Inside NIST's Final Cybersecurity Framework

Law360, New York (February 12, 2014, 11:48 PM ET) –

On Feb. 12, 2014, the National Institute of Standards and Technology released the "Framework for Improving Critical Infrastructure Cybersecurity."[1] The framework results from a year-long process involving an extensive public and private sector collaboration to develop voluntary standards for managing cyber risk to critical infrastructure.

Last February, President Obama, in Executive Order 13636, directed the development of a framework that utilizes existing standards where possible to reduce the risk to critical infrastructure and to improve the sharing of information between the public and private sectors about cyberattacks. The executive order acknowledged that cyberattacks on critical infrastructure — systems and assets that if incapacitated or destroyed, would have a debilitating impact on national security, economic security, or public health, such as transportation, financial services, energy and utilities, government, and the public Internet — were "one of the most serious national security challenges we must confront."

The framework is based in part on hundreds of comments made by stakeholders on a preliminary framework[2] released on Oct. 22, 2013. The final version has emerged to provide a risk-based, cost-effective approach to cybersecurity. In conjunction with the release of the framework, NIST also issued a "Roadmap for Improving Critical Infrastructure Cybersecurity"[3] that outlined a series of next steps to further the cybersecurity of critical infrastructure beyond Version 1.0 of the framework.

The Framework

Borrowing from a variety of existing industry security standards, the framework encourages organizations in the critical infrastructure sector to (1) map out a "current profile" of an organization's cyberattack readiness, (2) pinpoint a "target profile" that reflects its readiness based on an analysis of the likelihood and impact of a cybersecurity event, (3) identify "gaps" between the profiles, and (4) implement an action plan that addresses and eliminates such gaps.

To carry out these objectives, the framework employs a three-level structure consisting of the framework core, the framework profile and the framework implementation tiers. This structure is intended to facilitate the efficient and effective implementation of standards for managing cyber risk to critical infrastructure and to be accessible to senior-level and operations-level personnel alike.

Framework Core

The framework core relies on certain core functions, including (1) identifying and prioritizing organizational systems, assets, data and capabilities that need to be protected, (2) protecting those systems, assets, data and capabilities with appropriate

safeguards to ensure the delivery of critical infrastructure services, (3) detecting a cybersecurity event, (4) responding to that event, and (5) restoring capabilities that may have been impaired by the event.

These core functions are divided into categories, which in turn are divided into subcategories. With each division, the framework's concepts become more concrete. For example, to guide organizations in establishing policies and procedures to identify the occurrence of a cybersecurity event, the "detect" function includes "security continuous monitoring" as a category to assess the monitoring of the organization's information systems and assets for cybersecurity events.

The framework then divides the "security continuous monitoring" category into subcategories, including one for the detection of unauthorized mobile code. For this subcategory, the framework references NIST SP 800-53 Rev. 4 as guidance, an NIST special publication for the computer security community. In this fashion, the framework borrows from existing industry security standards such as NIST, ISA, ISO and COBIT standards to lessen the burdens associated with compliance and avoid a one-size-fits-all approach to cybersecurity. Moreover, by referring to existing industry standards within the framework's three-tiered structure, the framework leverages preferred cybersecurity outcomes with solutions already known to critical infrastructure organizations.

Framework Profile and Use of the Framework Implementation Tiers

The framework profile describes how the framework core may be used by a critical infrastructure organization to create a plan to reduce its cyber risk. The framework's implementation tiers provide a ranking system that assists organizations in assessing the sophistication of their cyber-risk management practices. At the upper end, an organization that engages in a continuous process of improving cyber-risk management and makes managing cyber risk part of its culture is classified as Tier 4. At the lower end, a Tier 1 organization shows a limited awareness of cyber risk and a lack of any formalized cyber-risk management or system for sharing cyber-risk information. Notably, progression to a higher-level tier is encouraged only when doing so would reduce risk and be cost effective.

The framework profile and implementation tiers, when used together, provide an organization with a flexible roadmap to achieve its cybersecurity goals. After considering the framework core functions, an organization will need to compare its current and desired cybersecurity profiles and to create an action plan to eliminate gaps between the two. NIST, however, does not provide industry or sector templates to facilitate an organization's analysis of current and target profiles. Rather, it allows for a high degree of flexibility in self-assessing both.

NIST's Roadmap

The framework is described as a "living document" meant to be updated and improved

in response to industry feedback. Consistent with this approach, NIST released an accompanying "Roadmap for Improving Critical Infrastructure Cybersecurity" that identifies next steps and areas for improvement — namely, international cybersecurity, cybersecurity workforce, data analytics, authentication, federal agency cybersecurity alignment, and supply chain risk management, among others — on which the NIST will continue to seek comment in advance of Version 2.0 of the framework.

The roadmap indicates that NIST will take steps to strengthen awareness and encourage the use of the roadmap. For example, NIST is partnering with the U.S. Department of Homeland Security to further its newly announced Critical Infrastructure Cyber Community C3 Voluntary Program[4] to encourage organizations to use the framework.

The roadmap also states that NIST is considering transitioning long-term responsibility for coordinating the advancement of the framework to a nongovernmental organization.

How the Framework Affects Organizations

The framework outlines cybersecurity issues for use by organizations to improve their policies, procedures and protocols for managing cyber risk, and to develop a governance structure to better respond to cyber incidents. The framework is a good tool for organizations with sophisticated cybersecurity programs in place and organizations that are now only beginning to develop a cybersecurity program. However, the framework will not be the only standard used to address significant and ongoing cyber threats to their critical infrastructure, intellectual property assets, and personal data. For as the framework and roadmap acknowledge, the framework does not address certain critical issues, including personal data privacy best practices and others.

Even though the actions called for in the framework are voluntary, the potential provision of incentives, such as grants, liability protection and others, may place those organizations that do not comply at a competitive disadvantage. Moreover, compliance with the framework ultimately may be viewed as part of a "set of industry standards and best practices" against which an organization's actions may be judged. The potential for either may in effect mandate compliance. These uncertainties may also prompt some form of legislative action.

—By Mauricio F. Paez, Jay Johnson and Bart Green, Jones Day

Mauricio Paez is a partner in Jones Day's New York office. Jay Johnson is of counsel in the firm's Dallas office. Bart Green is an associate in the firm's New York office.

This article is adapted from a prior article published in Law360 on Oct. 23, 2013, titled "Spotlight on the New US Cybersecurity Plan."

affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] Available at: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

[2] Mauricio F. Paez, Jay Johnson, Bart Green, "Spotlight on the New US Cybersecurity Plan," Law360 (Oct. 23, 2013). Available at: http://www.law360.com/articles/482455.

[3] Available at: http://www.nist.gov/cyberframework/upload/roadmap-021214.pdf.

[4] Available at: http://www.dhs.gov/about-critical-infrastructure-cyber-community-c%C2%B3-voluntary-program.