Update on the Development of the Cybersecurity Framework

January 15, 2014

Under Executive Order 13636, Improving Critical Infrastructure Cybersecurity, the National Institute of Standards and Technology (NIST) is responsible for leading the development of a voluntary framework – based on existing standards, guidelines, and practices – for reducing cybersecurity risk to critical infrastructure.

NIST has been developing the Framework by collaborating extensively with critical infrastructure owners and operators, industry leaders, government partners, and other stakeholders. The process has included a public request for information and five NIST workshops as well as numerous meetings, webinars, and informal sessions to gather feedback. The goal of these interactions has been not only to receive input and feedback on the approach for developing the Framework, but also for drafting, shaping, and revising initial versions of the Framework and supporting material.

Based on these engagements, on October 29 a preliminary version of the Framework was published for formal comment, with a Note to Reviewers that highlighted key issues identified throughout the process.[1] That comment period formally closed on December 13th. A total of 202 submissions were received from a diverse group of stakeholders, reflecting nearly 2,500 separate comments. All submissions have been posted for public review.[2]

Based on NIST's analysis, many themes emerged from the comments received. These include—but are not limited to:

- *Privacy and Civil Liberties.* Stakeholders have consistently identified incorporating privacy needs as an important consideration for the Framework. NIST believes that the separate methodology for privacy and civil liberties found in Appendix B did not generate sufficient support through the comments to be included in the final Framework. While stakeholders have said they see the value of guidance relating to privacy, many comments stated a concern that the methodology did not reflect consensus private sector practices and therefore might limit use of the Framework. Many commenters also stated their belief that privacy considerations should be fully integrated into the Framework Core. Several commenters also expressed support for an alternative methodology proposed by stakeholders and discussed publicly at the 5th NIST Framework Workshop in November.[3]

[1] http://www.nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf

[2] http://csrc.nist.gov/cyberframework/preliminary_framework_comments.html

[3] For the initial submission see: http://csrc.nist.gov/cyberframework/framework_comments/20131205_harriet_pearson_hoganlovells.pdf. A

In response to these concerns, NIST intends to incorporate the alternative methodology into the How To Use section of the final Framework with additional context on privacy derived from comments and public input. This will allow organizations to better incorporate general privacy principles when implementing a cybersecurity program. NIST will continue to consider privacy standards and best practices as an area of focus for future work and in the next version of the Framework.

- *Implementation Needs.* A significant number of commenters stated that the Framework should reinforce throughout the document that it is intended to be voluntary. Similarly, NIST received comments recommending that the Framework state clearly that its focus is on the nation's critical infrastructure, while acknowledging that the document has broader utility and can be helpful to many parts of the economy. While many commenters suggested incorporating the definition of "adoption" previously identified by NIST,[4] this was not an area of consensus as alternative definitions were proposed, and several commenters preferred that detail around adoption be reflected in use of the Framework or in supporting material.

- *Nature and Use of Profiles and Framework Implementation Tiers.* Many commenters requested NIST to clarify or modify the Framework's approach to the concept of profiles and Framework Implementation Tiers. More specifically, commenters requested greater clarification on the purpose and use of the tiers, and on the relationship between and among the Framework core, profiles, and tiers. Some commenters proposed new or revised tier characteristics related to risk management processes, integrated risk management programs, and external participation.

- *Framework Core*. Commenters generally supported the taxonomy of functions, categories, subcategories, and informative references. Some commenters offered recommendations for new or revised categories and subcategories, and suggested additional informative references and mappings. Commenters also asked to ensure that it is clear that the identified informative references are solely intended to provide examples, and are not intended to suggest that organizations are limited in terms of which standards, guidelines, and practices can be used to implement the Framework.

- NIST received a variety of comments recommending expansion of the Framework to include specific types of data – including threat information – that would assist critical infrastructure organizations in using the Framework to develop a cybersecurity program, particularly for small and medium-sized organizations. These comments must be balanced with the ability for the Framework to remain

---

webcast of the privacy panel at the 5th workshop can be found here: http://www.nist.gov/itl/csd/5th-cybersecurity-framework-workshop-november-14-15-2013.cfm

[4] http://www.nist.gov/itl/upload/nist_cybersecurity_framework_update_120413.pdf

relevant across sectors, threat landscapes, infrastructures, and individual organizations that will have evolving needs.

Each comment received by NIST is being considered carefully as revisions are made to the Preliminary Framework to ensure the Final Framework is effective in helping to reduce cybersecurity risk to the Nation's critical infrastructure.

Release of the Final Cybersecurity Framework and Next Steps

Industry stakeholders have volunteered their time and expertise in the Framework development process through participation in the workshops, responding to formal submissions, and other engagements. NIST will continue to support use of the Framework as it is put into practice, ensuring that owners and operators of critical infrastructure can rely on a diverse market of products and services to help meet their cybersecurity needs.

On February 13, 2014, NIST expects to publish the Cybersecurity Framework (Version 1.0).[5] As the Framework has always been intended to be a "living document," there will be a need to update and refine the Framework based on lessons learned through use as well as integration of new standards, guidelines, and practices that become available.

NIST intends to continue to serve as the "convener" until the document can be transitioned to a non-government organization. This will assure that the momentum that has been generated to date will continue, and that the framework advances steadily and addresses key areas that need further development.

Over the past several months, many stakeholders have suggested that it would be beneficial for NIST to develop and share a roadmap and path forward after the February release of the Cybersecurity Framework, building off the "Areas for Improvement" section of the Preliminary Framework. NIST is developing such a roadmap that will include areas for further development and harmonization. These may include: authentication; automated indicator sharing; conformity assessment; cybersecurity workforce; data analytics; international aspects; privacy standards; and supply chain risk management.

Several of these topics may be addressed in focused workshops and meetings over the next several months. More broadly, NIST is considering sponsoring a workshop in the next 4-6 months to review stakeholder experience with Version 1.0, progress with implementing the roadmap, and questions around long-term governance.

[5] The Final Framework will be posted here: http://www.nist.gov/cyberframework