KAISER PERMANENTE®

Kaiser Foundation Health Plan
Program Offices

January 19, 2018

National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

Submitted to *cyberframework@nist.gov*

RE: *Framework for Improving Critical Infrastructure Cybersecurity Draft Version 1.1 – Draft 2*

Kaiser Permanente offers the following comments on the *Framework for Improving Critical Infrastructure Cybersecurity Draft Version 1.1 – Draft 2 ("Framework").*

Kaiser Permanente identified these gaps in the previous draft version:

- Clarifications and revisions to cybersecurity measurement language
- Clarification of the use of the Framework to manage cybersecurity within supply chains
- Refinements to better account for authorization, authentication, and identity proofing
- Consideration of coordinated vulnerability disclosure

We also agree the federal alignment section should be removed to make the document industry-agnostic, which is important in wider adoption of the Framework. We appreciate the opportunity to provide our responses to questions in the draft version as outlined below.

Question #1: Do the revisions in Version 1.1 Draft 2 reflect the changes in the current cybersecurity ecosystem (threats, vulnerabilities, risks, practices, technological approaches) including those developments in the Roadmap items?

We agree with the revised scope of the Framework that now includes cyber-physical systems (CPS) and connected devices more generally (including the Internet of Things or IOT) in addition to information technology (IT) and industrial control systems (ICS). However, that change is not uniform throughout. For example, Section 1.2 and Appendix A still refer to IT and ICS only and do not include CPS and IOT. Also, Operational Technology (OT) is not included in the scope or the Appendix B: Glossary (Glossary). NIST should refer to the Framework Core as *Core***,** consistently throughout the document, as it did with Tiers and Profiles.

Kaiser Permanente welcomes the clarification of Tiers in Section 2.2, specially, the following excellent explanation of the Tiers and impact of Profiles:

> Tiers do not necessarily represent maturity levels. Tiers are meant to support organizational decision making about how to manage cybersecurity risk, as well as which dimensions of the organization are higher priority and should receive additional resources…. Successful

implementation of the Framework is based upon achieving the outcomes described in the organization's Target Profile(s) and not upon Tier determination.

We support NIST's expansion of the *External Participation* discussion topics within the Tiers, particularly as it relates to the management of cybersecurity within the supply chain. Section 3.0 contains an implied definition of dependencies among systems in the discussion of compensating and common controls. However, there may be broader or more global explanation of dependents and dependencies, and if so the Framework should include definitions of those terms in the Glossary.

Protecting individual privacy and civil liberties was discussed at length at the NIST Cybersecurity Framework Workshops, but developing the appropriate methodology to achieve that goal appears to be a work in progress. Keeping *Privacy Engineering* (formerly *Technical Privacy Standards*) on the Roadmap signals that this is an area of on-going development, alignment, and collaboration. Kaiser Permanente recommends the Roadmap incorporate *NIST SP 800-122 – Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* to help frame the appropriate protections.

We also welcome the addition of the Cyber-Attack Lifecycle, Measuring Cybersecurity and Referencing Techniques sections in the Roadmap. The Department of Homeland Security (DHS) is sponsoring excellent information sharing programs[1]. Those efforts, as well as *NIST SP 800-150 – Guide to Cyber Threat Information Sharing, ISO/IEC 29147 – Information technology – Security techniques – Vulnerability disclosure* and *ISO/IEC 30111 - Information technology – Security techniques – Vulnerability handling processes* will provide a solid foundation for this work. Expanding the scope of cybersecurity information sharing to address big data analytic techniques will be a key factor, particularly for successfully evaluating vendor products and identifying solutions.

Implementing the online version envisioned in the Roadmap's Referencing Techniques area would help to promote use of the Framework. Developing a standardized anthology and a governance model and collaborating with current Informative Reference document owners to expand mappings and offer them online enhances the Framework's usability and relevance.

A single, authoritative taxonomy of cybersecurity terms is needed. Definitions of cybersecurity event versus cybersecurity incident differ from those *in NIST SP 800-61 Rev 2 – Computer Security Incident Handling Guide* and *NIST IR 7298r2 – Glossary of Key Information Security Terms*. NIST should reconcile these definitions, consistent with other NIST special publications. Moreover, for the Framework, NIST should clarify differences between cybersecurity incident and cybersecurity event prior to the discussion of the Core Functions. Unless the reader is referred to Glossary, it will not be clear why the text has changed from "event" to "incident" in the discussion of the Core Functions, and why events are relevant for Core Functions **Identify**, **Protect**, and **Detect**, and the term incident is applicable for **Respond** and **Recover.**

NIST introduces some new terms in this update to the Framework that are missing from the Glossary, including "Technology Supplier," and "OT" as it pertains to Subcategories of the Core. We would

[1] https://www.dhs.gov/topic/cybersecurity-information-sharing

recommend that NIST provide clarity either by adding these terms to the Glossary (e.g., Technology Supplier) and/or within the text (e.g., Operational Technology (OT)).[2]

Table 1 of Appendix A: Framework Core provides informative references, many of which have been updated. The sources of the informative references are provided at the end of the table, as well as in Appendix C: Acronyms; two acronyms, CIS (Center for Internet Security) and CSC (Critical Security Controls), are missing and should be added in Appendix A.

Question #2: For those using Version 1.0, would the proposed changes affect their current use of the Framework? If so, how?

Kaiser Permanente has no concerns with how the proposed changes would affect our current implementation of the Version 1.0 Framework. We view these changes as an evolution of the Framework. Our approach would be to start with this document, then tailor the Framework for our organizational needs. Thus, the minimal number of changes and the type of changes introduced will not alter our use of the Framework as a starting point and reference.

Currently, Kaiser Permanente maps the Framework to information security controls that are based on NIST SP 800-53 Revision 4, The Framework allows Kaiser Permanente to leverage industry standard terminology for metrics and measurements, which is a significant enabler for continuous monitoring. The proposed changes are viewed as a positive addition, with one of the most useful effects likely being an enhancement of Kaiser Permanente's current use of the Framework to more strongly address supply chain management.

Question #3: For those not currently using Version 1.0, would the proposed changes affect their decision about using the Framework? If so, how?

Kaiser Permanente does not offer a response on this question as a current user of the Framework.

We appreciate your willingness to consider our comments, and applaud NIST's role as a convener of the public-private partnership. Please contact me at (510)-271-5639 (email: jamie.ferguson@kp.org) or Beth Pumo at (303) 246-8258 (email: beth.pumo@kp.org) with any questions or concerns.

Sincerely,

JAFerg

Jamie Ferguson
Vice President
Health IT Strategy and Policy

[2] We also note that OT is not included in the updated scope statement in Section 1.0 Framework Introduction (lines 184-185). If included, that would impact other statements that reference the updated scope (e.g. Section 1.2 and Appendix A as stated earlier).