NIST and DHS Release Final Cybersecurity Framework, Roadmap, and Voluntary Program for Cybersecurity Assistance

2014-02-13

Yesterday, the National Institute of Standards and Technology (NIST) released the final version of the voluntary federal cybersecurity standards known as the Cybersecurity Framework, along with a "Roadmap" explaining how the government will work with the private sector, other countries, and international organizations to refine and improve the Framework over the next several years.[1] In conjunction with the issuance of the Framework and the Roadmap, the Department of Homeland Security (DHS) launched a program—called the Critical Infrastructure Cyber Community (C3) Voluntary Program—to assist owners and operators of critical infrastructure systems in using the Framework to improve their network security.[2] These developments come exactly a year after President Obama issued the Executive Order on Improving Critical Infrastructure Cybersecurity that mandated them. [3]

The NIST Framework is designed for owners and operators of critical infrastructure systems, but regulators and courts may well look to the Framework for guidance in assessing the adequacy of the cybersecurity practices of companies and organizations throughout the economy. Thus, every organization that maintains important information on computer systems has an interest in learning about the Framework and determining how it may assist their network security.

The Framework issued yesterday (known as version 1.0) is identical in many respects to the preliminary version issued in October 2013,[4] but several differences are notable:

- In response to industry complaints and counter-proposals, version 1.0 replaces the preliminary version's detailed appendix on privacy protection with a much briefer, less prescriptive set of privacy recommendations;
- A few of the substantive standards in the Framework's Core have been removed, including one on protecting intellectual property, while several have been added, particularly focusing on identification of new risks and on recovery activities;
- The Roadmap provides more specifics than did the equivalent section in the preliminary version about how NIST envisions development of the Framework, particularly
  - a goal of transitioning governance of the Framework to a non-governmental

    organization after the release of version 2.0;
    - several initiatives, including development of NIST special publications, addressing improved, multi-factor authentication methods;
    - several initiatives, including production of NIST special publications, on the application of big data analytic techniques to access controls, continuous monitoring, attack warning and indicators, and security automation;
    - a bigger push for international coordination on cybersecurity standards and best practices; and
    - a call for the development of more precise technical standards and best practices to gauge privacy impacts, beginning with a workshop to be held by NIST in the second quarter of 2014;
- The C^3 Voluntary Program will both provide assistance in using the Framework—through self-assessment materials, on-site evaluations by DHS personnel, and the development of sector-specific implementation guidance—and serve as point of contact for user feedback.

The Cybersecurity Framework is the centerpiece of the efforts required by the Executive Order on Improving Critical Infrastructure Cybersecurity, but the Executive Order and its accompanying Presidential Policy Directive mandate many other initiatives as well, including ones that may ultimately lead to mandatory federal cybersecurity rules. That larger array of initiatives is described systematically in our earlier publication, available here.

Here is a fuller description of the Framework, Roadmap, and C^3 Voluntary Program:

Framework

Version 1.0 maintains the same basic approach—risk management—and the same structure as the preliminary version, with three main components: Core, Implementation Tiers, and Profiles.

The Core consists of key cybersecurity activities, desired outcomes, and applicable technical standards. They are grouped under five basic functions designed to provide company decision-makers with a strategic view of cybersecurity risk management:

> Identify—This function includes asset management and risk assessment, which are “foundational for effective implementation of the Framework.”
>
> Protect—This function includes access control, training, and data security, and is to be implemented consistent with risk strategies from the “identify” function.
>
> Detect—This function includes monitoring and detection processes to enable timely response and containment of cyber incidents.
>
> Respond—This function includes response planning, communication, and mitigation efforts.

Recover—This function includes recovery planning and improvements.

For each function, the preliminary Framework identifies existing technical standards, from NIST and other international standards bodies, to serve as “informative references” in support of the technical implementation of the functions.

The Profiles are intended to help organizations “establish a roadmap” for reducing cybersecurity risks in line with organizational and sector goals, legal requirements, best practices, and risk management priorities. Organizations are encouraged to focus on identifying and eliminating gaps between their current Profile, which describes cybersecurity outcomes currently being achieved, and their target Profile, which indicates the outcomes needed to achieve their cybersecurity risk-management goals.

The Implementation Tiers describe the nature of the organization’s cybersecurity risk management practices, from partial (lowest tier in term of rigor and sophistication) to risk-informed, to repeatable, to adaptive (highest tier in terms of rigor and sophistication). Version 1.0 explicitly notes that, while organizations identified in lower tiers are “encouraged” to consider moving to higher ones, “[t]iers do not represent maturity levels,” and “progression to higher Tiers is encouraged when such a change would reduce cybersecurity risk and be cost effective.” Version 1.0 states that “[s]uccessful implementation of the Framework is based upon achievement of the outcomes described in the organization’s Target Profile(s) and not upon Tier determination.”

Version 1.0’s privacy recommendations allow for considerably more flexibility than those in the preliminary version’s privacy appendix. Version 1.0 characterizes the privacy recommendations as “a general set of considerations and processes” and simply suggests that “organizations may address these considerations and processes with a range of technical implementations.” Version 1.0 provides specific examples of possible means to address these implications for only seven of the 22 categories in the Core: governance, access control, awareness and training, detection, monitoring, communications, and mitigation. Even then, the suggestions are less specific and prescriptive than those in the preliminary version.

Roadmap

The Roadmap, which builds on the “Areas for Improvement” discussion in the preliminary version, addresses nine subjects: (1) authentication; (2) automated indicator sharing; (3) conformity assessment; (4) the cybersecurity workforce; (5) data analytics; (6) federal agency cybersecurity alignment; (7) international aspects, impacts, and alignment; (8) supply chain risk management; and (9) technical privacy standards.[5]

Describing the Framework as a “living document,” the Roadmap identifies for each of these areas specific initiatives NIST intends to undertake to extend and improve the Framework. Many of the most notable of these proposals were noted above, but they all deserve attention because they reflect the considered judgments by a group of government experts, informed by extensive private-sector input, about the most important avenues for improving cybersecurity practices. They thus are likely to reflect and influence efforts outside the government as well as inside, as well as efforts in other countries.

C^3 Voluntary Program

The C^3 Voluntary Program has two basic functions: to assist stakeholders in making use of the Framework and to serve as a venue for ongoing dialogue between the government and stakeholders about how the Framework can be put into practice and improved.

Assistance will be provided in several ways, including through the development by DHS and sector-specific agencies of implementation guidance for particular sectors; through on-site non-technical assessments by DHS personnel in regional offices around the country; and through the provision of materials organizations can use to undertake self-assessments of cybersecurity preparedness.

The launch of this program may be of particular importance for owners and operators of “critical infrastructure at greatest risk,” a category defined in the Executive Order as those “where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security,” but excluding commercial IT products or consumer IT services.[6] The government was to have identified and confidentially notified entities in this category by July 12 of last year, which were then to have an opportunity to challenge the determination. Government agencies have to report to the President annually on the extent of participation by these entities in the Voluntary Program.[7]

[1] The final Cybersecurity Framework (version 1.0) is available here. The Roadmap is available here.

[2] *About the Critical Infrastructure Cyber Community C^3 Voluntary Program*, U.S. Department of Homeland Security, available here. Information about joining the program is available at the “C3 Voluntary Program US-CERT Gateway, here.

[3] Exec. Order No. 13636, Improving Critical Infrastructure Cybersecurity, 78 Fed. Reg. 11738, §7(e) (Feb. 19, 2013), available here.

[4] Our analysis of the preliminary version is available here. Our analysis of the draft version made public in August 2013 can be found here.

[5] This list is intended to meet the requirement of Section 7(b) of the Executive Order to “identify areas for improvement that should be addressed through future collaboration with particular sectors and standards-developing organizations.”

[6] E.O. 13636, § 9.

[7] Id. § 8(c).

Authors

Benjamin A. Powell

PARTNER

Co-Chair, Cybersecurity and Privacy Practice

Co-Chair, Artificial Intelligence Practice

✉ benjamin.powell@wilmerhale.com

☎ +1 202 663 6770

Jamie Gorelick

PARTNER

Chair, Regulatory and Government Affairs Department

✉ jamie.gorelick@wilmerhale.com

☎ +1 202 663 6500

Jason C. Chipman

PARTNER

✉ jason.chipman@wilmerhale.com

☎ +1 202 663 6195

Wilmer Cutler Pickering Hale and Dorr LLP is a Delaware limited liability partnership. WilmerHale principal law offices: 60 State Street, Boston, Massachusetts 02109, +1 617 526 6000; 2100 Pennsylvania Avenue, NW, Washington, DC 20037, +1 202 663 6000. Our United Kingdom office is operated under a separate Delaware limited liability partnership of solicitors and registered foreign lawyers authorized and regulated by the Solicitors Regulation Authority (SRA No. 287488). Our professional rules can be found at www.sra.org.uk/solicitors/code-of-conduct.page. A list of partners and their professional qualifications is available for inspection at our UK office. In Beijing, we are registered to operate as a Foreign Law Firm Representative Office. This material is for general informational purposes only and does not represent our advice as to any particular set of facts; nor does it represent any undertaking to keep recipients advised of all legal developments. Prior results do not guarantee a similar outcome. © 2004-2024 Wilmer Cutler Pickering Hale and Dorr LLP