Update on the Development of the Cybersecurity Framework

June 18, 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 cyber risks to critical infrastructure.

NIST began the development of the Cybersecurity Framework by issuing a Request for Information (RFI) in February to gather relevant input from industry, academia, and other stakeholders. In addition to analyzing the comments, NIST has begun a series of workshops and events to ensure that the breadth of necessary considerations is included during the development of the Framework. An initial session was held on April 3rd at the Department of Commerce to prioritize issues to be addressed as part of the Framework.

At the end of May, a second workshop at Carnegie Mellon University brought together a broad cross-section of participants representing critical infrastructure owners and operators, industry associations, standards developing organizations, individual companies, and government agencies. This 3-day working session was designed to identify and achieve consensus on cross-sector standards, guidelines, and practices that will be used in the Framework.

Based on the responses to the RFI, conclusions from the workshops, and NIST analysis, the preliminary Framework will have the elements below.

- The Cybersecurity Framework will identify effective existing practices to inform an organization's risk management decisions related to the prevention and detection of, response to, and recovery from cybersecurity issues.

- The Cybersecurity Framework will provide a modular and flexible approach to enable organizations to relate cybersecurity needs to diverse sector and organization business drivers, and to be scalable and useful to organizations of varying sizes, business needs, and levels of maturity.

- The Cybersecurity Framework will reinforce cybersecurity risk management as it relates to the enterprise risk management processes of an organization. This includes the importance of senior leadership's engagement in the cybersecurity risk management process, the definition and expression of accountability and responsibility, and the fusion of threat and vulnerability information with potential impact to business needs and operational capabilities.

- The Cybersecurity Framework will provide a means for an organization to express the maturity of their cybersecurity risk management practices to illustrate how those practices are integrated into the overall management processes of the organization.

- Workforce considerations will be included in the development of the Cybersecurity Framework. As a foundation, all users, including employees, partners, and customers, have a need for general cybersecurity awareness. Additionally, the cybersecurity workforce must be trained and must maintain the skills necessary to understand the operating environment, the threats and vulnerabilities to that environment, and the practices available to combat those threats and vulnerabilities.

- The Cybersecurity Framework will address the need for organizations to manage the various types of dependencies, including those related to providers, processes, and technologies. More specifically, it is essential to identify and analyze the criticality of cross-sector and supply chain dependencies and the critical components for which failure would hurt the organization's ability to provide essential services.

In several areas, NIST is seeking more information, including in the identification and availability of foundational cybersecurity practices, the actionable expression and management of privacy and civil liberties needs, and the availability of outcome-oriented metrics that leaders can use in evaluating the position and progress of the organization's cybersecurity status. Better information is also needed on mechanisms to enable critical dependency analysis for supply chains based on mission/business function.

Next Steps

In June 2013, NIST expects to post an outline of the preliminary Cybersecurity Framework, including identified existing standards and practices, for stakeholder review and input. Materials will be posted at http://www.nist.gov/itl/cyberframework.cfm.

The third Cybersecurity Framework workshop will be held from July 10-12, 2013 in San Diego, California. All organizations and individuals interested in the Cybersecurity Framework are asked to review the posted materials prior to the workshop. Those participating in San Diego 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 gaps – especially those cited above. Those not attending the workshop are encouraged to provide their input via email.

NIST expects the outputs of this third workshop will include an initial draft of the preliminary Cybersecurity Framework and a corresponding list of standards, guidelines, and practices that are currently being used by industry. This version of the Framework will continue to be expanded and refined through stakeholder engagement in preparation for a fourth Workshop in September 2013.

Stay Engaged

All organizations comprising the nation's critical infrastructure have an opportunity to be part of the process and contribute to the development of the Cybersecurity Framework.

Please send us your notes, continued observations, further suggestions, and other applicable information at cyberframework@nist.gov.

To gain context as to what others have already contributed, consult the Analysis and Responses at http://www.nist.gov/itl/cyberframework.cfm.

Register for the 3rd Cybersecurity Framework Workshop at http://www.nist.gov/itl/csd/3rd-cybersecurity-framework-workshop-july-10-12-2013-san-diego-ca.cfm.