KING & SPALDING

Client Alert

Privacy & Information Security Practice Group

December 2, 2013

NIST Publishes Draft Cybersecurity Framework For Critical Infrastructure Industries

On October 23, 2013, the National Institute of Standards and Technology (NIST) released a long-anticipated draft of its Cybersecurity Framework. The Framework, as NIST explains, is "not a risk management process itself,"[1] but is intended to provide a common language for addressing cybersecurity risk that can be used by all personnel in critical infrastructure industries from senior executives to frontline IT staff members. "Critical infrastructure" includes organizations in the energy, finance and banking, healthcare, transportation, telecommunications, defense, food and agriculture, water, and utilities sectors.[2] Organizations in such fields (or closely associated with them) should familiarize themselves with the Framework, and may wish to comment on it formally by the end of the public comment period on December 13, 2013.

Background

Executive Order 13636, which President Obama issued in early 2013, recognizes that "[t]he national and economic security of the United States depends on the reliable functioning of the Nation's critical infrastructure in the face of [cyber] threats," and calls for the development of a "Cybersecurity Framework" that provides a "prioritized, flexible, repeatable, performance-based, and cost-effective approach . . . to help owners and operators of critical infrastructure identify, assess, and manage cyber risk."[3] President Obama directed NIST to consult with government agencies, industry stakeholders, and the public before issuing a final Framework by February 2014. Over the past year, as a result, NIST has issued Requests for Information and a preliminary version of the document, as well as held a number of public workshops. The draft Framework marks the last chance for stakeholders to provide comments before the document becomes final.

Structure of the Draft Framework

The draft Framework is composed of four parts: the Framework Core; the Framework Profile; the Framework Implementation Tiers; and the Informative References. The Framework Core divides cybersecurity functions into five broad categories: *Identifying* the risk; *Protecting* against the risk; *Detecting* the risk; *Responding* to an incident; and *Recovering* from the incident. These five high-level functions are then broken down further into

For more information, contact:

J.C. Boggs
+1 202 626 2383
jboggs@kslaw.com

Alexander K. Haas
+1 202 626 5502
ahaas@kslaw.com

John A. Drennan
+1 202 626 9605
jdrennan@kslaw.com

King & Spalding
Washington, D.C.
1700 Pennsylvania Avenue, NW
Washington, D.C. 20006-4707
Tel: +1 202 737 0500
Fax: +1 202 626 3737

www.kslaw.com

multiple Categories and Subcategories that operate at a more granular level. For example, the "Identify" function is associated with the Category "Asset Management," which in turn is associated with the Subcategory "Physical devises within the organization are cataloged." The Informative References provide illustrative methods and "best practices" for accomplishing that action.

The Framework Profile, which provides a picture of an organization's cybersecurity readiness, applies both to the organization's current state and its desired future state. To achieve this, an organization measures its own readiness against each of the Categories, and then determines what level of readiness it believes it should have for those Categories, taking into account factors such as the organization's tolerance for risk. This allows the organization to spot potential "gaps" in its security posture and to track its progress in implementing security protocols. Relatedly, the Framework Implementation Tiers are a yardstick that can be used to measure an organization's cybersecurity readiness. The Tiers, which are ranked 1 (Partial) through 4 (Adaptive), reflect increasing levels of sophistication in the organization's cybersecurity programs.

Significantly, the Framework also contains a privacy appendix,[4] which responds to the Executive Order's direction that the Framework include "methodologies . . . to protect individual privacy and civil liberties."[5] The privacy appendix is intended to protect personally identifiable information (or PII), and is based on the Fair Information Practice Principles (or FIPPS).[6] The appendix generally tracks the organization of the Framework Core, and provides privacy "methodologies" for most of the Categories identified in the Framework Core, as well as an Informative Reference for implementing the methodology. NIST explains that "[a]s organizations review and select relevant categories from the Framework Core, they should review the corresponding category section in the privacy methodology."[7] Many of these privacy methodologies are applicable to *government* information and privacy protections but have never been required of *private* sector stakeholders.

Recommendations

Organizations in, or closely associated with, critical infrastructure industries should take note of the draft Framework and consider providing formal comments, which are due by December 13, 2013. Following a review period, NIST will incorporate changes recommended by stakeholders and release a final version of the Framework in February 2014.

The Framework is potentially significant for several reasons. For one thing, it arguably has the potential to create new bases for legal liability for stakeholders in critical infrastructure sectors. While both the Executive Order and NIST stress that adoption of the Framework is voluntary,[8] government regulators and parties to litigations (or other disputes) often look to industry standards when judging whether a company's conduct was reasonable. Indeed, although the Framework does not contain prescriptive language, it is not hard to envision how the Framework could be viewed as reflecting the standard of care on cybersecurity matters, particularly if the Framework is adopted or implemented widely within a critical infrastructure sector. In this way, the Framework could become a benchmark against which critical infrastructure industries' cybersecurity efforts are judged. For this reason, stakeholders within critical infrastructure sectors should pay particular attention to Executive Branch efforts to encourage adoption or implementation of the Framework. We note, for example, that Section 8 of President Obama's Executive Order calls on the Secretary of Homeland Security and sector-specific agencies to "establish a voluntary program to support the adoption of the Cybersecurity Framework by owners and operators of critical infrastructure and any other interested entities."[9] In this connection, the agencies, in consultation with the Secretary, are required to "coordinate with the Sector Coordinating

Councils to review the Cybersecurity Framework and, if necessary, develop implementation guidance or supplemental materials to address sector-specific risks and operating environments."[10] The nature of such guidance or supplemental materials may well have a bearing on the development of a cybersecurity standard of care within particular critical infrastructure sectors and the expectations of regulators and the public.

At the same time, the Framework does not close the door to new executive regulation of, or new legislation in, this area. Far from it: the Executive Order requires the sector-specific regulatory agencies to work with the Department of Homeland Security, the Office of Management and Budget, and the National Security Staff to review the final Framework and "determine if current cybersecurity regulatory requirements are sufficient given current and projected risks."[11] These agencies must report to the President 90 days after the Framework is published on whether they have the authority to establish mandatory requirements based on the Framework "to sufficiently address" cyber risks to critical infrastructure.[12] This process could result in mandatory cybersecurity requirements and standards.[13]

There are potential carrots as well as sticks. The Executive Order directs the Departments of Homeland Security, Commerce, and Treasury to identify and evaluate positive incentives that could be used to encourage organization to adopt the Framework.[14] In August 2013, the White House released a list of the incentives that are under consideration. These include developing cybersecurity insurance; using voluntary adoption of the Framework as a condition of, or as one of the weighted criteria for, federal critical infrastructure grants; using process preferences (in other words, access preference to government technical assistance in non-emergency situations); liability limitations; streamlining regulations; public recognition; rate recovery for price-regulated industries; and cybersecurity research.[15] Additional incentives are possible. Notably, a Department of Homeland Security official has recently suggested that Congress may need to enact some form of liability protection for critical infrastructure operators to ensure that private sector companies appropriately share information with the government and with one another.[16]

To help clarify how the Framework is intended to function, King & Spalding conducted a webinar in early November. The program addressed Executive Order 13636, the operation and implementation of the draft Framework, recent cybersecurity legislation, and potential paths forward in this area. Readers may wish to listen to the program online or review the accompanying slide deck.

If you have any questions regarding this or related issues, please contact J.C. Boggs at +1 202 626 2383, Alexander Haas at +1 202 626 5502, or John A. Drennan at +1 202 626 9605.

King & Spalding is particularly well equipped to assist clients in the area of privacy and information security law. Our Privacy & Information Security Practice regularly advises clients regarding the myriad statutory and regulatory requirements businesses face when handling personal and other sensitive information in the U.S. and globally. Our Privacy & Information Security Practice regularly advises clients regarding the myriad statutory and regulatory requirements businesses face when handling—either in gathering, managing, securing, transferring, sharing, selling or disposing of—personal and other sensitive information concerning individuals such as employees, consumers, customers, or patients, in the U.S. and globally. Collectively, the members of King & Spalding's Privacy & Information Security Practice have unparalleled experience in areas ranging from providing regulatory compliance advice, to responding to security incidents, interfacing with stakeholders and the government (both federal and state), engaging in complex civil litigation (such as class actions), handling state and federal government investigations and enforcement actions, and advocating on behalf of our clients before the highest levels of state and federal government.

---

[1] The National Institute of Standards and Technology, Cybersecurity Framework [The "Framework"]at 3.
[2] The Executive Order 13636 defines "critical infrastructure" as "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 security, national economic security, national public health or safety, or any combination of those matters." Executive Order No. 13636, 78 Federal Register 11739 (Feb. 19, 2013). Under Presidential Policy Directive 21, "critical infrastructure" includes the following 16 sectors: chemicals; communications; dams; emergency services; financial services; government facilities; commercial facilities; critical manufacturing; defense industrial base; energy; food and agriculture; healthcare and public health; nuclear reactors, materials and waste; water and wastewater systems. *See* Presidential Policy Directive/PPD-21, The White House, Office of the Press Secretary, Critical Infrastructure Security and Resilience (Feb. 12, 2013).
[3] 78 Fed. Reg. 11739, 11741 (Feb. 19, 2013)
[4] Framework at 26.
[5] 78 Fed. Reg. 11739, 11741.
[6] See 78 Fed. Reg. 11739, 11741. The FIPPS are a set of widely recognized principles for addressing the privacy of information about individuals. See . 78 Fed. Reg. 11739, 11743. The Department of Homeland Security recognizes eight such principles: transparency; individual participation; purpose specification; data minimization; use limitation; data quality and integrity; security; and accountability and auditing. *See* Department of Homeland Security, Privacy Policy Guidance Memorandum (2008) (Mem. No. 2008-1), available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf .
information about individuals.
[7] Framework at 2.
[8] 78 Fed.Reg. 11739, 11741. Framework at 1.
[9] 78 Fed.Reg. 11739, 11741.
[10] 78 Fed.Reg. 11739, 11741-11742.
[11] 78 Fed. Reg. 11739, 11742.
[12] Ibid.
[13] 78 Fed. Reg. 11739, 11743.
[14] 78 Fed. Reg. 11739, 11742.
[15] See http://www.whitehouse.gov/blog/2013/08/06/incentives-support-adoption-cybersecurity-framework .
[16] See Audio File at 51:55, Suzanne E. Spaulding, cting Undersecretary for the National Protection and Programs Directorate, Department of Homeland Security, *The Cybersecurity Executive Order and Presidential Directive: What Does Success Look Like?*, available at http://www.brookings.edu/events/2013/11/19-cybersecurity-executive-order.