WILMERHALE

NIST and DoD Issue Cybersecurity Guidance and Rules

2013-10-24

The government promulgated two important cybersecurity documents this week that will be of interest to a wide range of companies that track developments to improve security of critical U.S. computer networks.

First, the National Institute of Standards and Technology ("NIST") issued a preliminary version of voluntary cybersecurity standards, known as the Cybersecurity Framework.[1]NIST was directed to develop the Cybersecurity Framework under the executive order entitled "Improving Critical Infrastructure Cybersecurity" issued by President Obama on February 12, 2013.[2] This preliminary Cybersecurity Framework will be subject to a 45-day public comment period. The publication of this preliminary Framework also starts a 90- day clock for agencies responsible for regulating the security of critical infrastructure to report to the President on whether current regulatory requirements are sufficient in light of cybersecurity risks, whether such agencies have clear authorities to establish requirements based on the Framework to address cyber risks, and whether any additional authority is required to address cyber risks to critical infrastructure.[3] The final version of the Cybersecurity Framework is scheduled to be released in February 2014.[4]

Second, the Department of Defense ("DoD") issued a final rule on the Defense Industrial Base ("DIB") Voluntary Cyber Security and Information Assurance ("CS/IA") program.[5] The DIB program is aimed at providing a framework for the government and certain defense sector companies to voluntarily share cyber threat information.

NIST Preliminary Cybersecurity Framework

In August, NIST released a discussion draft of the preliminary Framework, the general structure of which has been maintained in the version released this week.[6] The preliminary Framework creates voluntary cybersecurity standards for protecting private sector computer networks owned or operated by critical infrastructure entities. The preliminary Framework is divided into three parts: Framework Core, Framework Profile, and Implementation Tiers.

The Framework Core is designed to identify key cybersecurity activities common across all critical

infrastructure networks. These are activities that companies should address when creating programs to protect critical computer systems and that identify best practices for communicating risks throughout an organization. Specifically, the Framework Core consists of five functions designed to provide company decision makers with a strategic view of cybersecurity risk management. These functions are subdivided into categories of outcomes:

- 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 anomalies and events, monitoring, and detection processes to enable timely response and containment of cyber incidents.
- Respond – This function includes response planning, mitigation, and improvements, and is to be performed consistent with the strategies developed under the "identify" function.
- Recover – This function includes recovery planning and communications, intended to support timely recovery after a cyber incident consistent with "strategies developed under the "identify" function.

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

The Framework Profile is intended to help organizations "establish a roadmap" for prioritization of organizational efforts to reduce cybersecurity risks. Organizations are encouraged to focus on identifying and eliminating gaps between the "Current Profile," which identifies cybersecurity outcomes currently being achieved, and the "Target Profile," which indicates the outcomes needed to achieve cybersecurity risk management goals.

The preliminary Framework includes several appendices, including one providing organizations with "methodologies to address privacy and civil liberties considerations around the deployment of cybersecurity activities and in the protection of [personally identifiable information]." An earlier version of the privacy appendix in the discussion draft raised some concerns for possibly going beyond the scope of the Executive Order. The current version of the privacy appendix addresses those concerns by emphasizing more clearly that the provisions are advisory and not mandatory. But critical infrastructure companies should still give close attention to that appendix. The preliminary Framework has added a new "informative references" section to the appendix which, similar to the "informative references" in the Framework Core, provides citations to various standards to support the technical implementation of the methodologies.

DoD Final Rule

The DIB CS/IA program is a voluntary cybersecurity information-sharing program between DoD and eligible DIB companies. The final rule issued this week responds to comments from an interim final

rule published in May 2012, which established the DIB CS/IA program and provided eligibility requirements for participation in the program.

In responding to the comments submitted in response to the interim final rule, DoD made three changes to the interim final rule. Specifically, the final rule adds definitions of "U.S. based"[7] and "U.S. citizen"[8] to the definition sections, and eliminates a statement found in 32 C.F.R. § 236.6(c) allowing the government to "request from any DIB participant additional information or assurances regarding such DIB participant's policies or practices, or the determination by the DIB participation that such policies or practices comply with applicable legal requirements."

Companies wishing to participate in the DIB CS/IA should not only conduct a careful assessment as to whether they meet the eligibility requirements for participation set forth in 32 C.F.R. § 236.7, but should also evaluate what types of information they will share with the government through the program and the underlying legal rationale supporting such information-sharing, as required by the remaining portions of 32 C.F.R. § 236.6(c).

---

[1] The preliminary Cybersecurity Framework is available here. The release of the preliminary Cybersecurity Framework, originally scheduled for October 10, 2013, was delayed due to the recent government shutdown.

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

[3] Exec. Order No. 13636, §10(a).

[4] A description of the executive order and the various tasks it assigned to different Executive Branch agencies can be found here.

[5] 78 Fed. Reg. 62430 (Oct. 22, 2013).

[6] A further discussion on the discussion draft is available here.

[7] The final rule defines "U.S. based" to mean "provisioned, maintained, or operated within the physical boundaries of the United States."

[8] The final rule defines "U.S. citizen" to mean "a person born in the United States or naturalized."

Authors

Benjamin A. Powell

PARTNER

Co-Chair, Cybersecurity and Privacy Practice

Co-Chair, Artificial Intelligence Practice

benjamin.powell@wilmerhale.com

+1 202 663 6770

Jason C. Chipman

PARTNER

jason.chipman@wilmerhale.com

+1 202 663 6195