and controls into the CSF. Such IoT guidance will provide consistent, reliable, and industry recommended practices for those seeking effective controls.

Third Party Cloud Management

Sutter would like to see more guidance provided in the CSF on how to remain secure while outsourcing system cloud management to a third-party. Third-party cloud management services are becoming more and more common, as many companies lack the in-house resources to develop their own systems. These companies leverage third-party vendors to handle both the legal and operational responsibility for managing all or some parts of their cloud platform. The current framework largely assumes that a company is fully in control of their system cloud management, and the framework only briefly acknowledges that companies may be utilizing third-party cloud management services. Given the increased use of these third-party services and the security gaps that can be created by utilizing them incorrectly, we urge NIST to provide more guidance on how companies can evaluate these services for vulnerabilities and leverage them without increasing security risk.

We appreciate your consideration of our feedback. Should you have questions, please do not hesitate to contact Jonathan Williams, vice president of government affairs, by phone at [redacted]

Sincerely,

Jacki Monson

Jacki Monson, Senior VP, Chief Integration Officer, Chief Privacy and Information Security Officer

Sutter Health