KAISER PERMANENTE®

Kaiser Foundation Health Plan
Program Offices

February 9, 2016

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

Submitted to *cyberframework@nist.gov*

RE: *Views on the Framework for Improving Critical Infrastructure Cybersecurity*

Kaiser Permanente offers the following comments on the *Framework for Improving Critical Infrastructure Cybersecurity.* We appreciate the opportunity to provide our feedback in the form of responses to questions in the RFI.

USE OF THE FRAMEWORK

Question #1: Describe your organization and its interest in the Framework.

The Kaiser Permanente (KP) Medical Care Program is the largest private integrated healthcare delivery system in the U.S., with 10.2 million members in eight states and the District of Columbia.[1] KP has implemented a secure Electronic Health Record ("EHR") system, KP HealthConnect®, to support the delivery of healthcare services to our members and to enhance communications among providers. KP is interested in the NIST Cybersecurity Framework as a common vocabulary and set of activities for organizing operations and resources to manage cybersecurity risk.

Question#2: Indicate whether you are responding as a Framework user/non-user, subject matter expert, or whether you represent multiple organizations that are or are not using the Framework.

The KP team is responding 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.

[1] Kaiser Permanente comprises Kaiser Foundation Health Plan, Inc., the nation's largest not-for-profit health plan, and its health plan subsidiaries outside California and Hawaii; the not-for-profit Kaiser Foundation Hospitals, which operates 38 hospitals and over 600 other clinical facilities; and the Permanente Medical Groups, which contract with Kaiser Foundation Health Plan to provide or arrange for health care services for Kaiser Permanente's members.

One Kaiser Plaza
Oakland, CA 94612

Question #3: If your organization uses the Framework, how do you use it? (e.g., internal management and communications, vendor management, C-suite communication).

C-level executives utilize the Framework as a principle-based way of thinking about information systems architecture and cybersecurity risk within KP. Mid-level leaders have a practical view of the Framework and use these principles, coupled with other security control structures and standards, such as HITRUST, SANS and ISO to implement specific security controls.

Question #4: What has been your organization's experience utilizing specific portions of the Framework (e.g., Core, Profile, Implementation Tiers, and Privacy Methodology)?

Within KP, Framework Core is the most widely used portion.

Question #5: What portions of the Framework are most useful?

Specifically, the Core is most useful.

Question #6: What portions of the Framework are least useful?

Because we implement the components of other methodologies such as TOGAF[2], we find the other components of the Framework besides the Core less useful.

Question #7: Has your organization's use of the Framework been limited in any way? If so, what is limiting your use of the Framework (e.g., sector circumstance, organizational factors, Framework features, lack of awareness)?

Across the operational areas where the Framework applies (e.g., the KP Technology Risk Office and the Chief Technology Office), it is well understood.

Question #8: To what extent do you believe the Framework has helped reduce your cybersecurity risk? Please cite the metrics you use to track such reductions, if any.

Attribution is difficult due to the many and complex security controls. However, the Framework reinforces our organizational position regarding industry collaboration: indicator sharing, authentication and trust, conformity, data analytics, and the training/education of a cybersecurity workforce.

Question #9: What steps should be taken to "prevent duplication of regulatory processes and prevent conflict with or superseding of regulatory requirements, mandatory standards, and related processes" as required by the Cybersecurity Enhancement Act of 2014?

Voluntary use of the NIST Framework provides organizations with the flexibility to help reduce or prevent duplication. Thus, we look to NIST to use its framework and associated guidance to promote harmonizing security requirements among regulators.

---

[2] The Open Group Architecture Forum

POSSIBLE FRAMEWORK UPDATES

Question #10: Should the Framework be updated? Why or why not?
We have no recommendations at this time.

Question #11: What portions of the Framework (if any) should be changed, or removed? What elements (if any) should be added to the Framework? Please be as specific as possible.

We recommend providing high-level success measurements/metrics for the Core elements to accelerate adoption and support executive reporting.

Question #12: Are there additions, updates or changes to the Framework's references to cybersecurity standards, guidelines, and practices that should be considered for the update to the Framework?

PCI deserves further study, as do aspects of data classification and encryption.

Question #13: Are there approaches undertaken by organizations – including those documented in sector-wide implementation guides – that could help other sectors or organizations if they were incorporated into the Framework?

We have no recommendations at this time.

Question #14: Should developments made in the nine areas identified by NIST in its Framework-related "Roadmap" be used to inform any updates to the Framework? If so, how?

Inclusion of the privacy engineering objectives from NISTIR 8062 – DRAFT Privacy Risk Management for Federal Information Systems should be considered.

Question #15: What is the best way to update the Framework while minimizing disruption for those currently using the Framework?

We recommend utilizing the current methodology for industry collaboration and updating other NIST Special Publications.

SHARING OF INFORMATION

Question #16: Has information that has been shared by NIST or others affected your use [of] the Framework? If so, please describe briefly what those resources are and what the effect has been on your use of the Framework. What resources, if any, have been most useful?

The many NIST Special Publications and NISTIR documents are extremely valuable in supporting design of security program deliverables.

Question #17: What, if anything, is inhibiting the sharing of best practices?

NIST is universally collaborative with industry and government security initiatives.

Question #18: What steps could the U.S. government take to increase sharing of best practices?

We recommend continuing to support the ISACs and US-CERT.

Question #19: What kind of program would help increase the likelihood that organizations would share information about their experiences, or the depth and breadth of information sharing (e.g., peer-recognition, trade association, consortia, and federal agency)?

We suggest developing an industry consortium that includes representatives from a cross-section of stakeholders that handle sensitive data or operate critical infrastructure systems to meet annually.

PRIVATE SECTOR INVOLVEMENT

Question #20: What should be the private sector's involvement in the future governance of the Framework?

The private sector should continue to support industry/USG collaboration as structured today.

Question #21: Should NIST consider transitioning some or even all of the Framework's coordination to another organization

No.

The remaining questions (#22 - #25) are not applicable.

We appreciate your willingness to consider our comments. 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,

Jamie Ferguson
Vice President
Health IT Strategy and Policy