Update on the Cybersecurity Framework

July 31, 2014

The Framework for Improving Critical Infrastructure Cybersecurity ("The Framework") was issued on February 12, 2014, as directed by the President in Executive Order 13636. This voluntary framework – based on existing standards, guidelines, and practices – provides guidance for reducing cybersecurity risk for organizations within the critical infrastructure. The Framework was developed in a yearlong process where NIST served as a convener for industry, academia and government stakeholders.

During the stakeholder engagement, areas were identified that would require additional development – where the needs of Critical Infrastructure owners and operators extend beyond those existing standards, guidelines, and practices. The Framework was also envisioned as a "living" document, improved based on feedback from users' experiences, while new standards, guidelines, and technology would assist with implementation and future versions of the Framework.

This update highlights new developments and activities over the past several months. In addition to the information presented in this update, NIST is planning to release a formal Request for Information (RFI) asking for further feedback on current awareness, initial experiences with the Framework, and related activities to support the use of the Framework.

Responses to the RFI will be shared publicly, and used as the basis for the next Cybersecurity Framework workshop to be hosted by the Florida Center for Cybersecurity (FC^2) located at the University of South Florida in Tampa on October 29-30. To obtain more information on this workshop and to register, visit the workshop page.

Raising Awareness, Encouraging Use, and Gaining Feedback About Experiences with the Framework

Since the release of the Framework, NIST has strengthened its collaboration with critical infrastructure owners and operators, industry leaders, government partners, and other stakeholders, building on interactions over the previous year that were critical to the Framework's development. The primary goals of these interactions have been to:

1) Raise awareness about the Framework and its intent, explaining the approach and details.
2) Encourage use of the Framework by organizations across the critical infrastructure, and those that support critical infrastructure.

3) Assist sectors developing sector-specific implementation guides with their government partners.

4) Gain feedback from users about their experiences with the Framework; including information about how the approach is helping them to better assess and address their needs, *and* challenges and shortcomings that they identify as they apply the Framework that need to be addressed in future versions or through supporting initiatives.

5) Get input and assistance in further advancing Framework areas for development, alignment, and collaboration identified previously by NIST in its Roadmap for Improving Critical Infrastructure Cybersecurity ("the Roadmap").

NIST, the Department of Homeland Security (DHS), and other government and industry partners have been seeking to accomplish the goals above by meeting frequently with stakeholders across the spectrum of critical infrastructure sectors. This has included discussions with regulatory agencies, targeted sessions on the needs for small and medium organizations, broader industry-led fora, and meetings hosted by the DHS C^3 Voluntary Program.

These interactions have often taken place through meetings and listening sessions at events convened by associations at a state, regional, or national level. Those exchanges will continue throughout 2014 to ensure awareness of the voluntary approach so that officials at all levels of these organizations, including senior executives are informed about and encouraged to use the Framework, participate in supporting initiatives, and then provide feedback to NIST.

The ecosystem of tools and guidance to assist use also continues to evolve. Several industry sectors, standards bodies, and complementary resource providers have taken the initiative to begin mapping their own sets of standards, guidelines, and best practices to the Cybersecurity Framework. Providers of IT products or services are also crucial in constructing, improving, and safeguarding the nation's critical infrastructure from cyberattacks. Their use of the Framework will be essential as the marketplace becomes more focused on, and capable of, dealing with cyber-based risks, and several organizations have announced that they are offering products and services that help organizations implement the Framework.

NIST recently released a Cybersecurity Framework Reference Tool to assist in navigating the Framework and its standards, guidelines, and best practices. This publicly available tool allows the user to browse the Framework Core by functions, categories, subcategories, and informative references; search for specific words; and export the data to various file types.

Advancing Areas Identified in the Cybersecurity Framework Roadmap.

In February 2014, NIST also published a Cybersecurity Framework Roadmap detailing several high-priority areas for development, alignment and collaboration that should be addressed in order to improve future versions of the Framework.

These important areas, identified by stakeholders, require continued focus; they are important areas that either have yet to be developed or may need further research and understanding. The following section highlights recent activities to advance these areas.

Authentication. NIST has continued to support the development of better identity and authentication solutions through the National Strategy for Trusted Identities in Cyberspace (NSTIC), as well as an active partnership with the Identity Ecosystem Steering Group (IDESG). NSTIC pilots are demonstrating new approaches to identity and authentication online. The IDESG in April agreed on a series of components for the Identity Ecosystem Framework and is currently crafting these components in anticipation of launching a self-assessment and self-attestation program early in 2015 with a more comprehensive program the following year.

Automated Indicator Sharing. NIST is currently developing a draft Special Publication (SP 800-150) that focuses on information sharing and coordination within the incident response life cycle. The publication will provide guidance on the safe and effective sharing of information in support of cross-organization incident response. The publication will address the steps for planning, implementing, and maintaining an information-sharing program; information sharing architectures; existing standards, specifications, and transport protocols; the types of information that could be shared (e.g., indicators, tactics, mitigations); and data handling considerations. A draft release of the publication is planned for Fall 2014.

Conformity Assessment. 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. There are public sector activities that could also be used by industry to demonstrate evidence of conformity to a given Framework profile. Efforts will be undertaken in both the private and public sectors to determine if drivers currently exist, or will exist, to require such demonstration.

Cybersecurity Workforce. A skilled cybersecurity workforce is needed to meet the unique cybersecurity needs of critical infrastructure. Various efforts, including the National Initiative for Cybersecurity Education (NICE), are currently fostering the training of a cybersecurity workforce for the future, establishing an operational, sustainable and continually improving cybersecurity education program to provide a pipeline of skilled workers for the private sector and government.

NICE is aligned with the Presidential Job-Driven Training Initiative and will contribute to this new effort by working to increase the number of individuals who complete high-quality cybersecurity training and education programs and attain skills that are in high demand in the national workforce. NICE aims to expand pathways to cyber skills and jobs by developing an interactive map of the United States that shows where cybersecurity job openings exist while identifying for applicants the skills the job requires and the training programs available to applicants seeking each job. NICE will also expand its active engagement with

employers, academic institutions, and industry to promote cybersecurity education and training programs and opportunities at colleges and universities (particularly community colleges), technical schools, and accredited two-year proprietary schools.

Data Analytics. Big data and the associated analytic tools coupled with the emergence of cloud, mobile, and social computing offer opportunities to process and analyze structured and unstructured cybersecurity-relevant data. NIST continues to explore issues in processing and analyzing big data, with an emerging focus on standards and measurement tools and techniques needed to enable greater understanding of complex infrastructures.

Federal Agency Cybersecurity Alignment. Along with DHS, NIST is developing a mapping of key federal policies and resources to the Framework to determine areas within the Framework that could inform efforts to improve Federal cybersecurity practices. This effort is intended to produce a document describing how existing laws, policies, and standards applicable to Federal agency cybersecurity operations align to the Cybersecurity Framework.

International Aspects, Impacts, and Alignment. NIST has also been actively engaging the international community on the Framework. NIST and other US government officials have had discussions about the Framework with multiple foreign governments and regional representatives including organizations throughout the world, including – but not limited to - the United Kingdom (UK), Japan, Korea, Estonia, Israel, Germany, and Australia.

Supply Chain Risk Management. Supply chain issues were among the most commonly mentioned concerns throughout the development of the Framework. NIST will continue to encourage broad industry involvement and leadership in supply chain risk management activities, promote the mapping of relevant standards, best practices and guidelines to the Framework Core, and identify key challenges and strategies to supply chain risk management to enable more effective Framework implementation. Additionally, NIST will continue to support and offer SCRM guidance to federal agencies. NIST recently released the second public draft of Special Publication 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, and is adjudicating comments received.

Technical Privacy Standards. A lack of clear standards, guidelines, and best practices to aid organizations in successfully implementing privacy considerations into their cybersecurity programs was identified during development of the Framework. Consequently, Version 1.0 of the Framework provided a methodology for addressing privacy. At the same time, NIST announced that it intended to convene experts in privacy policies, programs, and engineering to advance understanding of how these areas intersect and to develop practical approaches for building privacy considerations.

NIST held a workshop on Privacy Engineering on April 9-10 2014, to solicit information and views to achieve that aim. Approximately 240 specialists in the legal, policy, and technical aspects of privacy participated in the workshop at NIST and another 100 attended via webcasts of plenary sessions. The attendees included

representatives from a varied array of companies, associations, civil societies, government agencies, and universities. The broad participation across sectors and disciplines illustrated both the complexity of the issue, and the demand for determining common goals. An initial summary of this workshop is available here.

On September 15-16, 2014, NIST will hold its second Privacy Engineering Workshop in San Jose, CA. Co-sponsored with International Association of Privacy Professionals (IAPP), this workshop will consider draft privacy engineering definitions and concepts. The results of this workshop will inform the development of the NIST report on privacy engineering. More information on this workshop is available here.

Stay Engaged

Those with feedback about the Framework – including how they are using it, their experiences, concerns, and specific suggestions for improvement – are encouraged to share them with NIST at: cyberframework@nist.gov.