Update on the Cybersecurity Framework

5 December 2014

Background

The Framework for Improving Critical Infrastructure Cybersecurity ("The Framework") was issued on February 12, 2014, as directed by President Obama in Executive Order 13636. This voluntary framework – based on existing standards, guidelines, and practices – provides guidance for reducing cybersecurity risk for organizations within critical infrastructure sectors. The Framework was developed in a year-long, collaborative process in which NIST served as a convener for industry, academia, and government stakeholders. This collaboration continues as NIST works with stakeholders from across the country and around the world.

The Framework is designed to be a "living" document that is shaped by user feedback and experiences. To gain insights into these experiences, NIST released a Request for Information[1] (RFI) on August 26, 2014, and held the 6th Cybersecurity Framework Workshop at the University of South Florida in Tampa, Fla., on October 29 and 30, 2014. Responses to the RFI came from industry, academia and government organizations at multiple levels, as well as organizations representing large constituencies and key stakeholders in critical infrastructure sectors. [2]

Building off those RFI responses, the Tampa workshop focused on the use of the Framework by individual organizations of various sizes and business types. Workshop attendees reported on the use of sector-specific guides, tools, products, standards, and services in support of their cybersecurity risk management practices. The Framework's impact on policy, including internationally, was also a key topic throughout the event. The workshop included sessions on authentication, automated indicator sharing, supply chain, conformity assessment, cybersecurity workforce, and privacy.

This update provides a summary of the RFI responses and feedback from the workshop and describes how NIST will support use of the Framework in the future.

General Awareness

Comments received from the RFI and the workshop indicated there is general awareness of the Framework among many major stakeholders in the nation's critical infrastructure. However, throughout the RFI comments and the workshop discussions, there was broad agreement that

[1] RFI - Experience with the Framework for Improving Critical Infrastructure Cybersecurity, August 26, 2014, https://federalregister.gov/a/2014-20315

[2] Comments Received in Response To: Federal Register Notice Developing a Framework To Improve Critical Infrastructure Cybersecurity, October 16, 2014, http://csrc.nist.gov/cyberframework/rfi_comments_10_2014.html

more could and should be done to raise Framework awareness and use by building on both government and industry-led efforts. Many industry participants committed to expanding awareness and understanding of the Framework and how to use it within their respective sectors and communities. This outreach effort would include small- and medium-sized businesses, state and local governments, and international organizations. The following is a representative comment from an information technology sector RFI respondent: "Our experience and interaction with other organizations have shown that the levels of knowledge of the Framework, as well as the process of its adoption, differ very significantly by industry sector and within the individual sectors we have been exposed to. This is understandable given that the process has only started and an initiative of this magnitude may take years to make a significant impact."

Many RFI respondents and workshop participants recommended that "real world" applications and case studies be published to showcase Framework use. Further, suggestions included the use of Web-based resources, including lessons learned and case studies, to help increase Framework awareness and understanding. Participants also recommended sharing more extensive mappings of existing standards and guidelines to the Framework.

Initial Experiences Using the Framework

Organizations are using the Framework in a variety of ways. Many users have found the Framework helpful in raising awareness and communicating with stakeholders within their organization, including executive leadership. The Framework is also improving communications across organizations, allowing cybersecurity expectations to be shared with business partners, suppliers, and among sectors. The Framework core mappings are being used to demonstrate alignment with standards, guidelines, best practices, and, in some cases, to regulatory requirements. The Framework is also being used as a strategic planning tool to assess risks and current practices.

Some organizations used the Framework to benchmark performance; others explicitly avoided applying the Framework in this way. Those who considered benchmarking detrimental were considering its use as a means of comparing *between* organizations. Generally, those who favored use of the Framework for benchmarking were largely focused on measurement *within* their own organization.

Of the three main components of the Framework (the Core, the Profile, and the Implementation Tiers), the tiers appear to be the least-used part of the Framework, likely because of their enterprise-level scope. Many organizations desired additional guidance on the appropriate use of tiers, while some use alternative approaches to self-assessment. There is some evidence that Framework profiles are being adapted by organizations to meet their organizational needs, though such tailoring does not appear to be widespread. A financial sector representative put it this way in response to the RFI: "While the notion of implementation tiers provides for a more flexible approach in the application of the Framework, the lack of practical examples or reference models through sample profiles either at a broad or sector level make it difficult to understand the expectations of external entities such as regulators."

"Getting started" guides as well as case studies or illustrative applications were cited as a means of increasing understanding and helping organizations better manage cybersecurity risk. Several participants envisioned these tools being hosted in a common public repository. NIST was told that reference tools are needed to express the Framework in multiple ways, to understand informative references, and to aid in developing profiles.

Although one of the most well-received aspects of the Framework has been its use as a common language for describing and sharing information and needs about cybersecurity and risk, comments offered during the workshop sessions made it clear that there remains some confusion over terminology that should be addressed in future efforts.

Framework Updates

There was widespread agreement among participants that it is too early to update the Framework and that more time is needed to understand and use the current version. Similarly, it is important for NIST to clarify how to productively use Framework tiers, how the Framework can be a cost-effective tool in addressing cybersecurity risks, and how the Framework's approach to cybersecurity risk management can be integrated with an organization's broader risk management processes, assessments, and decision making.

In the months ahead, NIST will focus on these aspects of the Framework and will consider producing guidance that will help organizations to address these areas. No modifications or new versions of the Framework are anticipated within the next year, although NIST will continue to work on areas singled out by the Roadmap. NIST also will continue to explore options for future governance of the Framework.

Small/Medium-Sized Businesses

Both RFI responses and workshop feedback indicated that closing gaps in cybersecurity risk management identified through the use of the Framework is especially challenging for organizations that do not have existing cybersecurity programs. At the same time, some workshop participants from smaller and medium companies are productively using the Framework to identify and manage their cybersecurity risks. One small rural telephone and Internet provider told participants that his information technology staff was initially concerned that the Framework would be a burden. They weren't engaged, he reported, "Until we realized that we can use the Framework as a way of helping to guide how we do things, rather than as an additional thing to do." He later added, "When we focused it down to one, two or three items we were trying to make some improvements on, with associated references, we found that actually very helpful." Workshop discussions suggested that other organizations might also benefit from such an incremental, iterative application of the Framework.

Some RFI respondents advocated for specific guidance from NIST in this area. For example, one suggested, "NIST and the SSAs [sector specific agencies] should continue efforts to increase awareness of the Cybersecurity Framework especially among small and medium sized owners and operators of energy sector critical infrastructure. These enterprises may have limited resources requiring tailored outreach and guidance activities."

Regulation and Regulatory Concerns

In response to the RFI, one information technology representative stated an issue that remains a concern despite repeated assurances by the Executive Office of the President[3] and multiple federal agencies: "There is concern that regulating agencies or Congress will make the Framework mandatory and turn it into a compliance mechanism."

RFI respondents and workshop participants recommended increased outreach to regulators in order to facilitate a consistent understanding of the Framework, and to reinforce that it is not designed to create additional regulation. Many stressed that the Framework is an organizing construct for aligning and communicating requirements. Further, it was suggested that regulatory agencies could promote use of the Framework by clear statements about the voluntary nature of the document. For example, one cross-sector representative said, "Regulatory agencies and the Federal government need to make it clear that adoption of the NIST Framework will be viewed as a best practice and positive factor, that the Framework will not be utilized as a discoverable during regulatory examinations, that firms who implement the Framework, in good faith, will not be punished for weaknesses identified during vulnerability assessments in their programs."

Guidance and Metrics/Measurability

A common theme heard was the perceived value of additional guidance about how to use the Framework. One healthcare respondent stated: "We have observed that the health sector has become acutely aware of cyber attacks, insider threats, and other malicious activity. However, traditionally, healthcare's focus has been on HIPAA compliance. Compliance, though, does not necessarily mean that information will be kept safe and secure. Accordingly, healthcare providers, other covered entities, and the business associates that do work on behalf of these covered entities, all need practical and detailed guidance on making the transition from 'compliance only' to being secure (in the same sense that other critical infrastructure sectors,

[3] "[T]he Administration has determined that existing regulatory requirements, when complemented with strong voluntary partnerships, are capable of mitigating cyber risks to our critical systems and information." http://www.whitehouse.gov/blog/2014/05/22/assessing-cybersecurity-regulations

such as the chemical, electrical, and financial sectors have adopted and embraced security).” For example, an information technology sector respondent to the RFI recommended that the Framework, “…provide an accelerating set of guidance profiles by implementation tier. Providing such mapping guidance will enable organizations to more easily understand how to achieve the desired end state of cybersecurity.”

Reinforcing the desire for use case examples, a communications sector RFI respondent suggested, “Our members report that there is a disconnect in the area of risk assessment guidance, methods, and tools, especially with respect to using the Framework to integrate cybersecurity into overall budget planning and master planning. Collecting and publicizing case studies for how this is done in other organizations (especially if organized by critical infrastructure sector) would be a powerful outreach tool.”

Some participants expressed concern about the production of standard templates, making the case that each organization needs to go through the process to get the value and context – and that organizations may otherwise lose focus on the larger cybersecurity risk posture and outcomes.

International Aspects, Impacts, and Alignments

Stakeholders have made it clear from the outset that global alignment is important to avoid confusion and duplication of effort – or even conflicting expectations in the global business environment. There was widespread agreement that there still is much more work needed to ensure that the Framework is known and understood overseas. As one information technology sector RFI respondent put it, “Many countries have a ‘wait and see’ attitude about the Framework. While there is genuine interest in what is happening domestically, they would like to see measurable change in both industry and government before committing to something like the Framework as part of their approach to increasing security.”

The importance of international standards organizations and trade associations was widely recognized. One respondent noted, “Perhaps the best way to build on this [international awareness] is to promote the Framework and its application through international organizations. This would include standards development organizations (e.g., ISA, IEC), professional societies such as the Automation Federation and IEEE, and industry trade associations, which typically have multi-national or global companies as members.”

Roadmap

In February 2014, in conjunction with the Framework’s release, NIST published a Roadmap[4] outlining several high-priority areas for development, alignment, and collaboration to improve

[4] http://www.nist.gov/cyberframework/upload/roadmap-021214.pdf

future versions of the Framework. These areas were discussed in the RFI responses. In addition, NIST facilitated working sessions on specific Roadmap areas including Authentication, Automated Indicator Sharing, Supply Chain and Conformity Assessment, Cybersecurity Workforce, Standards Supporting the Framework, and Privacy Methodology during the Tampa workshop.

A summary of themes and comments from the RFI responses and workshop proceedings regarding several of the Roadmap areas is provided below. Some respondents suggested that while these areas should be pursued, some may ultimately not be appropriate for inclusion in a future version of the Framework.

Authentication

Workshop participants agreed that identity management and authentication are important to meeting cybersecurity goals, and suggested that the Framework could provide better coverage of advances in authentication solutions. Authentication was viewed as a high-risk area, but also an area with promising solutions under development to help reduce this risk. Participants identified the need for approaches and solutions that could be tailored to address an individual organization's priorities. NIST supports the development of better identity and authentication solutions through its participation in the National Strategy for Trusted Identities in Cyberspace (NSTIC), as well as its partnership with the Identity Ecosystem Steering Group (IDESG). NSTIC pilots are demonstrating new approaches to identity and authentication online.

Automated Indicator Sharing

Real time indicator sharing was an interest to several RFI respondents and to participants in workshop breakout sessions on automated indicator sharing. Expanding indicator sharing initiatives to include tools and best practices for indicator management was deemed to be equally important. On this topic, participants noted that threat intelligence requires context if it is to be actionable, and that it must be integrated into an organization's workflow and risk management practices. Moreover, the size and sophistication of an organization determined, to a large extent, the threat information that it can use.

Workshop participants pointed out that sharing private sector information with government still has many legal hurdles; many said that navigating the legal issues was more difficult than addressing the technical challenges. For example, an information technology sector RFI respondent suggested that "Automated Indicator Sharing may also emerge as a valuable component for Framework inclusion in the future, but a great deal of work needs to be done outside of the Framework process before this area is sufficiently mature to incorporate elements into the Framework."

Before the workshop, NIST released a draft of Special Publication (SP 800-150), which focuses on cyber threat information sharing. The publication provides guidance on the safe and effective sharing of information in support of cross-organization incident response. Early feedback from the workshop attendees was positive and NIST is considering this feedback along with that received through the formal comment period.

Supply Chain and Conformity Assessment

Supply Chain Risk Management was readily recognized as a complex, broad cybersecurity concern worthy of collective action. However, participants and RFI respondents urged that any efforts to explicitly address supply chain risk in the Framework should recognize the global nature of technology and avoid guidance based on country of origin, which would impede international commerce.

NIST continues to discuss public and private sector conformity assessment needs and activities during industry and federal engagements. There are private sector conformity assessment activities that could, in part, meet the needs of industry demonstrating evidence of conformity to a given Framework profile. At the workshop, NIST speakers reiterated that the agency has no intention of developing a conformity assessment program, and that industry should define how the Framework should be implemented in their organizations based on their overall risk management plans. That approach has generally been well received.

NIST officials suggested that industry first consider the need for “confidence” (i.e., confidence that risk is managed appropriately) prior to considering the need for “conformity”. The need for confidence is a significant driver that determines an appropriate conformity assessment approach. Breakout session participants indicated that they still want and need further clarity around terminology and concepts with respect to compliance, conformance, confidence, and their inter-relationship.

Cybersecurity Workforce

There was strong agreement at the workshop that attracting and retaining a multidisciplinary cybersecurity workforce is critical, but also a general consensus that the cybersecurity workforce is an area more appropriately undertaken outside of Framework improvement efforts. Better connecting educators to industry (the classroom to the job) was deemed critical by breakout session participants. One RFI respondent suggested that a “broad-based campaign involving federal, state, and local governments and multiple sectors of the U.S. economy would spur greater awareness of cyber threats and aggregate demand for market-driven cyber solutions.”

Standards Supporting the Framework

Many participants in the workshop and RFI respondents reinforced the Framework developers’ intention to encourage alignment among standards already in use, particularly those that are developed and accepted internationally. One information technology sector representative “…found the Framework’s direct mapping to ISO/IEC 27001 and NIST SP 800-53 to be particularly helpful. First, the mapping established an immediate linkage between our ongoing risk management and certification efforts. The mapping also continues to provide an extremely helpful example to share with governments outside of the United States that may be considering a national cybersecurity framework. By mapping the Framework's security guidance to an international standard, NIST has demonstrated that national cybersecurity concerns can be addressed in alignment with standards." Another RFI respondent asserted, "The state of the international standards (e.g., ISA/IEC 62443, ISO 27000, etc.) continues to improve and evolve. These developments should be monitored carefully to allow the Framework to be updated if and as required."

Privacy Methodology

The privacy session breakouts focused on whether organizations were implementing the privacy and civil liberties methodology contained within the Framework and any associated benefits or barriers. A number of participants noted that their organizations already had robust privacy compliance programs, but they were often not integrated with the cybersecurity teams, making it more challenging for organizations to distinguish between security risks and privacy risks arising out of how they are conducting cybersecurity measures. NIST is developing a risk management approach for privacy within the federal government to facilitate better identification of privacy risk in information systems. Eventually, this work could enable organizations to make more purposeful decisions about resource allocation and to implement more effective controls to mitigate privacy risks.

Next Steps

NIST will continue to increase efforts to raise awareness of the Framework, including through partnerships with other organizations. These efforts will be conducted in the same open and collaborative manner in which the Framework was developed. One priority will be to develop and disseminate information and training materials that advance use of the Framework, such as actual or exemplary illustrations of how organizations of varying sizes, types, and cybersecurity capabilities can practically employ the Framework to make themselves more secure.

In addition, NIST will develop material on aligning the Framework with business processes, including integrating cybersecurity risk management with broader enterprise risk management. NIST will explore options for hosting publicly-available Framework reference materials and will continue to hold workshops, webinars, and similar meetings on the Framework to bring in additional stakeholders.

Feedback and Engagement

Feedback – including how organizations are using the Framework, specific suggestions for improvement, and possible outreach activities – can be shared with NIST at: cyberframework@nist.gov.