Cybersecurity Framework Feedback: What We Heard and Next Steps

National Institute of Standards and Technology

June 9, 2016

1. Background

The importance of informed and more capable cybersecurity risk management continues to grow for all organizations. In accordance with President Obama's Executive Order 13636, the National Institute of Standards and Technology (NIST) utilized a year-long consultative process with stakeholders to create the Framework for Improving Critical Infrastructure Cybersecurity (the Framework). Released in February 2014, the Framework consists of a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks.

In December 2015, carrying out its role as further defined in the Cybersecurity Enhancement Act of 2014, NIST issued a request for information (RFI). This RFI solicited feedback regarding Cybersecurity Framework use, how best practices for using the Framework are shared, the possible need for an update of the Framework, and options for its long-term governance. NIST received and analyzed 105 responses. In addition, NIST held a workshop in Gaithersburg, MD, on April 6-7, 2016, to encourage additional feedback from stakeholders on the Framework, including case studies, best practice sharing, analysis of items from the *NIST Roadmap for Improving Critical Infrastructure Cybersecurity*, and the Framework's further development. Approximately 800 individuals from across the country and around the world participated in the workshop both in person at the NIST Gaithersburg, Maryland campus and via webcast.

This document highlights the most prevalent themes and findings from the December 2015 request for information (RFI), Views on the Framework for Improving Critical Infrastructure Cybersecurity, which were validated by the workshop participants. It summarizes areas of agreement as well as issues in which there is a diversity of opinion or a lack of solid information. Based on feedback provided, this document also describes NIST's plans and recommended private sector actions to bring about more effective near-term and long-term use of the Framework.

2. Cybersecurity Framework Use

RFI respondents and workshop participants provided insight on their use of the Framework or use by others that they observed. The results indicate use of the Framework across a variety of industries and organizations. The Framework has been implemented by businesses of all sizes. Respondents represented numerous critical infrastructure sectors, including energy, chemical, finance, healthcare, manufacturing, public safety, communications, and information technology. Among respondents associated with the Federal Government, the Framework was identified as either an internal tool, used in addition to the NIST Risk Management Framework (RMF) to help mitigate risks associated with Federal information systems, or a method of communicating risk posture for Federal Information Security Management Act (FISMA) reporting.

There was general agreement among users that the Framework has proven to be a useful tool for coordinating cybersecurity at a high level. Both RFI respondents and Workshop attendees cited the use of the Framework as an organization and system level tool. Respondents also noted increasing use of the Framework as an assessment methodology both within the organization and among third party assessment organizations. The Framework was also identified as useful in communicating cybersecurity requirements with vendors, service providers, and partners.

RFI respondents and workshop participants provided suggestions about improving the usability of the Framework. They expressed a need for clarity regarding the relationship between the Cybersecurity Framework and the NIST RMF. Respondents and workshop participants also identified a need for additional guidance to operationalize the Framework and suggested that sample Profiles and case studies may be a good starting point for doing that. Many also felt that an ongoing ecosystem to facilitate sharing of practices and lessons learned would improve guidance and promote Framework use.

3. Evolution and Maintenance

Future evolution and maintenance of the Framework was a key topic in the RFI and the recent Workshop, with near unanimous feedback from RFI and Workshop participants. NIST was encouraged to maintain a significant presence in the Framework's governance for the foreseeable future. NIST received positive feedback for the way that it has collaborated with private sector during the development of the Framework, and private sector clearly indicated that this role should continue. A majority of participants suggested that it may be too early in the Framework's evolution for a different governance structure to be considered. In the event of increased private sector leadership of the Framework, private sector recommended that NIST still be substantively involved, continuing to guide the discussion.

4. "Best Practice" Sharing

Especially with regard to sharing practices amongst organizations, participants recommended NIST more properly describe "best practice" sharing as "current practice" sharing or simply "practice" sharing. Participants felt the moniker of "best" should be reserved for practices that are measured and adjudicated as truly beyond others in practice. Further, the label of "best" would need to be conferred by an impartial organization, recognized for its cybersecurity expertise.

Assessing and measuring progress and performance using the Framework was identified by respondents as a fundamental component of practice sharing. However, workshop participants suggested that the potential for practice sharing was limited due to the early state of Framework use and the absence of widely accepted assessment methodologies. There was general agreement that it was feasible to share internal assessment processes outside of their respective organizations. Participants identified Profiles, case studies, guides, subcategory examples, sector specific guidance, and Framework ecosystem repositories as the most helpful topics for sharing.

NIST was deemed well positioned to facilitate the sharing of information and current practices on Framework use, and was encouraged to more vigorously raise awareness about current efforts, including the Industry Resources section of the Cybersecurity Framework web pages; many participants at the workshop were unaware of those resources. Participants suggested that NIST continue to hold workshops but focus on information and current practice sharing, eventually including best practice sharing once robust evaluations were available. Additionally, participants supported NIST's management of sharing sites that aggregate and correlate information gathered from Framework users.

Some participants felt that NIST should publish assessment criteria to help evaluate the effectiveness of cybersecurity processes. A potential NIST self-assessment tool modeled after the approach taken by the NIST Baldrige Performance Excellence Program attracted interest, with a few caveats; the use of the self-assessment tool must strictly be voluntary and any form of third-party assessment coupled with public recognition may be prohibitive due to the potential legal, compliance, and cybersecurity impacts.

A general concern reflected by respondents was that publicly sharing current practices might embolden adversaries and provide potential intelligence gathering opportunities for cyber-attack. Some workshop participants felt that providing best practices would put their organization at a competitive disadvantage by increasing liability, specifically regarding customer/vendor non-disclosure agreements, while others reported they had no such concerns. Moreover, several participants expressed concern about performing self-assessments, suggesting that doing so might also raise liability exposure. Others disagreed with this conclusion, so consensus was not reached on the topic.

5. Roadmap for Improving Cybersecurity

In conjunction with the February 2014 release of the Cybersecurity Framework, NIST published the *NIST Roadmap for Improving Critical Infrastructure Cybersecurity* (Roadmap). The Roadmap discusses key areas for development, alignment, and collaboration identified by stakeholders in the NIST Cybersecurity Framework development process. As part of the December 2015 RFI, NIST received and analyzed feedback from stakeholders regarding using the identified areas to inform updates to the Framework. Additionally, NIST held breakout sessions during the April 2016 workshop to further solicit stakeholder input and validate RFI responses.

5.1 Authentication

RFI respondents and workshop participants identified authentication as a major area in need of further development in the Framework. They indicated that significant progress has been made in the area of authentication since February 2014. Participants frequently discussed authentication schemes under development by both federal and private organizations. Some RFI respondents and workshop participants expressed concern regarding private sectors' involvement in authentication methodologies, highlighting a preference for public and nonprofit development groups or steering committees. Participants generally felt that the Framework Core could be updated to include authentication, with many singling out the Protect Function specifically.

5.2 Automated Indicator Sharing

NIST received RFI responses about threat information from two key groups of respondents. Those include vendors specialized in aggregating and distributing threat information, as well as end-point organizations that identify and use threat information. Workshop participants mirrored RFI commenters request for additional guidance in the Framework document about applying the outputs of threat table top exercises and automated indicators from cyber threat intelligence feeds. Participants expressed support for current threat standardization models (STIX, TAXII, and CybOX). Participants also felt the level of manual processing associated with developing, sorting, and implementing automated threat indicators is still too high.

5.3 Assessment and Confidence Mechanisms

Workshop attendees echoed RFI responses that called for NIST to develop assessment guidance for the Framework (see the discussion above regarding a potential voluntary NIST self-assessment tool based on the Baldrige approach). The notion of industry Framework certifications was also discussed as a potential confidence mechanism. Additionally, workshop participants and RFI respondents expressed interest in using the Framework as a method of translating assessment results across sector, regulatory, and geographic environments.

5.4 Cybersecurity Workforce

RFI respondents and Workshop participants identified workforce development as a major issue, and one that requires further guidance in the Framework. They agreed that the Framework should extend guidance for cybersecurity education beyond the practitioner level, across all strata of the organization. The National Initiative for Cybersecurity Education (NICE) National Cybersecurity Workforce Framework was identified by workshop participants and RFI respondents as key guidance for the development of a cybersecurity workforce that should be leveraged by the Framework.

5.5 Federal Alignment

RFI respondents and workshop attendees clearly agreed that clarification of the relationship between the NIST Risk Management Framework (RMF) and the Cybersecurity Framework is needed. Workshop participants identified the *Fiscal Year 2016 CIO FISMA Metrics* as an area of convergence between the Framework and the RMF. Workshop participants also identified the *Department of Defense RMF for Information Technology* and FedRAMP as key approaches for alignment with the Framework. Federal respondents felt that the Fiscal Year 2016 CIO FISMA Metrics reporting requirements, organized by the Framework Core Functions, facilitated a streamlined view. In general, participants found that the Framework fit at upper echelons of the organization and that the Framework was not granular enough to be the only framework or standard in use.

5.6 International Aspects, Impacts, and Alignment

Many RFI respondents and workshop participants felt that facilitating international adoption of the Framework was important and identified multiple international organizations that have implemented the Framework. The respondents were largely supportive of NIST maintaining some facet of control over the Framework as it moves into the international sphere, adding that NIST's international outreach should continue. RFI respondents and workshop participants also felt that harmonization of international standards was among the most effective methods of promoting international adoption. There was, however, general concern that, unless carefully addressed, incorporation of privacy and civil liberties guidance in the Framework may hinder international adoption, as international requirements for privacy and civil liberties often differ from those in the United States.

5.7 Supply Chain Risk Management

RFI respondents and workshop participants identified supply chain risk management as a critical area of inclusion for the Framework. Many commented that in order to facilitate supply chain security, the Framework should expand upon its common lexicon of standards and practices. This expansion should consider the differing approaches of various sectors to supply chain risk management. Respondents felt that guidance for acquisitions was an area of improvement for the Framework specifically concerning supply chain risk management. There was inconclusive debate among workshop participants as to where supply chain guidance should reside within the Framework. Some participants felt that the supply chain risk management topics should be moved into the Framework Core, while others suggested it belonged in an appendix or elsewhere. It was clear that this is an area that demands further consideration for inclusion in future updates.

5.8 Technical Privacy Standards

Workshop participants were generally in agreement that the *Methodology to Protect Privacy and Civil Liberties* presented in the Framework should be expanded to offer more actionable guidance in mitigating the risk to privacy and civil liberties inherent in cybersecurity. Participants identified NIST's ongoing Privacy Engineering efforts as key to building the vocabulary and facilitating discussions pertinent to the Framework effort.

6. Update

The majority of Framework stakeholders that offered views felt that NIST should update the Framework, in some respect, in the near term. Many RFI respondents and workshop participants desired additional guidance on how to implement outcomes and activities outlined in the Framework. These comments focused on Profile development, gap assessment, risk assessment, and Framework implementation assessments. Additionally, many RFI respondents and workshop participants desired examples of use that incorporate Framework Roadmap topics. Many participants advocated for a NIST-sponsored ecosystem to facilitate examples and results sharing between organizations. To alleviate regulatory concerns, participants felt that NIST should facilitate the Framework's role as non-mandatory guidance suitable for enhancing cybersecurity across multiple sectors by mapping various sector regulations to the Framework Core.

RFI respondents and workshop participants commonly expressed concern regarding the Framework Tiers and what they perceived as a lack of clarity about how the tiers should be utilized in following the Framework's approach. NIST was encouraged to explore alternate methods of addressing organizational capability and maturity. RFI respondents and workshop participants also recognized there could be a potential impact to current implementations of the Framework associated with new updates and urged strongly that any updates to the Framework be made mindful of the need to minimize disruption to the ecosystem. This was one of the clearest takeaways from the feedback provided to NIST.

7. Next Steps

The robust feedback provided to NIST by RFI responses and the heavily attended workshop augment over two years of feedback NIST has received on Framework use, best practice, outreach, prospective updates, and governance. This body of feedback is the basis for the following plan.

7.1 NIST Next Steps

NIST is proceeding with a minor update to the Framework. Per feedback from RFI respondents and Workshop participants, NIST will minimize disruption to current Framework users by focusing on clarifying and refining the Framework. Topics under strong consideration for the update include updating the Informative References, clarifying guidance for Implementation Tiers, placement of cyber threat intelligence in the Core, and guidance for applying the Framework for supply chain risk management. NIST will continue collaborative development of the Framework by releasing a draft of the next Framework version for comment in early calendar year 2017. Some suggested refinements to the Framework may occur outside of the Framework document. The Roadmap, Framework frequently asked questions, and a number of work products and publications associated with Framework Roadmap items (see Computer Security Resource Center for examples) are all under consideration as places to enact refinements.

Per RFI and Workshop feedback, NIST will continue its role as convener of Framework stakeholders. Additionally, NIST observes many positive practices in supporting Framework use and sharing “best practices” in sectors and communities. To institutionalize the process of Framework maintenance and evolution, and to highlight positive Framework practices in sectors and communities, NIST will publish a Framework governance methodology as a part of the upcoming minor update. This document will codify basic stakeholder roles in the Framework ecosystem, establish approximate timeframes for future Framework updates, and provide guidance on what constitutes a minor versus a major update. The Framework governance methodology will also help sectors and communities understand how they can support adaptation of Framework for their constituencies, and how those adaptations can help refine future versions of Framework.

NIST has also begun authorship of self-assessment criteria to support organizational understanding of cybersecurity risk management business practices. The Cybersecurity Excellence Builder will provide detailed criteria for an organization to assess its cybersecurity risk management process. It will be based on Framework and key concepts from the Baldrige Performance Excellence Program.

RFI respondents and Workshop participants validated the focus of NIST outreach efforts. NIST will continue to focus on international, small and medium-sized business (SMB), and regulators.

International outreach will focus on multi-national organizations and foreign governments, in particular national cybersecurity guidance organizations with similar charter as NIST. The focus of this outreach will be further alignment around the standardized set of cybersecurity outcomes articulated in Framework. An optimal outcome of these interactions will be national-level endorsement or adaptation of Framework for use within a given nation.

NIST will continue its multi-program approach to SMB outreach. The NIST SMB Outreach Program will provide general cybersecurity awareness and education. Historically, the SMB Outreach Program has provided 20+ regional training seminars each year. The Cybersecurity Framework program will educate SMBs on iterative cybersecurity risk management using Framework. Recognizing RFI feedback on the importance of get-started guides and case studies, the Framework program will also continue cataloging such resources and highlighting those in sessions with SMBs. This education will continue in the form of presentations and meetings with SMB-specific groups, as well as mixed groups (*i.e.*, both small and large business in one venue). NIST will leverage other programs for SMB outreach, such as the NICE Framework, the Hollings Manufacturing Extension Partnership (MEP), and the Baldrige National Performance Excellence Program.

Regulatory dialogs will continue to emphasize the importance of the voluntary nature of Framework. NIST will also convey ways regulators can use Framework as a communication tool to support a healthy regulatory ecosystem.

7.2 Stakeholder Recommended Actions

The Framework ecosystem shows continued signs of health over time. As evidence, Framework stakeholders are expending increasing effort to share Framework information and practices. NIST applauds these activities. Propagation through the broader community magnifies the positives benefits of the Framework. The following activities are recommended for stakeholders:

Customize the Framework for your sector or community. This might involve a) determining parts of the Framework that are more, or less, applicable, and b) suggesting generalized cybersecurity priorities based on your sector or community's needs. Applicability and prioritization are two key properties of a Framework Profile, so you may wish to customize using a Profile. Publication of Profiles is extremely beneficial to the ecosystem, because it helps other organizations accelerate their customization process.

Publish a sector or community Profile or relevant "crosswalk." Mappings of important legislation, regulation, or guidelines to Framework Categories or Subcategories are considered a crosswalk. These artifacts are important, because they are the basis for requirements reconciliation that often precedes prioritization within a Profile.

Advocate for the Framework throughout your sector or community, with related sectors and communities. Whether on a local, national, or international scale, this will help your organization use Framework with other organizations, and it also helps the larger ecosystem. Beyond informal advocacy, hosting Framework informational meetings, workshops, and conferences are great ways to help others understand and refine use of Framework.

Publish "summaries of use" or case studies of your Framework implementation. The entire Framework ecosystem will benefit from your confirmation of Framework use, understanding the ways you customized and are using the Framework, understanding the positive results you are achieving, and areas for improving the Framework.

Share your Framework resources with NIST. The NIST team benefits greatly from understanding resources. NIST may have suggestions for collaborators, (with your permission) will spread the word about your resource, and (if it qualifies) list your resources at our Industry Resources web page.

8. Feedback and Engagement

Thank you for your continued feedback. NIST continuously seeks feedback on topics such as how organizations are using the Framework, specific suggestions for improvement, and possible outreach activities. Please share those comments with NIST at: cyberframework@nist.gov.