VENABLE® LLP

Cybersecurity Alert

February 2014

NIST Releases Framework for Improving Critical Infrastructure Cybersecurity

AUTHORS

Michael J. Baader
Jamie Barnett, Rear Admiral (Ret.)
Stuart P. Ingis
Dismas Locaria
Anthony J. Rosso
Brian M. Zimmet
Keir X. Bancroft
Peter S. Frechette
Ariel S. Wolf
Jason R. Wool

RELATED PRACTICES

Communications
Government Contracts

RELATED INDUSTRIES

Cybersecurity
Financial Services
Government Contractors

ARCHIVES

2014 2010 2006
2013 2009 2005
2012 2008 2004
2011 2007

On February 12, 2014, the White House **announced** the release of the final version of the **Framework for Improving Critical Infrastructure Cybersecurity**. The Cybersecurity Framework includes standards and processes for assessing and reducing cyber risks to critical infrastructure, and reflects numerous changes to the **preliminary version** of the Framework that was issued in October 2013. NIST implemented many of these changes in response to comments received regarding the preliminary Framework in written comments and at a November **workshop in Raleigh**. Venable has attended all of NIST's workshops on the Framework and has closely monitored its development into its final form.

There are generally only minor differences between the structure and content of the Framework and its preliminary version. However, one major change is the removal of the preliminary Framework's "Methodology to Protect Privacy and Civil Liberties for a Cybersecurity Program," a separate appendix that listed a number of privacy-oriented controls. Instead, a reformulated methodology was included in the final Framework's body text. (See below for more information on privacy.)

Overview

The centerpiece of the Framework, called the "Framework Core," contains five cybersecurity functions:

- **Identify** – Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
- **Protect** – Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
- **Detect** – Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
- **Respond** – Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
- **Recover** – Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

Each function has multiple categories tied to programmatic activities. Examples of programmatic activities are "Asset Management," "Access Control," and "Detection Processes." The categories are broken down into subcategories that describe the activities that support technical implementation – such as "[a]sset vulnerabilities are identified and documented" and "[o]rganizational information security policy is established."

NIST implemented several minor changes to the subcategories of Framework Core, most notably by removing one that called for the protection of intellectual property and another that stated "Privacy of individuals and personally identifiable information (PII) is protected."

The Framework also presents four "Implementation Tiers" that describe the "degree of rigor and sophistication in cybersecurity risk management practices" as informed by business needs (with "Tier 1 – Partial" being the lowest, moving through "Tier 4 – Adaptive"). The Tiers are based on how entities view their level of cyber risk against processes already in place. The Framework notes that progression to another Tier is "encouraged when it would reduce cybersecurity risk and be cost-effective."

Similarly, the Framework Profile is an expression of the application of the Tiers to the Functions, Categories, and Subcategories of the Framework Core. In keeping with its goal of providing flexibility and scalability, NIST states that entities may choose to implement multiple profiles to fit their needs. Ultimately, the profile is intended both to describe an entity's current state of cybersecurity as well as its desired future state, which can help facilitate gap analyses and the prioritization of risk mitigation

activities.

Finally, the **NIST Roadmap for Improving Critical Infrastructure Cybersecurity** asks for private sector involvement and sets out nine "Areas for Development, Alignment, and Collaboration:"

- Authentication
- Automated Indicator
- Conformity Assessment
- Cybersecurity Workforce
- Data Analysis
- Federal Agency Cybersecurity Alignment
- International Aspects, Impacts, and Alignment
- Supply Chain Risk Management
- Technical Privacy Standards

Privacy

Having removed the privacy appendix featured in the preliminary Framework, NIST instead opted to provide general privacy and civil liberties considerations for entities as they implement a cybersecurity program. The new section, "Methodology to Protect Privacy and Civil Liberties," does not contain controls but rather notes the potential privacy implications of certain activities recommended by the Framework. Whereas the privacy appendix was widely viewed as prescriptive and potentially overreaching, the final Framework notes that "not all activities in a cybersecurity program may give rise to [privacy and civil liberties] considerations" and otherwise carefully avoids any imperative language.

Nonetheless, in the "Roadmap" published on the same day the Framework was issued, NIST lists the development of technical privacy standards as an area for development, alignment, and collaboration. Noting the historical difficulty in achieving consensus on the definition and scope of privacy management, NIST posits that the lack of a common privacy risk management model or privacy standards and supporting metrics makes assessing an entity's privacy practices a difficult undertaking. As a result, NIST announced that it will hold a privacy workshop in the second quarter of 2014 "to focus on the advancement of privacy engineering as the foundation for the identification of technical standards and best practices that could be developed to mitigate the impact of cybersecurity activities on individuals' privacy or civil liberties." No additional details on this workshop have been released to date.

Appeal to Business and International Organizations

The final Cybersecurity Framework more clearly addresses business and international perspectives. For example, the Framework acknowledges that large organizations with varying components may have multiple Cybersecurity Profiles that assess differing degrees of cybersecurity risk across those components. Elsewhere, the Framework details that business needs are among the factors that will drive efforts to address gaps in organizational cybersecurity profiles. Finally, the Framework clarifies that it is not country-specific, and is promulgated to help develop "a common language for international cooperation on infrastructure cybersecurity." This language is intended to attract adoption by businesses by promoting flexibility and demonstrating the utility of the Framework to multi-national organizations.

Incentives

On the same day the Framework was released, the Department of Homeland Security announced the launch of the **Critical Infrastructure Cyber Community (C3) Voluntary Program**, its voluntary program to support the use of, perform outreach and communications on, and serve as a communications channel for the Framework. As expected, the C3 will offer technical assistance to organizations that adopt the Framework. At this time, however, such technical assistance is the only "incentive" being offered by the federal government to promote adoption. As a result, organizations looking for financial or other incentives to formally adopt the Framework must continue to look elsewhere.

Indeed, many observers believe the SAFETY Act, which provides a limitation or elimination of civil liability arising from acts of terrorism, could be harnessed in combination with the Framework. Notably, the **National Cybersecurity and Critical Infrastructure Protection Act of 2013**, a bill recently passed by the House Homeland Security Committee, would amend the SAFETY Act to cover "Qualifying Cyber Incidents" in addition to acts of terror, which would expand the applicability of the Act to cyber incidents even further.

Venable will continue to closely follow NIST's finalization of the Cybersecurity Framework, as well as DHS' implementation of C3. Venable's attorneys are well-positioned to answer any and all questions regarding the Cybersecurity Framework, having participated in and attended all relevant meetings conducted by NIST since the Executive Order was released in February 2013.

* * * * *

Venable LLP offers a broad array of legal services to a variety of different players within the cybersecurity arena. Our attorneys are adept at understanding complex client issues and tapping into the extensive experience of our many practice areas including privacy and data security, e-commerce, intellectual property, government contracting, telecommunications, energy, and corporate.

If you have any questions concerning this alert, please contact any of the authors.