KING & SPALDING

Client Alert

Data, Privacy & Security Practice Group

May 22, 2017

President Trump's Executive Order on Cybersecurity

On May 11, 2017, President Trump signed a long-awaited Executive Order[1] that aims to bolster the cybersecurity of federal networks and critical infrastructure. In an effort to fulfill the President's promise to get "tough on cyber," the Order contains three major components:

(1) Protecting cybersecurity of federal networks by mandating adherence to the NIST Framework and by requiring agency heads to prepare a risk management report;

(2) Protecting cybersecurity of critical infrastructure by requiring various agency heads to identify how they can support the cybersecurity efforts of critical infrastructure entities, engage those entities, and prepare a risk management report; and

(3) Promoting cybersecurity workforce development and defending against international cybersecurity threats, by requiring agency heads to assess the sufficiency of efforts in this area and prepare risk management and other reports.

The Order does not currently impose obligations on private entities, but the risk management reports required by the Order may guide the regulation of private entities in the future.

Cybersecurity of Federal Networks

The first section of the Order requires all executive agency heads to implement "risk management measures commensurate with the risk and magnitude of the harm that would result from unauthorized access, use, disclosure, disruption, modification, or destruction of IT and data."[2] Specifically, the Order directs executive agencies to immediately use the "Framework for Improving Critical Infrastructure Cybersecurity"[3] developed by the National Institute of Standards and Technology ("NIST"), or any successor document to manage the agency's cybersecurity risk.

The NIST Framework is a set of voluntary guidelines that encourage organizations to use a risk-management model of cybersecurity. Since its development, the NIST Framework has been widely adopted and adapted by critical infrastructure operators and various private entities and businesses, and several federal agencies have used it as a foundational document for cybersecurity.[4] Still, in announcing the Order, Assistant to the President Tom Bossert said, "It is something that we have asked the private sector to

For more information, contact:

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

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

Nicholas A. Oldham
+1 202 626 3740
noldham@kslaw.com

Elizabeth D. Adler
+1 404 572 3555
eadler@kslaw.com

Claudia A. Hrvatin
+1 202 661 7950
chrvatin@kslaw.com

Bethany Rupert
+1 404 572 3525
brupert@kslaw.com

Anush Emelianova
+1 404 572 4616
aemelianova@kslaw.com

www.kslaw.com

implement, and not forced upon ourselves."[5] The Order states that the "executive branch has for too long accepted antiquated and difficult–to-defend IT," and that agencies must take proactive steps to mitigate known vulnerabilities.[6] The NIST Framework has been updated once since its inception, in January 2017 (albeit in draft form).[7] While the NIST Framework remains voluntary for private entities, its mandatory application to federal agencies may well evolve into de facto standards against which an organization's actions may be judged in litigation and regulatory enforcement actions.

In addition to using the NIST Framework, all executive federal agencies must "provide a risk management report to the Secretary of Homeland Security and the Director of the Office of Management and Budget (OMB) within 90 days" of the Order,[8] and this report must describe how the agency plans to implement the NIST Framework and document "the risk mitigation and acceptance choices made by each agency head."[9] The Secretary of Homeland Security and the Director of OMB will jointly evaluate each agency's report "to determine whether the risk mitigation and acceptance choices set forth in the reports are appropriate and sufficient to manage the cybersecurity risk to the executive branch enterprise in the aggregate."[10] Based on this evaluation, the Secretary and the Director will submit a plan to the President for addressing insufficiencies where they exist and creating a "regular process" going forward for assessing whether the agencies are aligning their policies with the NIST Framework.[11]

The Order also requires a report regarding the "modernization of Federal IT" to promote "the policy of the executive branch to build and maintain a modern, secure, and more resilient executive branch IT architecture," and directs agency heads to "show preference in their procurement for shared IT services" among the agencies.[12] In the days following this Order, we may see new opportunities for companies to provide the systems and resolutions needed by federal agencies to comply with the Order.

Cybersecurity of Critical Infrastructure

The second section of the Order aims to support the "cybersecurity risk management efforts of the owners and operators of the Nation's critical infrastructure."[13] The Order continues the Obama Administration's public-private partnerships in this arena, defining critical infrastructure entities as those identified pursuant to section 9 of Obama's Executive Order 13636 of February 12, 2013 (Improving Critical Infrastructure Cybersecurity), which was the original catalyst for the NIST Framework.[14] Within 180 days, the Secretary of Homeland Security, in coordination with the Secretary of Defense and other agency heads, must "identify authorities and capabilities that agencies could employ to support the cybersecurity efforts" of those infrastructure entities, engage those entities and solicit input, and finally, provide a report to the President that will include findings and recommendations for better supporting the cybersecurity risk management efforts of those entities.[15]

While the stated policy of the Order is to "support" critical infrastructure entities, the Order also requires the Secretary of Homeland Security, in cooperation with other agency heads, to identify shortcomings with respect to some areas pertaining to critical infrastructure[16] — which may ultimately impose obligations on the private sector. The Secretaries of Homeland Security and Commerce must "evaluate the sufficiency" of federal policies promoting the market transparency of cybersecurity risk management practices, especially regarding publicly traded critical infrastructure entities. Supporting cybersecurity transparency in the marketplace may prove to be a difficult balancing act, as President Trump has previously indicated that the "methods, tools and tactics we use to keep America safe [from cyberattacks] should not be a public discussion that will benefit those who seek to do us harm."[17]

The Order also directs various agency heads to address three types of potential threats: (1) botnets (automated and distributed attacks);[18] (2) power outages associated with a significant cyber incident;[19] and (3) cybersecurity risks facing the defense industrial base and its supply chain.[20] The agencies must create a process to "improve the resilience of the internet and communications ecosystem and to encourage collaboration with the goal of dramatically reducing threats perpetrated by automated and distributed attacks."[21]

This process will begin with a report submitted to the President and a preliminary plan to be derived therefrom. Executive agencies also are instructed to assess any gaps in capabilities required to mitigate the consequences of these threats with the goal of improving cybersecurity in these areas. Moreover, various defense and security agency heads are charged with preparing a report to the President, within 90 days of the date of the Order, "on cybersecurity risks facing the defense industrial base, including its supply chain, and United States military platforms, systems, networks, and capabilities, and recommendations for mitigating these risks."[22]

Cybersecurity for the Nation

The final section of the Order addresses maintaining an open and reliable internet that fosters economic prosperity, "while respecting privacy and guarding against disruption, fraud, and theft." To determine the best approach to accomplish these goals, the Order directs a variety of agency heads, including the Secretary of State and the Attorney General, to jointly submit two reports to the President – the first to focus "on the Nation's strategic options for deterring adversaries and better protecting the American people from cyber threats,"[23] and the second to document "an engagement strategy for international cooperation in cybersecurity."[24]

The Order also directs various agency heads to "jointly assess" the cybersecurity workforce—specifically, "the sufficiency of efforts to educate and train" that workforce, both in the public and private sectors.[25] The Director of National Intelligence must evaluate similar efforts taken by "potential foreign cyber peers," and the Secretary of Defense must determine whether the United States' efforts will maintain or increase "its advantage in national-security-related cyber capabilities."[26]

In sum, although this Order directs its requirements to U.S. government agencies, the private sector should take note of its focus on foreign security threats, and the potential for the various requirements to be implemented, at least in part, by federal agencies when regulating private entities. And private businesses, in general, should be aware of the strong significance that the Order places on the NIST Framework, and how that framework may be used as a "national bar" for cybersecurity standards, by both federal agencies and private businesses. Following quickly on the heels of the Order, NIST issued draft guidance (Interagency Report 8170) on how federal agencies can implement the NIST Framework.[27] According to the draft guidance, NIST will use the feedback it receives from federal agencies to incorporate "Cybersecurity Framework concepts into its various cybersecurity risk management publications."[28] Due to the NIST Framework's influence amongst private businesses, and now mandated central position in federal agencies, it is rapidly becoming the de facto standard for reasonableness with regard to data practices, whether in the public or private sectors.[29]

King & Spalding's Data, Privacy & Security Practice

With more than 60 Data, Privacy & Security lawyers in offices across the United States, Europe, and the Middle East, King & Spalding is able to provide substantive expertise and collaborative support to clients across a wide spectrum of industries and jurisdictions facing privacy and cybersecurity-based legal concerns. We apply a multidisciplinary approach to such issues, bringing together attorneys with backgrounds in corporate governance and transactions, healthcare, intellectual property rights, complex civil litigation, e-discovery, government investigations, government advocacy, insurance recovery, and public policy. Our Data, Privacy & Security Practice has unparalleled experience in areas ranging from providing regulatory compliance advice, to responding to security incidents including data breaches and cybersecurity incidents, interfacing with stakeholders and the government, 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 White House, "Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," May 11, 2017, (hereafter "Executive Order on Cybersecurity (2017)"), Section 1(c)(i), available at https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal.

[2] Executive Order on Cybersecurity (2017), Section 1(c)(i).

[3] National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, February 12, 2014, available at https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

[4] Tara Seals, "Most Federal Agencies Now Use NIST Cybersecurity Framework," Infosecurity Magazine (December 11, 2015), available at https://www.infosecurity-magazine.com/news/most-federal-agencies-nist-cyber/.

[5] Eric Chabrow, "NIST Tailors Framework for Federal Agencies," Careers Info Security (May 17, 2017), available at http://www.careersinfosecurity.com/nist-tailors-framework-for-federal-agencies-a-9927.

[6] Executive Order on Cybersecurity (2017), Section 1(b)(ii).

[7] National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, January 10, 2017, available at https://www.nist.gov/sites/default/files/documents/draft-cybersecurity-framework-v1.11.pdf.

[8] Executive Order on Cybersecurity (2017), Section 1(c)(ii).

[9] *Id.*

[10] *Id.* at Section 1(c)(iii).

[11] *See id.* at Section 1(c)(iv).

[12] *Id.* at Section 1(c)(vi).

[13] *Id.* at Section 2(a).

[14] *Id.* at Section 2(b)(i).

[15] *Id.* at Section 2(b).

[16] *Id.* at Sections 2(a), (c)–(f).

[17] Statement by President-Elect Donald J. Trump, GreatAgain.gov (Jan. 6, 2017), available at https://greatagain.gov/intel-meeting-3b6542ca6500.

[18] Executive Order on Cybersecurity (2017), Section 2(d).

[19] *Id.* at Section 2(e).

[20] *Id.* at Section 2(f).

[21] *Id.* at Section 2(d).

[22] *Id.* at Section 2(f).

[23] *Id.* at Section 3(b).

[24] *Id.* at Section 3(c)

[25] *Id.* at Section 3(d)(i).

[26] *Id.* at Section 3(d)(ii)&(iii).

[27] National Institute of Standards and Technology, The Cybersecurity Framework: Implementation Guidance for Federal Agencies (May 17, 2017), available at http://csrc.nist.gov/publications/drafts/nistir-8170/nistir8170-draft.pdf.

[28] *Id.* at 10.

[29] *See* Andrea Arias, "The NIST Cybersecurity Framework and the FTC," The Federal Trade Commission (August 31, 2016), available at https://www.ftc.gov/news-events/blogs/business-blog/2016/08/nist-cybersecurity-framework-ftc?utm_source=govdelivery ("For that reason, the touchstone of the FTC's approach to data security has been reasonableness—that is, a company's data security measures must be reasonable in light of the volume and sensitivity of information the company holds, the size and complexity of the company's operations, the cost of the tools that are available to address vulnerabilities, and other factors. Moreover, the FTC's cases focus on whether the company has undertaken a reasonable process to secure data.").