KING & SPALDING

Client Alert

Government Advocacy & Public Policy Group

March 15, 2013

NIST Seeks Private Sector Information on Cybersecurity Framework Outlined in President's Executive Order and Notices First Public Meeting

On February 26, 2013, the National Institute of Standards and Technology (NIST) published a Request for Information (RFI) in the *Federal Register* soliciting views from both government and industry on developing the Cybersecurity Framework required by President Obama's recent Executive Order on Cybersecurity. The Framework will consist of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks. NIST's RFI seeks information on these topics in the context of critical infrastructure, which is defined so broadly that it includes not only stakeholders in the defense industrial base but also providers of banking, energy, transport, health, Internet, and, e-commerce services. Private companies in these diverse industries have the unique opportunity to take part in shaping cybersecurity standards prior to the potential implementation of legislatively mandated standards. Stakeholders must act quickly as comments are due by April 5, 2013 and NIST's first meeting and public workshop with critical infrastructure stakeholders will be held April 3, 2013 at NIST's headquarters.

Background on President Obama's Cybersecurity Executive Order

On February 12, 2013, President Obama issued an Executive Order on Cybersecurity seeking to improve the cybersecurity of critical infrastructure across a broad range of industries. Section 7 of the Executive Order requires NIST to lead the creation of a "Cybersecurity Framework" that would include best practices, standards, and technical approach that incorporates "voluntary consensus standards and industry best practices to the fullest extent possible" that would be set forth in a guidance that is technology neutral. The Framework's purpose is to assist owners and operators of critical infrastructure to identify and manage risks posed from cyber threats and that would allow for continued collaboration of products and services to reduce and address cyber risks. Once the Framework is established, the Department of Homeland Security will establish a voluntary program to support adoption of the Framework by owners and operators of critical infrastructure. The President directed NIST to develop the Framework through an "open public review and comment process" with a preliminary framework to be published within 240 days and a final framework within one-year. More information on the Executive Order can be found at this link.

NIST Solicits Views From Critical Infrastructure Stakeholders

NIST's RFI, entitled Developing a Framework To Improve Critical Infrastructure Cybersecurity, seeks information related to the protection of "critical

For more information, contact:

Eleanor Hill
+1 202 626 2955
ehill@kslaw.com

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

Dan Donovan
+1 202 661 7815
ddonovan@kslaw.com

Phyllis Sumner
+1 404 572 4799
psumner@kslaw.com

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

King & Spalding
Atlanta, GA
1180 Peachtree Street, NE
Atlanta, GA 30309-3521
Tel: +1 404 572 4600
Fax: +1 404 572 5100

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

infrastructure" in three areas: (i) current risk management practices within industry; (ii) the use of frameworks, standards, guidelines, and best practices; and (iii) specific industry practices. The RFI defines "critical infrastructure" in accordance with 42 U.S.C. § 5195c(e) to mean "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." Given the breadth of this definition, the RFI seeks comment to create a Cybersecurity Framework that will include voluntary baseline cybersecurity standards and best practices that could cover diverse sectors from energy to pharmaceuticals to agriculture to banking to technology companies and everything in between.

Concerning current risk management practices, NIST's questions focus on risk assessment and how cybersecurity factors into that risk assessment as well as the current usage of various frameworks and standards. In addition, NIST is interested in understanding whether particular frameworks, standards, guidelines, and/or best practices are mandated by legal or regulatory requirements and the challenges organizations perceive in meeting such requirements. Aside from these general risk management questions, the RFI also seeks to understand "the current regulatory and regulatory reporting requirements in the United States (e.g. local, state, national, and other) for organizations relating to cybersecurity" and what occurs where an organization is required to report to more than one regulatory body and what resulting information must be reported under these current regulations. The RFI also solicits stakeholders' opinions on what role national and international standards and organizations developing those standards should "play in critical infrastructure cybersecurity conformity assessment."

NIST's RFI also seeks input on the applicability and usage of existing publications that address cybersecurity needs such as those developed by international standards organizations, federal and state regulators including public utility commissions, as well as industrial organizations, non-profit organizations or other NGOs. Moreover, NIST seeks to identify "core practices that are broadly applicable across sectors and throughout industry." NIST's RFI seeks information concerning the adoption of a particular set of standards, systems, and practices as they pertain to critical infrastructure components, including: (1) Separation of business from operational systems; (2) Use of encryption and key management; (3) Identification and authorization of users accessing systems; (4) Asset identification and management; (5) Monitoring and incident detection tools and capabilities; (6) Incident handling policies and procedures; (7) Mission/system resiliency practices; (8) Security engineering practices; and (9) Privacy and civil liberties protection. NIST has set forth a series of specific questions that seek insight into industry specific practices and the relative significance of the use of those practices, the development and implementation of these practices and allocation of business resources to invest in such standards and practices; how organizations address cybersecurity risks that suddenly increase in severity; and the relationship between cybersecurity standards and privacy and civil liberties interests.

What's Next

Stakeholders must provide comments on the RFI to NIST by 5:00 p.m. EST on April 5, 2012 and can find information about NIST's first public forum for stakeholders on April 3, 2013 here. Although this RFI and the current NIST process focus on developing voluntary baseline standards to improve cybersecurity of critical infrastructure, private sector input in the development of those standards is important. Congressional and Executive branch interest in these issues is increasing, and could generate significant pressure for industry adoption of those voluntary standards. Moreover, if and when there is a congressional effort to establish some level of mandatory standards, it is likely that those would be based to a large degree on the voluntary standards developed by NIST. In any case, once the Framework is established, there will clearly be an increased expectation, including potentially by both governmental authorities and in civil litigation related to cyber incidents, that private sector stakeholders will adopt those standards. The RFI is an important opportunity for stakeholders to have their views considered and, hopefully, adopted as those standards are still being developed.

The RFI may also provide an opportunity to raise private sector concerns about other related, but still unresolved, issues. For example, only congressional action can provide industry with liability protection related to cybersecurity incidents. Without liability protection, industry and critical infrastructure operations face litigation risks, investigations, and other potential harms even with the adoption of voluntary baseline standards or through their sharing of cyber threat information with the government. Similarly, only Congress could ameliorate industry concerns over engaging in collective action that could be viewed as creating friction with prohibitions in Federal antitrust law. Finally, congressional action would be necessary to establish federal baseline standards that would preempt conflicting state requirements (either in legislation or state tort actions) and provide certainty and protection to industry.

On Capitol Hill, House Select Intelligence Committee Chairman Mike Rogers (R-MI) and Ranking Member Dutch Ruppersberger (D-MD) re-introduced their cybersecurity bill which focuses on information sharing, and held a hearing last month to examine cyber threats. H.R. 624 is identical to a bill that passed the House last year but that Senate Democrats criticized, citing privacy concerns and arguing that the bill did not go far enough by prescribing only voluntary measures. Rep. Mike McCaul (R-TX), the new chairman of the House Homeland Security Committee, similarly announced plans to introduce legislation that would "enhance coordination between the private sector and government in order to protect our critical infrastructure." On March 13, the Committee held a hearing focusing on the role of the Department of Homeland Security in cybersecurity. The House Judiciary Committee also held a hearing earlier this week entitled “Investigating and Prosecuting 21st Century Cyberthreats" which featured testimony from the FBI and examined current criminal and data breach laws that help combat cyber intrusions and protect sensitive information. The Committee also considered potential legislative solutions designed to ensure greater security in the private and public sectors. In addition, the Senate Homeland Security and Governmental Affairs Committee held a joint hearing on cybersecurity with the Commerce, Science and Transportation Committee on March 7 to consider legislation that would supplement the President’s Executive Order.

Recommendations

As NIST implements the Executive Order and presses forward with the creation of the Cybersecurity Framework and the 113th Congress reviews multiple cybersecurity proposals, the business community needs to ensure they are in compliance with the Order and that their views and concerns are heard both in NIST’s development of the Framework and in congressional consideration of cybersecurity legislation. King & Spalding has the expertise and experience needed to assist clients in both areas. For the fifth consecutive year, King & Spalding’s government relations practice was recognized by *Chambers USA*: America’s Leading Lawyers for Business, and was selected by *U.S. News and World Report* as the “Law Firm of the Year” for government relations in 2012, based on the positive feedback of clients and peers regarding the firm’s work in this area. King & Spalding has one of the nation’s most active and respected government relations practices and is particularly well-equipped to advise companies on these important data security issues.

If you have any questions regarding NIST RFI or Cybersecurity issues or related issues, please contact Eleanor Hill at +1 202 626 2955, J.C. Boggs at +1 202 626 2383, Dan Donovan at +1 202 661 7815, Phyllis Sumner at +1 404 572 4799 or Alexander Haas at +1 202 626 5502.