Update on the Development of the Cybersecurity Framework

July 24, 2013

Under Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, the National Institute of Standards and Technology (NIST) has the responsibility to develop 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 and interested parties. 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), and at the University of California, San Diego (July).

The goals of the most recent workshop were to receive feedback on the draft outline for the preliminary Framework, generate specific content for the Framework, and discuss several topics that will help inform and guide NIST as the Framework is developed.

Based on the feedback provided before and during the San Diego workshop, several points of consensus were identified and reinforced, including:

- The Cybersecurity Framework needs to be scalable, actionable, threat-informed, and risk-based. The intent is to allow companies and other organizations to assess their own risk in order to make cost-effective cybersecurity risk management decisions.
- The Cybersecurity Framework needs to be informative, not prescriptive; it must have sufficient detail to be both actionable and flexible in implementation.
- The Cybersecurity Framework needs to acknowledge that cybersecurity risk management must incorporate people, process, and technology considerations.
- The proposed Cybersecurity Framework structure – functions, categories, subcategories, and informative references – was supported by many participants. Participants used the proposed structure to suggest categories, subcategories and informative references. NIST is analyzing those inputs to present in the draft Preliminary Framework.
- Participants generally supported the proposed functions— *Know*, *Prevent*, *Detect*, *Respond*, and *Recover* — and suggested refinements to the terms and their definitions. As a result of stakeholder input, NIST is revising the proposed functions to *Identify*, *Protect*, *Detect*, *Respond*, and *Recover* in the draft Preliminary Framework.
- Many participants observed that the order of the proposed functions appeared to be presented in a way that implied that they were to be addressed sequentially. It was widely agreed that organizing and presenting these functions to reflect the importance of implementing a dynamic, continuous improvement process needs emphasis.

- The Framework Implementation Levels (FILs) – which were proposed in the draft outline – can serve as an indicator of an organization's implementation of the Cybersecurity Framework, as well as an indicator of how an organization is managing risk. Concern was expressed that the FILs would not reflect many organizations' structures, particularly those typically found in small businesses.

Additionally, several sessions examined special topics in more detail. Key points made by participants included:

- Small Business Applicability session:
  - Characteristics recommended by the Framework should not introduce costly burdens on small businesses. The Framework should not be prescriptive; instead, it should provide guidance for implementing security commensurate with risk.
- Executive Engagement session:
  - Significant government outreach to CEOs is critical. A marketing and communications strategy that promotes a broader understanding of cybersecurity risk to critical infrastructure is essential.
- International Context session:
  - NIST should encourage and actively seek input from international participants. NIST should utilize a variety of outreach mechanisms, including the 4th Framework workshop, to ensure greater awareness of and standards harmonization with the Cybersecurity Framework.
- Awareness and Training session:
  - Awareness and training, tailored to the organization, is essential to effective implementation of the Framework.
- Privacy session:
  - The identification of common privacy standards and practices continues to be a gap area. NIST should conduct targeted outreach to the privacy community.

Next Steps

In August 2013, NIST expects to publish the Draft Preliminary Cybersecurity Framework for stakeholder review and input at http://www.nist.gov/itl/cyberframework.cfm. Posted materials will include revisions and suggestions proposed before and during the San Diego workshop.

NIST will host the 4th Cybersecurity Framework workshop at the University of Texas at Dallas on September 11-13, 2013. This workshop will focus on the August draft and several special topics to be announced. All organizations and individuals interested in the Cybersecurity Framework are asked to review the posted materials prior to the workshop. Those participating in Dallas should come prepared to offer substantive, specific input on these materials including: the level of guidance needed, integration with existing standards, practices, and guidelines, and gap areas. Those not attending the workshop are encouraged to provide their input via email at cyberframework@nist.gov.

After the workshop and other comments are analyzed and incorporated as appropriate, NIST will publish the Preliminary Framework for formal public comment on October 10, 2013.

Stay Engaged

All organizations and individuals have an opportunity to be part of the process and contribute to the development of the Cybersecurity Framework. Please send us your notes, observations, suggestions, and other information to cyberframework@nist.gov.

To review what some others have already contributed, consult the Analysis and Responses section at http://www.nist.gov/itl/cyberframework.cfm.

Register for the 4th Cybersecurity Framework Workshop at http://www.nist.gov/itl/csd/4th-cybersecurity-framework-workshop.cfm.