FEBRUARY 20, 2014

LTN
LAW TECHNOLOGY NEWS

An ALM Publication

NIST Debuts Cybersecurity Framework

The U.S. government publishes version 1.0 of its cybersecurity framework targeting critical infrastructure, asking for volunteers.

A year ago, U.S. President Barack Obama directed the development of a voluntary, risk-based cybersecurity framework in his executive order a year ago. On Feb. 12, 2014, the U.S. Department of Commerce's National Institute of Standards and Technology issued a "Framework for Improving Critical Infrastructure Cybersecurity (version 1.0)."

The framework seeks to enable organizations—"regardless of size, degree of cybersecurity risk, or cybersecurity sophistication—to apply the principles and best practices of risk management to improving the security and resilience of critical infrastructure." At its core, it is a cybersecurity risk management tool designed to create a shared vocabulary about cybersecurity and help decision-makers from board rooms to the government better manage cybersecurity risks.

The project took a year of drafting and collaboration between NIST and 3,000+ infrastructure "stakeholders" from the private and public sector, including workshops, meetings and public comments. The end result is a set of industry standards and best practices, in the 39-page and an accompanying roadmap.

The document has three key components: core, profiles and tiers.

- **Core** is a set of cybersecurity activities grouped by five functions: identify, protect, detect, respond and recover. These activities provide a high-level view of an organization's management of cybersecurity risks, and are paired with references to existing standards, guidelines and practices.
- **Profiles** are intended to help organizations 1) align cybersecurity activities with business requirements, risk tolerances and resources, and 2) understand their current cybersecurity posture, assist in prioritization and measure progress.
- **Tiers** help organizations view their approach and processes for managing cybersecurity risks. The tiers range from partial (Tier 1) to adaptive (Tier 4), describing an increasing degree of rigor in risk management practices, the degree to which cybersecurity risk management is informed by business needs and integration into the organization's overall risk management practices.

Alexander Southwell of Gibson Dunn & Crutcher

Stephenie Gosnell Handler of Gibson Dunn & Crutcher

CHANGES

A preliminary framework was released in Oct. 2013; two changes are worth highlighting:

Privacy: The most notable change in the final iteration affects its approach to privacy protections. The preliminary framework included a standalone appendix on privacy. Responding to feedback criticizing the privacy section as too prescriptive and costly to implement, the appendix was removed.

Instead, privacy needs have been integrated throughout the document, and specifically into the Core, as sets of processes and activities that should be "considered." While the framework's approach to privacy and civil liberties concerns is not as robust as the preliminary drafts, NIST remains focused on the topic and it is likely that future versions will contain revisions addressing protection of privacy and civil liberties. NIST has announced that it will host a privacy workshop in the second quarter of 2014 as part of its continuing efforts.

Roadmap: The "NIST Roadmap for Improving Critical Infrastructure Cybersecurity" also released on Feb. 14, 2014, is a companion to the framework. It lays out a path toward future revisions, and identifies key areas for cybersecurity development, alignment and collaboration. Some of the areas that

NIST will focus on include the development of better identity and authentication technologies, automated indicator sharing, conformity assessments, data analytics and the cybersecurity workforce. NIST states that it will continue to oversee further development of the framework, at least through the second version.

A VOLUNTARY TOOL

President Obama made clear in last year's executive order that the framework is a voluntary tool, a position that has been reaffirmed by the executive branch. The language in the document stipulates that it is a voluntary resource. However, while there may not be a specific statutory or regulatory requirement to implement the framework, there are several reasons why organizations may find it prudent to adopt the protocol.

First, while the current administration has emphasized that it does not seek to expand regulation, it has also stated that it is working to streamline existing regulations where possible, and to bring those regulations into alignment with the framework. See "Background Briefing on the Launch of the Cybersecurity Framework," (Feb. 12, 2013).

Executive agencies tasked with regulating critical infrastructure sectors are being encouraged to focus on voluntary efforts and programs that support adoption of the framework. Where regulations currently exist, the current administration is supporting efforts to "harmonize and align" current regulations with the framework. Depending on the sector, some organizations may find that adoption of the framework facilitates regulatory compliance. Yet, some organizations may find that existing regulations are more specific than the guidance provided in the framework, such as the Federal Energy Regulatory Commission's reliability standards that apply to bulk power systems, such as electric utilities, in the energy sector.

Second, the Obama administration is in the process of developing incentives that will encourage use of the framework. These are expected to be publicly released over the next few months, and may prove an effective mechanism for encouraging the adoption of the framework.

Finally, the framework's standards and guidelines may effectively establish a baseline cybersecurity risk management approach for organizations in the critical infrastructure sectors, regardless of whether these organizations adopt the framework. The framework may become the minimum standard of care relating to cybersecurity risk.

Therefore, organizations that do not adopt the framework (or have an equivalent risk management approach) could potentially face tort liability for any losses suffered as a result of cybersecurity threats. It is possible that organizations may face heightened regulatory scrutiny if they do not meet the framework's standard of care.

Conversely, organizations that suffer a cybersecurity incident that have adopted the framework may find that fact an important defense if it is viewed as the appropriate baseline standard of care.

The framework is targeted specifically at organizations in the 16 designated "critical infrastructure sectors," (according to the framework, that includes "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on cybersecurity, national economic security, national public health or safety, or any combination of those matters.") However, the administration has taken an expansive view in identifying such infrastructures. Organizations that are not in a sector traditionally associated with national security (for example, retail facilities) may still fall under one of the critical infrastructure sectors, and should carefully consider implementation.

ACTIONS TO CONSIDER

- Conduct a thorough review of the Framework and identify how the Framework could complement existing cybersecurity risk management practices. This review should include input from technical experts, key leadership and legal counsel, and should evaluate the Framework from a strategic, organizational risk management perspective that focuses on potential liability. The Framework is intended to be a flexible tool, and if it is determined that implementing the Framework is in an organization's best interests, it will require a thoughtful approach, again, with input from technical experts, key leadership and legal counsel, in order to tailor it to the unique cybersecurity risks, resources and constraints faced by an organization. Organizations considering establishing or improving their cybersecurity risk management programs can review the steps outlined in the Framework to assist in this process.
- Sign up for the Department of Homeland Security's new public-private partnership, the "Critical Infrastructure Cyber Community Voluntary Program. It seeks to support the critical infrastructure industry in increasing cyber resilience, increase awareness and use of the framework, and encourage organizations to view cybersecurity risk as part of their risk management. The program provides assistanc, tools and resources to participants implementing the framework, and will also support Cyber Resilience Reviews--assessments to evaluate an organization's IT resilience, and can help companies' analysis of current cybersecurity risk management practices and compare them to the principles of the framework.
- Participate in the forums that NIST is expected to establish in the coming months to further refine and improve this cybersecurity risk management tool. Currently, NIST intends to hold at least one workshop within the next six months.

NIST has made clear that the framework is only a first step in a continuous process to improve cybersecurity--it will be updated as appropriate based on changes in technology, threats and other factors, as well as to incorporate lessons learned from its use

Alexander Southwell *is co-chair of Gibson Dunn & Crutcher's information technology and data privacy practice group;* ***Stephenie Gosnell Handler*** *(shandler@gibsondunn.com) is an associate; both are based in New York.* ***Ryan Bergsieker*** *(rbergsieker@gibsondunn.com) of counsel, based in Denver, also contributed to the article.*