KING & SPALDING

Client Alert

Privacy & Information Security Practice Group

February 18, 2014

NIST Finalizes Cybersecurity Framework For Critical Infrastructure—Implementation Next On The Agenda

On February 12, 2014, exactly one year to the day on which President Obama tasked the National Institute of Standards and Technology (NIST) with creating a Cybersecurity Framework to help protect critical infrastructure, NIST released the initial version of the final document. It is the culmination of an extensive public-private collaboration during which NIST held five multi-day workshops at locations across the country and collected thousands of stakeholder comments. The Framework implements President Obama's call in Executive Order 13636 for a voluntary risk-based set of industry standards and best practices to help organizations manage cybersecurity risks. Dubbed "Version 1.0" of the NIST Cybersecurity Critical Infrastructure Framework, a copy of the Framework can be found **here.**

On the same day it released the Framework, NIST also released a companion document, the ***Roadmap for Improving Critical Infrastructure Cybersecurity***. The Roadmap addresses "NIST's next steps with the Framework and identifies key areas of development, alignment, and collaboration" for implementing the Framework. Relatedly, on February 12, 2014, the Department of Homeland Security (DHS) also announced that it is launching an new program, the Critical Infrastructure Cyber Community Voluntary Program, or the "**C^3 Voluntary Program.**" The C^3 Voluntary Program is a public-private partnership that seeks to increase awareness and use of the NIST Framework. The C^3 Voluntary Program is intended to connect stakeholders to DHS and other federal government programs to encourage coordination with the government, increase cyber resilience, and assist the stakeholders in managing their cyber risks. Among the benefits that DHS offers to encourage participation are free technical assistance, tools, and resources to strengthen cyber risk management capabilities, a Cyber Resilience Review, and assistance with meeting fiduciary responsibilities to manage cyber risks. More information about the C^3 Voluntary Program can be found **here.**

Whether the Framework achieves the lofty goal of permitting critical infrastructure businesses to "manage cybersecurity risk in a cost-effective way based on business needs without placing additional regulatory requirements on businesses" will be subject to much debate in the coming months and years. But given the breadth of what constitutes "**critical infrastructure**," organizations in diverse fields such as energy, finance and banking, healthcare, transportation, telecommunications, defense, food and

For more information, contact:

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

Phyllis B. Sumner
+1 404 572 4799
psumner@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

Atlanta
1180 Peachtree Street, NE
Atlanta, Georgia 30309-3521
Tel: +1 404 572 4600
Fax: +1 404 572 5100

www.kslaw.com

agriculture, water, and utilities should familiarize themselves with the Framework. Perhaps more important than the Framework itself, however, will be regulatory and industry efforts to implement the Framework. Such efforts will require especially close attention from stakeholders, including companies outside of the critical infrastructure sectors.

Summary of the Final Cybersecurity Framework

The Framework consists of three basic components: the Framework Core; the Framework Profiles; and the Framework Implementation Tiers. The Framework Core is a set of cybersecurity activities and informative references that are common across critical infrastructure sectors. These cybersecurity activities are grouped by five functions – Identify, Protect, Detect, Respond, Recover – that provide a high-level view of an organization's management of cyber risks. The Framework Profiles help to align an organization's cybersecurity activities with its business requirements, risk tolerances, and resources. The Framework Profiles will assist companies to better understand their current cybersecurity state, support prioritization, and measure progress. Finally, the Framework Tiers are a mechanism for organizations to assess their approach and processes for managing cyber risk. The Tiers range from Partial (Tier 1) — the lowest level of cyber resiliency and risk management practices—to Adaptive (Tier 4) and describe an increasing degree of robustness in a company's risk-management practices.

For people who have been watching the Framework's development, perhaps the most striking thing about the final Framework is its similarity to the formal draft that NIST released for comment in October 2013. Our prior summary of these cybersecurity provisions can be found **here**, and we also conducted a **webinar** in early November 2013 to help clarify how the Framework is intended to function. 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. However, the most significant change between the draft and final versions of the Framework is the appendices. The draft Framework included a fairly controversial privacy appendix that sought to meld privacy methodologies based on Fair Information Practice Principles (FIPPS) to cybersecurity methodologies. Industry expressed significant concern over the privacy appendix and the final Framework drops this appendix entirely, although NIST has identified privacy protection as a high-priority action for future discussion.

The Path Forward—NIST's Roadmap & Implementation of the Framework

The release of the Cybersecurity Framework is the start, rather than the completion, of a major push towards greater cybersecurity in U.S. industry. NIST has made clear that it intends the Framework to be a "living document," which will be updated and improved based on industry feedback and implementation. NIST will continue to play a central role and will informally consider comments on the Framework until it issues a formal notice of revision to Version 1.0. After that, the Roadmap notes that NIST will seek input on the long-term governance of the Framework, including transitioning NIST's responsibilities to a non-governmental organization (although no such organization is identified).

Finally, the Roadmap identifies nine "high-priority" areas in which NIST will pursue additional development, industry alignment, and collaboration. These include:

- Authentication – supporting better identity and authentication solutions
- Automated Indicator Sharing – working with public and private stakeholders to fill gaps in existing standards and provide guidance on sharing information about detecting and responding to cybersecurity events as they occur
- Conformity Assessment – leveraging existing programs to ensure that products, services, or systems meet specified requirements for managing cybersecurity risks
- Cybersecurity Workforce – promoting workforce development activities along with other federal agencies and expanding engagement with academia to increase the number of skilled cybersecurity employees
- Data Analytics – improving benchmarking and measurement of big data analytics and supporting international standards bodies

- Federal Agency Cybersecurity Alignment – working with other federal agencies to align the Framework with Federal Information Processing Standards and guidelines and identify gaps where additional guidance may improve the federal government's ability to manage cybersecurity risk
- International Aspects, Impacts, and Alignment – continuing to engage foreign governments and entities to explain the Framework and seek international alignment were possible
- Supply Chain Risk Management – working to increase adoption of supply chain risk management practices and promote greater understanding of supply chain risk
- Technical Privacy Standards – continuing to work towards increased consensus on protecting privacy, including hosting a privacy workshop in the second quarter of 2014

Over and above NIST's future efforts in these areas, the action will shift during the coming year to sector-specific agencies and industry associations as they work on ways to tailor or implement the Framework for specific industries. Section 10 of Executive Order 13636 directs agencies with responsibility over the security of critical infrastructure – including the Departments of Defense, Energy, Health & Human Services, and others – to work with the Secretary of Homeland Security, the Office of Management and Budget, and the National Security Staff to assess current regulatory requirements and provide reports to the President on whether clear authority exists to establish requirements based upon the Framework. Within the next 90 days, these agencies are to propose "prioritized, risk-based, efficient and coordinated actions" in the event that their current regulatory requirements are found to be insufficient to mitigate cyber risk. In addition, Executive Order 13636 encourages independent regulatory agencies to work with the Secretary of Homeland Security to consider additional actions to mitigate cyber risks for **critical infrastructure sectors**.

Discussion

February 12, 2014, was a significant day for several reasons. As we have noted in connection with the draft Framework, the Framework will potentially create new bases for legal liability for stakeholders in critical infrastructure sectors. Government regulators and parties to litigations may look to industry standards when judging whether a company's conduct was reasonable. While the Framework is not prescriptive, private law mechanisms, such as the tort system, could treat the Framework as reflecting the standard of care on cybersecurity. For this reason, stakeholders within **critical infrastructure sectors** should pay particular attention to Executive Branch efforts to encourage adoption or implementation of the Framework. Indeed, implementing the Framework within particular sectors could increase the likelihood that it, or implementation guidance tailored to those sectors, might be viewed as a standard of care by which a company's cybersecurity efforts are to be measured. We will discuss further implications of the Cybersecurity Framework in future client alerts.

The C^3 Voluntary Program is also just the beginning of the Government's efforts to promote cybersecurity efforts and encourage adoption of the Cybersecurity Framework. Other incentives are still under consideration by DHS and the Executive Branch.

The private sector, however, must be cautious of making public assertions concerning cybersecurity and its adoption or use of the Framework to ensure that such statements are accurate. The Federal Trade Commission (FTC) has begun bringing lawsuits against entities related to their cybersecurity policies. We think it is likely that the FTC could insert itself into policing company statements to the public concerning the Framework where there is a possibility of deceptive or misleading statements that are made in violation of the broad strictures of Section 5 of the FTC Act.

If you have any questions regarding this or related issues, please contact J.C. Boggs at +1 202 626 2383, Phyllis Sumner at +1 404 572 4799, 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—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.*

* * *

Celebrating more than 125 years of service, King & Spalding is an international law firm that represents a broad array of clients, including half of the Fortune Global 100, with 800 lawyers in 17 offices in the United States, Europe, the Middle East and Asia. The firm has handled matters in over 160 countries on six continents and is consistently recognized for the results it obtains, uncompromising commitment to quality and dedication to understanding the business and culture of its clients. More information is available at ***www.kslaw.com****.*

This alert provides a general summary of recent legal developments. It is not intended to be and should not be relied upon as legal advice. In some jurisdictions, this may be considered "Attorney Advertising."