KAISER PERMANENTE®

Kaiser Foundation Health Plan
Program Offices

April 25, 2022

National Institute of Standards and Technology (NIST)
100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899

RE: *Request for information regarding Cybersecurity Framework and Cybersecurity Supply Chain Risk Management (NIST-2022-0001)*

Submitted electronically via www.regulations.gov

Kaiser Permanente (KP) appreciates the opportunity to offer comments on the above-captioned request for information (RFI).[1] The Kaiser Permanente Medical Care Program is the largest private integrated health care delivery system in the U.S., delivering health care to over 12 million members in eight states and the District of Columbia[2] and is committed to providing the highest quality health care.

Security breaches and disruptions in supply chains can have devastating consequences for health care organizations and the patients we serve. The NIST Cybersecurity Framework (NIST CSF) has become the gold standard and community best practice that many organizations, including KP, rely upon to formulate their own cybersecurity and risk management strategies. We applaud efforts by NIST to update the NIST CSF and address supply chain risk management, and offer the following in response to questions posed:

Use of the NIST Cyber Security Framework

1. *The usefulness of the NIST Cybersecurity Framework for aiding organizations in organizing cybersecurity efforts via the five functions in the Framework and actively managing risks using those five functions.*

   There is tremendous value in having a national framework that can be adapted to serve organizations of all sizes and across sectors. The NIST CSF provides industry standards, guidelines, and practices in a manner that allows for communication of cybersecurity activities and outcomes across the organization from the executive level to operations. The NIST CSF also allows organizations to build strong cybersecurity foundations and identify risk and compliance gaps. However, the NIST CSF is high level and refers to other frameworks that are organized differently, which may be confusing. Additionally, organizations need a common understanding of how the NIST CSF should and should not be used. Guidance could clarify, for example, that the NIST CSF subcategories are not to be viewed as an alternate source of security controls (separate from the security controls in NIST SP 800-53).

[1] https://www.federalregister.gov/documents/2022/02/22/2022-03642/evaluating-and-improving-nist-cybersecurity-resources-the-cybersecurity-framework-and-cybersecurity

[2] Kaiser Permanente comprises Kaiser Foundation Health Plan, Inc. and its health plan subsidiaries outside California and Hawaii; the not-for-profit Kaiser Foundation Hospitals, which operates 39 hospitals and over 720 other clinical facilities; and the Permanente Medical Groups, self-governed physician group practices that exclusively contract with Kaiser Foundation Health Plan and its health plan subsidiaries to meet the health needs of Kaiser Permanente's members.

2. *Current benefits of using the NIST Cybersecurity Framework. Are communications improved within and between organizations and entities (e.g., supply chain partners, customers, or insurers)? Does the Framework allow for better assessment of risks, more effective management of risks, and/or increase the number of potential ways to manage risks? What might be relevant metrics for improvements to cybersecurity as a result of implementation of the Framework?*

   The NIST CSF is non-prescriptive and provides flexibility for organizations to implement in accordance with their mission and priorities. It can be a powerful mechanism to create common understanding about resiliency and demonstrate measurable improvements in maturity. KP manages threats and vulnerabilities through operational processes that align with NIST CSF's five functions (Identify, Protect, Detect, Respond, Recover). We appreciate that the NIST CSF provides the ability to compare with peers (e.g. benchmarking) and to speak the same language via an industry standard. We recommend organizations use the NIST CSF to assess and optimize the Target Profile and Tiers, rather than treating subcategories as requirements or controls.

3. *Challenges that may prevent organizations from using the NIST Cybersecurity Framework or using it more easily or extensively (e.g., resource considerations, information sharing restrictions, organizational factors, workforce gaps, or complexity).*

   The NIST CSF provides a good starting point for organizations to adopt as the basis for organizational policies within their own IT/IS/Cybersecurity Department. However, implementing these policies can be labor intensive and requires dedicated resources. Additionally, organizations need commitment, socialization, and support from senior leadership. Implementation of the NIST CSF also requires collaboration within the organization to ensure that mappings of varying control sets for different security assessment initiatives (e.g. International Organization for Standardization (ISO) or Health Information Trust Alliance (HITRUST)) are aligned under the NIST CSF. Some organizations experience challenges related to over-reliance on mappings, often at the expense of improving the maturity of their cybersecurity practices.

4. *Any features of the NIST Cybersecurity Framework that should be changed, added, or removed. These might include additions or modifications of: Functions, Categories, or Subcategories; Tiers; Profile Templates; references to standards, frameworks, models, and guidelines; guidance on how to use the Cybersecurity Framework; or references to critical infrastructure versus the Framework's broader use.*

   We recommend that NIST take the following actions to update features of the NIST Cybersecurity Framework:

   - Working in conjunction with HHS, update the NIST CSF Crosswalk to the HIPAA Security Rule[3] that was created using v1.0 of the NIST CSF (in 2016). An updated crosswalk would help

[3] https://www.hhs.gov/sites/default/files/nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf

healthcare organizations implement relevant HIPAA safeguards for the new NIST CSF subcategories, including those related to supply chain risk management.

- Provide additional guidance on selection and documentation of specific controls mapped to each subcategory, with a focus on healthcare organizations' need for mandatory HIPAA documentation that shows effective due diligence.
- Update partial NIST CSF References to implementation details and Revision 5 of NIST 800-53[4].
- Clarify and reinforce guidance that organizations adopting the NIST CSF must apply their own risk factors, risk appetite, level of details, business processes, etc. to assist new and less experienced organizations achieve successful cybersecurity.

5. *Impact to the usability and backward compatibility of the NIST Cybersecurity Framework if the structure of the framework such as Functions, Categories, Subcategories, etc. is modified or changed.*

   We do not expect additional guidance to adversely impact the NIST CSF usability or compatibility.

6. *Additional ways in which NIST could improve the Cybersecurity Framework, or make it more useful.*

   No comments.

Relationship of the NIST Cybersecurity Framework to Other Risk Management Resources

7. *Suggestions for improving alignment or integration of the Cybersecurity Framework with other NIST risk management resources. As part of the response, please indicate benefits and challenges of using these resources alone or in conjunction with the Cybersecurity Framework.*

   The resources cited in the RFI provide excellent guidance and should be cross-referenced with the NIST CSF to demonstrate a comprehensive view of managing Privacy, Security and Risk in an organization. This allows for organized objectives and purposes, prioritization of work and resources, capture of relevant risks in company risk register, and appropriate treatment of threats and vulnerabilities. We recommend NIST provide further mapping guidance to assist organizations better understand and achieve a common understanding of the different frameworks.

8. *Use of non-NIST frameworks or approaches in conjunction with the NIST Cybersecurity Framework. Are there commonalities or conflicts between the NIST framework and other voluntary, consensus resources? Are there commonalities or conflicts between the NIST framework and cybersecurity-related mandates or resources from government agencies? Are there ways to improve alignment or integration of the NIST*

[4] https://csrc nist.gov/publications/detail/sp/800-53/rev-5/final

framework with other frameworks, such as international approaches like the ISO/IEC 27000-series, including ISO/IEC TS 27110?

We find there is sufficient synergy between the NIST CSF and ISO/IEC 2700-series approaches and recommend that NIST focus on efforts to encourage organizations to improve their maturity with respect to Cybersecurity and Privacy (i.e., moving toward the organization's Target Profile), rather than attempting to further improve alignment. We recommend that NIST develop and prescribe different levels of the NIST CSF applicable to NIST SP 800-53 security controls and highlight the common vulnerability and exposures (CVE) oriented items. We also encourage NIST to review and align the NIST CSF with the current version of Center for Internet Security Critical Security Controls (CIS CSC).

9. *There are numerous examples of international adaptations of the Cybersecurity Framework by other countries. The continued use of international standards for cybersecurity, with a focus on interoperability, security, usability, and resilience can promote innovation and competitiveness while enabling organizations to more easily and effectively integrate new technologies and services. Given this importance, what steps should NIST consider to ensure any update increases international use of the Cybersecurity Framework?*

   We recommend NIST define standards applicable to specific regulations with international impact, such as the General Data Protection Regulation (GDPR) and requirements of the Center for Medicare and Medicaid Services (CMS) related to offshoring. We also recommend NIST identify varying state regulations and take them into account when considering updates to the NIST CSF to enhance international interoperability, security, usability, and resilience.

10. *References that should be considered for inclusion within NIST's Online Informative References Program. This program is an effort to define standardized relationships between NIST and industry resources and elements of documents, products, and services and various NIST documents such as the NIST Cybersecurity Framework, NIST Privacy Framework, Security and Privacy Controls for Information Systems and Organizations (NIST Special Publication 800-53), NIST Secure Software Development Framework, and the NIST Internet of Things (IoT) Cybersecurity Capabilities Baseline.*

    NIST should consider the following references from the US Cybersecurity & Infrastructure Security Agency (CISA):

    - CISA guidance regarding adoption of NIST CSF across sectors: https://www.cisa.gov/uscert/resources/cybersecurity-framework
    - CISA guidance on Implementation of NIST CSF in the Health and Public Health Critical Infrastructure Sector: Healthcare Sector Cybersecurity Framework Implementation Guide v1.1 (cisa.gov)

Cybersecurity Supply Chain Risk Management

11. *National Initiative for Improving Cybersecurity in Supply Chains (NIICS). What are the greatest challenges related to the cybersecurity aspects of supply chain risk management that the NIICS could address? How can NIST build on its current work on supply chain security, including software security work stemming from E.O. 14028, to increase trust and assurance in technology products, devices, and services?*

    One of the greatest challenges related to cybersecurity aspects of supply chain risk management is that many manufacturers/developers of technological products do not adequately consider cybersecurity when designing their products. It is much more difficult to add cybersecurity attributes to products mid-cycle or post-deployment. Even when manufacturers/developers consider cybersecurity during the design phase, there is not a consistent set of standards to ensure a minimum level of security assurance. We recommend that NIST include a requirement or incentive for off-the-shelf product guarantees in the NIICS to promote efficiency and buyer confidence in technological products and software. The NIICS should also provide guidance for improvements in early detection and communication of supply-chain vulnerabilities to enable an easier and less-punitive path for entities to self-disclose security breaches and communicate more quickly with other impacted entities. Additionally, NIST should reference the E.O. 14028, criteria for Consumer Cybersecurity Labeling of IoT products and Software and Application of risk management for IT network incorporating medical devices (IEC 80001) in the NIICS.

12. *Approaches, tools, standards, guidelines, or other resources necessary for managing cybersecurity-related risks in supply chains. NIST welcomes input on such resources in narrowly defined areas (e.g. pieces of hardware or software assurance or assured services, or specific to only one or two sectors) that may be useful to utilize more broadly; potential low risk, high reward resources that could be facilitated across diverse disciplines, sectors, or stakeholders; as well as large-scale and extremely difficult areas.*

    We recommend NIICS guidance include the following to manage cybersecurity-related risks in supply chains:

    - Require a vendor relationship accountability policy. Organizations should be required to enforce a formal internal organizational accountability policy for vendor relationships that includes a specific and up to date point of contact name for every vendor/supplier contract.
    - Require a security clause in vendor contracts. Organizations should be required to include a data security requirement clause in all vendor contracts where vendors have access to company data (including an update to include this clause in evergreen contracts). Additionally, healthcare organizations should be required to ensure linkage to Business Associate Agreement (BAA) requirements pursuant to the HIPAA Security Rule.

13. *Are there gaps observed in existing cybersecurity supply chain risk management guidance and resources, including how they apply to information and communications technology, operational technology, IoT, and industrial IoT? In addition, do NIST software and supply chain guidance and resources appropriately address cybersecurity challenges associated with open-source software? Are there additional*

approaches, tools, standards, guidelines, or other resources that NIST should consider to achieve greater assurance throughout the software supply chain, including for open-source software?

No comment.

14. *Integration of Framework and Cybersecurity Supply Chain Risk Management Guidance. Whether and how cybersecurity supply chain risk management considerations might be further integrated into an updated NIST Cybersecurity Framework—or whether and how a new and separate framework focused on cybersecurity supply chain risk management might be valuable and more appropriately be developed by NIST.*

    We do not support creation of a separate framework for NIST Cybersecurity Supply Chain Risk Management. A separate framework would be likely to create confusion and misunderstanding with the existing Cybersecurity and Privacy Frameworks because the scope of the Supply Chain Framework resides within and not separate from these existing Frameworks. We recommend that cybersecurity supply chain risk management considerations be further integrated into existing Frameworks and caution against creating new frameworks unless they exist independent of existing frameworks.

***

Thank you for considering our feedback. If you have questions or concerns, please contact me at [redacted]

Sincerely,

Jamie Ferguson
Vice President, Health IT Strategy and Policy
Kaiser Foundation Health Plan, Inc.