From: Lori Potter
Date: Wed, Apr 5, 2017 at 4:24 PM
Subject: KP Comments Re: Framework for Improving Critical Infrastructure Cybersecurity Draft Version 1.1
To: cyberframework@nist.gov
Cc: Jamie Ferguson, Beth Pumo

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

Thank you for the opportunity to provide feedback.

Lori Potter
Senior Counsel
Kaiser Foundation Health Plan, Inc,
Government Relations Department
One Kaiser Plaza, 27L
Oakland, CA 94612

[Attachment Copied Below]

Kaiser Foundation Health Plan
Program Offices

April 5, 2017

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*

Kaiser Permanente offers the following comments on the *Framework for Improving Critical Infrastructure Cybersecurity Draft Version 1.1 ("Draft Framework").* We appreciate the opportunity to provide our responses to questions in the draft version.

Our review of the Draft Framework identified these critical updates:

- Cybersecurity Measurement and Metrics
- Framework use for third parties through Supply Chain Risk Management
- Identity refinements for authentication, authorization, and identity proofing
- Additional language for the integration of the draft Framework Version 1.1 within organizational risk management programs

Question #1: Are there any topics not addressed in the draft Framework Version 1.1 that could be added in the final?

Kaiser Permanente did not identify any additional topics to be addressed**,** but we offer these general comments

The Draft Framework provides a basis for measurement and an overview of practices, process, metrics, management and technical considerations. Even an organization with a mature integrated risk management program can benefit from continued analysis and evolution of these processes. This is essential to predict operational, financial, and system level risks.

The overarching objective of a cybersecurity program is the security triad: confidentiality, integrity, and availability ("CIA"). However, metrics also can apply to an organization's broader mission and goals. A well-designed cybersecurity program can support business functions and growth. Easy authentication can attract new customers; federation capabilities can reduce cost of operations directly; and in cases where customers care about security, data protection can be an attractive incentive. However, it is important to balance measurements appropriately and we are concerned about the use of metrics primarily to derive cost-based outcomes. Cost-driven measures, unless well-designed, may end up favoring financial impacts over security content.

The Draft Framework can apply to systems engineering processes, deployment, and ongoing operations; we recommend developing a stronger correlation of the systems engineering with a software development life cycle ("SDLC") to facilitate adoption of the Draft Framework by organizations more familiar with other frameworks. Leveraging NIST SP 800-160 (*Systems Security*

Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems) more directly would be beneficial. Lastly, the section on privacy and civil liberties addresses concerns and confusion identified during NIST's 2016 workshop.

Question#2: How do the changes made in the draft Version 1.1 impact the cybersecurity ecosystem?

Kaiser Permanente has no comment at this time.

Question #3: For those using Version 1.0, would the proposed changes impact your current use of the Framework? If so, how?

Proposed changes focus on information sharing practices (*Cybersecurity Measurement and Metrics* section), but Kaiser Permanente is already engaged with industry partners on collaboration and information sharing. We do not anticipate any impact on our current use of the Draft Framework.

As we commented previously, Kaiser Permanente has not used the Framework Implementation Tiers explicitly. However, we support incorporating the cyber supply chain into risk management needs, and generally agree with proposed related tier definitions. For Tier 4, we recommend that the Supply Chain Risk Management include a dedicated, structured process to on-board and/or manage suppliers, partners, and individual organizational buyers, based on risk assessment, requirements criteria, mapping, identified gaps, and current remediation status. This dedicated process should feed into the overall risk management dashboard.

Kaiser Permanente also has not implemented the Framework Profiles. However, we have established baselines for gap analysis. We recommend incorporating guidance into Section 3.4 (*Buying Decisions*) to help organizations compare which products under evaluation meet their target profiles with the resulting gaps outlined. This guidance could include a quick design exercise to remediate gaps and identify where to implement security controls in the operating environment.

Question #4: For those not currently using Version 1.0, does the draft Version 1.1 affect your decision to use the Framework? If so, how?

N/A. Kaiser Permanente previously responded as a user of the NIST Framework and as a stakeholder organization that encompasses health plans, hospitals, ambulatory services (pharmacies, labs, etc.) and physician groups.

Question #5: Does this proposed update adequately reflect advances made in the Roadmap areas?

Proposed updates largely reflect advances made in the Roadmap area. See our response to Question 7 (*below*) for further recommendations.

Question #6: Is there a better label than "version 1.1" for this update?

Kaiser Permanente does not have a recommendation.

Question #7: Based on this update, activities in Roadmap areas, and activities in the cybersecurity ecosystem, are there additional areas that should be added to the Roadmap? Are there any areas that should be removed from the Roadmap?

We have not identified additional areas to be included in the Roadmap. However, Kaiser Permanente recommends expanding the content in several areas.
We recommend minor modifications of the five Draft Framework Core Functions (including *Table 2: Function and Category Unique Identifiers*) be to achieve a more comprehensive framework:

- Expand either "Respond" or "Protect" to include a deterrence function

    - Per the updated framework v1.1, "The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event.". Deterrence activities have become a necessity to 'limit…the impact of a cybersecurity event'. Deterrence may include but not be limited to all activities that discourage attacks against an organization such as offensively capable security solutions and legal repercussions to the attackers.

- Expand "Recover" to "Recover and Evolve" or "Recover and Mature"

    - While "improvements" is listed in both the Respond and Recover functions as an implied technical maturation, it is not sufficient to limit maturation as a sub-component within multiple functions. Striving to continually advance the level of maturity needs to be a continual focus of all cybersecurity programs; therefore it makes sense to expand the Recover function to include maturation. This also highlights the nature of any cybersecurity program as a cyclical, living effort which must adapt or it will quickly become obsolete.

We also recommend that NIST should provide opportunities to comment about leveraging cybersecurity risk information in other risk disciplines, and how to simplify the process, as valuable additions to the Draft Framework Implementation Tiers definition.

We recommend that the Risk Management Process should explicitly identify technical gaps, mitigation/control recommendations, and business risk as defined by the organization's risk assessment and risk tolerance. The statement under Section 3.2 – Step 1 "Implementation Tiers may be used to express varying risk tolerances" should be moved to Section 2.2. Although the measures and metrics provided can help to initiate strategy and planning activities, additional examples of cybersecurity and business risk would be useful for managing the actual organizational process.

We appreciate your willingness to consider our comments. Please contact me with any questions or concerns.

Sincerely,

Jamie Ferguson
Vice President
Health IT Strategy and Policy