Sutter Health

April 25, 2022

Department of Commerce
Requesting Party: National Institute of Standards and Technology (NIST)
Responding Party: Sutter Health, Jacki Monson, SH VP, CTRO, CISO & CPO
ACTION: Notice; request for information.
Docket Number: 220210–0045 Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management

Re: **"NIST Cybersecurity RFI"**

Sutter Health is a not-for-profit healthcare organization providing comprehensive, integrated medical services in more than 100 Northern California communities. Our organization is staffed by over 55,000 employees and affiliated with 12,000 physicians providing care to more than 3 million patients. Central to our values are commitments to working with the diverse communities we serve, providing excellence, quality, safety to our patients, and ensuring the privacy and security of our patients' information.

Sutter is appreciative of NIST providing the opportunity to submit comments on the NIST Cybersecurity Framework (CSF) and all your organization does in sharing resources, guidance, and strategy in cybersecurity governance. Sutter's comments relate to the following arears: (1) How Sutter currently integrates the CSF into its operations, (2) Improvements to consider moving forward to the CSF, and (3) Existing Supply Chain Cybersecurity Needs.

HOW SUTTER USES NIST CYBERSECURITY FRAMEWORK (CSF) AND ITS USEFULESS

As a critical infrastructure organization, Sutter Health currently integrates the NIST Cybersecurity framework (CSF) into its Privacy and Information Security Program to protect, better understand, manage, and reduce cybersecurity risks. Sutter has adopted many of the security controls identified within the CSF. The CSF provides Sutter with excellent guidance in helping to provide best practice standards to increase patient safety in reducing cyber risk by increasing data confidentiality and data integrity. Per the CSF, Sutter drafts policies, procedures, and processes to manage and align with the organization's regulatory risk, legal, and operational requirements to help manage and monitor cybersecurity risks. The NIST CSF provides Sutter with clear insight into identifying risk, vulnerability management strategy, and helping to provide quality metrics to leaders to make qualitative decisions in managing risks. Sutter also utilizes the CSF to implement information security measures that encompasses user access, infrastructure, and physical security. The NIST CSF provides an organized framework to implement a structured security program for organizations, including Sutter, to maintain compliance, mitigate cyber risks, and cyberattacks while protecting the safety of our patients and their data.

HOW NIST CSF COULD IMPROVE – PROVIDING STANDARDS FOR PROTECTION OF IoT DEVICES

Today's business systems are vast networks of interconnected devices surrounded by the world-wide web, also known as the Internet. IoT devices present a clear and present risk to most business networks because of both the potential and actual access these platforms provide to cyber criminals looking for opportune ways to infiltrate critical business structures. With the rise of ransomware, malware, and nation-state attacks on our critical infrastructure, NIST should integrate into its CSF an IoT template for standards and controls for critical infrastructure organizations. Such IoT guidance will provide consistent, reliable, and industry recommended practices for those seeking effective controls.

HOW NIST CSF COULD IMPROVE – THIRD-PARTY CLOUD MANAGEMENT

Complying with NIST assumes a company is fully in control of their system cloud management, but most are managed by third parties. Most companies don't manage or secure their own cloud infrastructure. Many take advantage of third-party companies to handle both the legal and operational responsibility for managing all or some parts of their cloud platform. Companies who want to take cybersecurity seriously but who lack the in-house resources to develop their own systems lack proper guidance on how to utilize these third-party cloud management services. According to cloud computing expert Barbara Ericson of Cloud Defense, "Security is often the number one reason why big businesses will look to private cloud computing instead of public cloud computing." NIST should consider that third-party cloud management is becoming more standard practice and provide industry guidance accordingly.

HOW NIST CSF COULD IMPROVE - "Role-Based Access Control" (RBAC)

Roles that staff are expected to perform within business network environments are more complex than ever. NIST, having been developed almost a decade ago doesn't effectively deal with this. NIST recommends that companies use what it calls RBAC – "Role-Based Access Control" – to secure systems. RBAC becomes extremely cumbersome when it comes to modern complex interconnected systems.

Individual employees are now expected to be system administrators for one system, staff managers within another, and mere users on a third. Assigning security credentials based on employees' roles within the company is very complex. It is important that companies go beyond the standard RBAC contained in NIST. "Admin" functions should be separate for various systems, which allows a more granular level of control over the rights granted to employees. Additionally, Admin functions and rights should be granted least privilege access as well. This will help to restrict access controls when required. These recommendations should be considered moving forward.

THE SUPPLY CHAIN CYBER SECURITY NEEDS

The cybersecurity supply chain represents many possible entry points for cybercriminals. Staying vigilant and implementing best practices can make the difference in successfully navigating today's ever-shifting, increasingly inter-connected industrial landscape. Supply chain risks inherently involve multiple parties and locations, which may involve complex and comprehensive controls. Many companies need the following cyber guidance in managing supply chain risks:

- ➢ **Best Practices on Establishing Vendor Partnerships**

  - Security self-assessment templates (what security tools they are using, what privileged access management policy they have in place, are they keeping up with their patches and updates, etc.)
  - Vendor audit templates
    - Recommendations on when to run penetration tests on vendors
  - Templates on when to advise vendors to acquire cyber insurance
- Templates on vendor education to ensure their employees are trained
- Best practices on safeguarding organization using multiple layers of protection

The above-referenced recommendations are some Sutter would like to see considered in updating the CSF, by NIST moving forward. On behalf of Sutter Health, thank you for the opportunity to provide these comments on the CSF. Please contact me directly with any questions via email
[redacted]

Respectfully,

Jacki Monson
SH VP, CTRO, CISO & CPO
Office of the General Counsel
[redacted]