KAISER PERMANENTE®

Kaiser Foundation Health Plan
Program Offices

November 6, 2023

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

RE: *Draft NIST Cybersecurity Framework 2.0* (NIST CSWP 29)

Submitted electronically via cyberframework@nist.gov

Kaiser Permanente (KP) appreciates the opportunity to offer comments on the above-captioned request for feedback on draft version 2.0 of the Cybersecurity Framework (CSF).[1] The Kaiser Permanente Medical Care Program[2] is the largest private integrated health care delivery system in the United States, with more than 12.6 million members in eight states and the District of Columbia. Kaiser Permanente's mission is to provide high-quality, affordable health care services and to improve the health of our members and the communities we serve.

Security threats and breaches 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 using it is a 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 CSF to keep pace with the evolving cybersecurity landscape and offer the following in response.

General Comments

This draft revision provides much needed enhancements to adapt NIST guidance to the current cybersecurity environment in alignment with leading practices and guidance resources. We also find that the draft revision reflects feedback provided so far, particularly in the reorganization of information, explanation of the Framework purpose and use and addition of the new core function "Govern". We are pleased that NIST accepted recommendations to develop sector-specific profiles for adopting the CSF and we look forward to contributing towards the development of the health care Community Profile.

We recommend that NIST include an appendix that maps v1.1 to v2.0 and highlights modifications, additions, and deletions to support organizations as they transition to the newer version.

Section 1 – Introduction

We recommend the following amendments to further improve this section:

- Add "monitoring" as a risk assessment/governance opportunity as part of the "Understand and Assess" activity. While "monitoring" is included as part of the "Govern" core function we think it should also be

[1] https://csrc.nist.gov/pubs/cswp/29/the-nist-cybersecurity-framework-20/ipd

[2] Kaiser Permanente comprises Kaiser Foundation Health Plan, Inc., one of the nation's largest not-for-profit health plans, and its health plan subsidiaries outside California and Hawaii; the not-for-profit Kaiser Foundation Hospitals, which operates 39 hospitals and more than 700 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.

included as an element of the "Understand and Assess" activity to reinforce the accepted practice[3] and make it clear that organizations should continuously monitor during this phase. It could also be added as an additional, stand-alone element in the framework.

- Include cybersecurity regulations in Section 1.1 Audience (line 157) to assist with common understanding and consistent application of cybersecurity framework recommendations across regulatory agencies. Proposed language edits are as follows: Additionally, the Framework can be useful to policymakers (such as associations, professional organizations, and regulators) to set and communicate priorities for cybersecurity risk management, as well as cybersecurity rules and regulations.

Section 2 – Understand the Framework Core

We recommend the following amendments to further improve this section:

- Page 5, line 203. IDENTIFY. We recommend edits to include the concept of identity instead of people, and to include suppliers (vendors or 3rd parties) in the example list. Also see comment on Appendix C ID.AM-02.
  - Proposed language edits: (e.g., data, hardware, software, systems, facilities, services, suppliers, ~~people~~ identities).
- Page 6, line 208. PROTECT. We recommend adding "mitigate" to the first sentence.
  - Proposed language edits: PROTECT (PR) – Use safeguards to prevent, mitigate, or reduce cybersecurity risks.
- Page 6, line 223-225. RECOVER. We recommend amending this language to ensure the recovery effort ends with capturing Lessons Learned and applicable revisions to current policies and processes to document new information previously unknown or incorrect before the incident.
  - Proposed language edits: RECOVER (RC) – Restore assets and operations that were impacted by a cybersecurity incident and documenting relevant process changes. RECOVER supports timely restoration of normal operations to reduce the impact of cybersecurity incidents and enable appropriate communication during recovery efforts. Conclude this phase by capturing lessons learned and updating relevant policies and processes to address future recurrence.

Addition of "Govern" Function

We support the addition of the "Govern" function, however, we recommend additional guidance and definition be included in both the Supply Chain (SC) and Vendor/Third Party Risk Management (TPRM) categories. We recommend that NIST consider both SC and TPRM as distinct risk categories and clearly define both risk domains as separate risks. The heavy focus of SC and light touch of TPRM do not appear to meet the risk of two important but different domains as many cyber adverse events in today's organizations are the direct result of reliance on third parties.

Informative References and Implementation Examples Provided as Part of CORE

The Informative References and Implementation Examples provided as part of CORE are helpful, however, we recommend that the Framework reinforce the message that the Informative References are informative and not

[3] NIST SP 800-137 Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. https://csrc nist.gov/pubs/sp/800/137/final

check-the-box prescriptive requirements. ISO/IEC 27001 and associated standards may be more widely used outside of the U.S., and we recommend including a reference to a site that highlights the differences between NIST SP 800-53 Rev5 and ISO/IEC 27002:2022. We also recommend that updates to Informative References be made available online to allow interested parties to download spreadsheets with current complete content.

Section 3- Using the Framework

Application of the Draft Framework Core to Create Specific Profiles for an Organization

Organizations that have achieved a moderate level of maturity should be able to apply the draft Framework Core to create specific profiles without significant challenge. However, many organizations may not be aware that they have not yet reached a sufficient level of maturity. To increase visibility for the health care sector, we recommend NIST collaborate with OCR to include CSF profile development in HHS Resolution Agreements (e.g., for major breaches).

Community Profile Creation

We recommend that NIST lead efforts to create specific Community Profiles, with a profile for each of the 16 critical infrastructure sectors as defined by CISA. We also recommend that NIST collaborate with relevant regulatory agencies to create supplemental resources that support use cases and implementation. For example, OCR previously provided a mapping of NIST CSF v1.0 subcategories to specific HIPAA Security Rule safeguards. It would be very useful to provide an update of this crosswalk as a resource for covered entities.

Addition of "Managing Cybersecurity Risk in Supply Chains"

The addition of this element in the Framework is crucial to capture Supply Chain impacts to an organization's enterprise risk management. As organizations increasingly rely on vendors/suppliers for products and services (including human resources), Supply Chain and Third-Party Risk Management becomes an increasingly high-risk factor, more so for cybersecurity risk. As mentioned previously, we recommend NIST makes a distinction between Supply Chain Risk Management (SCRM) and Third-Party Risk Management (TPRM) as the industry views them differently.

Section 4 – Integrating Cybersecurity Risk Management with Other Risk Management Domains Using the Framework

We recommend the following amendments to further improve this section:

- Line 611 (page 26) "Target Profiles": We recommend including Third Party Risk Management (TPRM). This section would benefit from outlining how profiles can help manage cybersecurity risk and associated residual risk with TPRM. Vendors should go through the same assessment of how they meet an organizations cybersecurity objective and the level of risk associated to the relationship.
- Section 4.1- Integrating the Cybersecurity Framework with the Privacy Framework: We recommend differentiating between monitoring within a function Governance and monitoring within an operational function/process because the values and outcomes are different. The relationship and interdependency of governance and monitoring is important to address in the framework guidance.

Integration of Framework and Privacy Framework

There is alignment and appropriate integration between NIST CSF 2.0 and NIST Privacy 1.0., both having similar framework constructs organized around Core Functions, Categories, and Sub-categories. However, we

recommend updating the "Govern" function in the Privacy Framework to align with the function in the Framework so that it is applicable to all CORE functions instead of acting as a stand-alone function.

Section 5 – Next Steps

We recommend providing additional enterprise risk management (ERM) resources and references to organizations that need help understanding this function and the value. The CSF appears to assume that all organizations are familiar and have a level of ERM profile that can easily adopt and align the Framework to existing governance and risk management functions and practices.

Appendix A

We recommend the following amendments to further improve this section:

- Current Internal Practices should list existing security controls (e.g., from NIST SP 800-53 Revision 5) that are in place on line 781.
- Target Selected Informative References should list the planned security controls (e.g., from NIST SP 800-53 Revision 5) that need to be included in the action plans to achieve the Target Profile on line 793.

Other Comments

We recommend that lessons learned over the past few years should be incorporated into CSF v2.0 to help readers avoid common mistakes. For example, NIST may have observed that some entities implement "checkbox" approaches to "achieve compliance" with the NIST CSF. These types of efforts may produce the appearance of compliance without satisfying the intent of regulatory requirements.

We also recommend highlighting examples of appropriate ways to implement the CSF in contrast with approaches that typically do not increase cybersecurity maturity. This could include coverage of common pitfalls observed in practice, such as introductory material that emphasizes the message that that CSF subcategories should be considered an "alternative set of controls" that assessors can checkbox, in lieu of adopting security controls like those in NIST SP 800-53.

***

Thank you for considering our feedback. We look forward to NIST CSF v2.0 and appreciate the increased focus on governance, cybersecurity supply chain risk management, cybersecurity measurement and assessment, and addition of sector-specific guidance via Community Profiles. 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.