Update on the Development of the Cybersecurity Framework

December 4, 2013

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

NIST is developing the Framework with critical infrastructure owners and operators, industry leaders, and other stakeholders. This engagement includes workshops, meetings, webinars, and informal sessions to gather feedback. To date, workshops were held in Washington, D.C. (April), at Carnegie Mellon University in Pittsburgh (May), at the University of California, San Diego (July), at the University of Texas at Dallas (September), and at North Carolina State University in Raleigh (November).

The goals of the most recent workshop were to receive additional feedback on the preliminary Framework that has been published for public comment and to discuss key aspects of further development that will help inform and guide NIST and the community as the Framework is advanced.

At the workshop, several participants raised the issue of what "adoption" of the Framework means, how it would be gauged, and whether or not specific steps needed to be taken and confirmed in order for an organization to be considered as having adopted the Framework.

Based on the discussion at the workshop, there was general consensus that the organizations were "adopting" the Framework if they were using it as a part of their risk management process, consistent with the following definition:

An organization <u>adopts</u> the framework when it <u>uses</u> the Cybersecurity Framework as a key part of its systematic <u>process</u> for identifying, assessing, prioritizing, and/or communicating:

- *cybersecurity risks,*
- *current approaches and efforts to address those risks, and*
- *steps needed to reduce cybersecurity risks as part of its management of the organization's broader risks and priorities.*

Other key points that were made throughout the workshop include:

- Greater emphasis is needed on the health, safety, and environment aspects of cybersecurity considerations specific to industrial control systems.

- Continued outreach to and engagement with all critical infrastructure sectors is necessary.
- Greater emphasis on the importance of senior leadership engagement in the cybersecurity risk management process is essential.
- It is vital to ensure that the Framework is, and remains, compatible with international standards.
- Increasing emphasis on sector-specific examples of using the Framework – including example profiles – is needed.
- Industry should play a significant role in guiding the future of the Framework.

Small and medium-sized organizations:

- Many – although not all – smaller organizations tend to have special challenges beyond the issue of resources to address cyber security matters. This often includes the lack of formal risk management approaches overall, making cyber risk management more difficult. Participants discussed the need to develop capabilities to enable use of the Framework by smaller organizations that are part of the Critical Infrastructure.
- Participants discussed how small and medium-sized organizations are not inherently insecure. These organizations may have greater cybersecurity capabilities due to reduced complexity and greater management visibility into the business and operational environments, and may operate in a more agile manner that fosters innovation.
- Partnering opportunities with the Department of Homeland Security, the Small Business Administration, sector-sharing organizations (e.g., ISACs) and associations should be explored to raise small and medium-sized organization awareness of the Framework.

Privacy and Civil Liberties:

- The main issue around privacy and civil liberties focused on whether the methodology proposed in Appendix B should focus on aspirational privacy-enhancing outcomes or be more closely tied to current consensus private sector practices.
- There was a lack of consensus around: the level of specificity of the privacy methodology; the question of whether the privacy methodology should remain separate or integrated into the Framework Core; and how best to address issues related to civil liberty protections.

Stakeholders also discussed the importance of a roadmap and path forward after the February release of the Cybersecurity Framework. Such a roadmap is likely to include the following areas for further harmonization and development, as highlighted in the preliminary Framework: authentication; automated indicator sharing; conformity assessment; cybersecurity workforce; data analytics; international aspects; privacy standards; and supply chain risk management.

Participants were asked to weigh in on whether these were the right areas for future work, and to identify others. Such a roadmap will also discuss the continued evolution of the Framework and its eventual transition of ownership to industry.

Next Steps: Stay Engaged

As has been the case from the very first workshop and request for input, the views and suggestions from the latest workshop in Raleigh have been very helpful. Additional feedback is requested. During the open comment period, the public is encouraged to continue to provide input via email at csfcomments@nist.gov by December 13, 2013. All comments will be posted publicly. To review – and comment on –what others have already contributed, consult the comments posted at http://csrc.nist.gov/cyberframework/preliminary_framework_comments.html.

On February 12, 2014, NIST expects to publish the Cybersecurity Framework (Version 1.0) at http://www.nist.gov/itl/cyberframework.cfm.