WILLKIE FARR & GALLAGHER LLP

NEW YORK WASHINGTON HOUSTON PARIS LONDON FRANKFURT BRUSSELS MILAN ROME

CLIENT MEMORANDUM

White House Issues Long-Awaited Executive Order on Cybersecurity

May 18, 2017

AUTHORS

Daniel K. Alvarez | Elizabeth J. Bower | James C. Dugan | Elizabeth P. Gray | Alex J. Moyer

Coincidentally, on the eve of one of the largest cyberattacks in history – spanning more than 100 countries and affecting connected devices on every continent, except perhaps Antarctica – the long-awaited Executive Order on Cybersecurity, entitled "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure" (the "Order"),[1] was signed by the President and released by the White House on May 11, 2017. The primary focus of the Order is the Administration's goals and plans to improve the federal government's "cyber-readiness." The Order represents a promising first step, as it evinces a view that cybersecurity is a priority for the Administration, underscored by measures like those placing accountability at the agency-head level. However, as with all things, the devil is in the details, and the Order does not delve into specifics of cybersecurity protocol. Rather, the Order effectively sets forth a "plan for a plan," primarily instructing federal agencies to study and report on specific cybersecurity issues, laying the groundwork for substantive policy changes at an undetermined time. As a part of this process, the Order includes a number of directives to relevant federal departments that merit close monitoring by entities in the private sector, and particularly entities that have been designated "critical infrastructure" by the Department of Homeland Security.

[1] Exec. Order No. 13228 (May 11, 2017), available here.

A. Points of Interest for the Private Sector

The Order contains a number of directives that implicate private-sector cybersecurity efforts, especially those of critical infrastructure entities. In particular:

- The Secretary of Homeland Security, in coordination with the Secretary of Defense, Attorney General, and other agency heads, is directed to identify authorities and capabilities the federal government can leverage to support the cyber efforts of critical infrastructure entities (as determined under Executive Order 13228[2]). The agency heads are directed to engage these entities and solicit their input about the avenues and obstacles for the agencies' support. This private sector feedback is to be folded into the analysis and included in a report to the President reflecting the agencies' findings and recommendations to improve the support offered these entities, with annual updates to the report.

- The Order directs the Secretary of Homeland Security, in coordination with the Secretary of Commerce, to study the "market transparency" of critical infrastructure entities' cybersecurity risk management practices and provide a report to the President examining the sufficiency of existing federal policies and practices promoting this sort of transparency. The focus of this report is publicly traded critical infrastructure entities; although all critical infrastructure entities, as well as private sector businesses of any kind, would be advised to monitor these developments.

- The Secretaries of Commerce and Homeland Security also are directed to "jointly lead an open and transparent process to identify and promote action by appropriate stakeholders" to improve resilience against botnets and other distributed attacks, encouraging collaboration to achieve that goal. Seeking to prevent future incidents like the October 2016 Distributed Denial of Service ("DDoS") attack that crippled large portions of the Internet, the Order calls for a wide-ranging process involving a number of agencies and regulators, including the Chairs of the Federal Communications Commission and the Federal Trade Commission, as well as appropriate stakeholders. The Order mandates that the Secretaries submit a public report on the effort, but provides 240 days for a preliminary report and one year for the final version.

- The Secretaries of Energy and Homeland Security, in consultation with other agency heads, must assess the potential for and likely result of cyberattacks against the nation's energy resources, including the power grid. This assessment must also address the country's readiness to manage the consequences of such an attack, as well as any gaps or shortcomings in the nation's ability to mitigate those consequences.

- Cybersecurity workforce development is a particular point of emphasis, as the Order mandates three separate assessments of relevant efforts. The first calls for a review of the scope and sufficiency of the education and

[2] Exec. Order No. 13636, § 9 (Feb. 12, 2013), available here.

training available in primary through higher education to prepare the American cybersecurity workforce of the future. The second will study the efforts of "potential foreign cyber peers" to identify practices likely to affect America's cyber competitiveness. Finally, the Secretary of Defense is directed to coordinate with other agency heads to examine U.S. efforts in order to ensure the country maintains or increases its advantage in national-security-related cyber capabilities.

B. Federal Government Cybersecurity

Cybersecurity and cyber-readiness are increasingly receiving attention, not just in the private sector, but in the public sector as well. Highly publicized incidents – from the 2015 breach of the Office of Personnel Management that exposed more than 21 million records to last week's WannaCrypt ransomware attack, which made use of a leaked NSA cyber tool and affected hundreds of thousands of computer systems and connected devices in over 100 countries – have demonstrated the far-reaching consequences of cybersecurity failures by the federal government. Although a report by the Office of Management and Budget ("OMB") released in March highlighted improvements in federal cybersecurity efforts, it recognized that substantial deficiencies still exist, a fact exemplified by the over 30,000 cyber incidents that compromised the information or system functionality of federal agencies in 2016 alone.[3] Recognizing the challenges and threats facing the federal government, the Order takes four key steps that seek to improve federal cyber-readiness:

- First, the Order makes agency heads accountable for managing cybersecurity risk to their respective agencies. Previously, this responsibility fell to agencies' respective IT staff and often followed an ad-hoc approach. The escalation of accountability, following the trend of private sector regulations imposing cybersecurity obligations on company executives, likely will increase emphasis of cyber preparations from the top down.

- Second, the Order directs agencies to implement the risk management measures set forth in the NIST Framework.[4] Not only would this result in a standardized approach to risk management across federal agencies, but it would also provide agency heads, who likely lack relevant cybersecurity expertise, a form of guidance as they set out to improve their agencies' protocols.

- Third, the Order requires each agency to provide a risk management report to the Secretary of Homeland Security and the Director of OMB to document the risk mitigation and acceptance choices, and describe the agency's implementation plan for the NIST Framework. After the Secretary and Director assess all the reports, the Director of OMB will submit to the President a report addressing the present state of cybersecurity of the entire Executive Branch and the plan for improvement.

---

[3] Office of Mgmt. & Budget, Exec. Office of the President, *Federal Information Security Modernization Act of 2014, FY 2016 Annual Report to Congress*, Mar. 10, 2017, available here.

[4] Nat'l Inst. of Stds. & Tech., *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0*, Feb. 12, 2014, available here. The NIST Framework is in the process of being updated to version 1.1, with comments on the proposed changes submitted last month.

- Fourth, the Order directs the recently created American Technology Council to compile a report regarding the various legal, policy, and budgetary considerations involved in modernizing and transitioning federal agencies to shared IT and consolidated networks. Similar to the adoption of the NIST Framework, the emphasis on transitioning agencies to shared, cloud-based networks allows for standardization, in addition to centralization and modernization.

Willkie's Cybersecurity & Privacy team will continue to monitor the implementation of the Order's directives, and can help assess and navigate any potential impact on your business.

If you have any questions regarding this memorandum, please contact Daniel K. Alvarez (202-303-1125, dalvarez@willkie.com), Elizabeth J. Bower (202-303-1252, ebower@willkie.com), James C. Dugan (212-728-8654, jdugan@willkie.com), Elizabeth P. Gray (202-303-1207, egray@willkie.com), Alex J. Moyer (202-303-1280, amoyer@willkie.com) or the Willkie attorney with whom you regularly work.

Willkie Farr & Gallagher LLP is an international law firm with offices in New York, Washington, Houston, Paris, London, Frankfurt, Brussels, Milan and Rome. The firm is headquartered at 787 Seventh Avenue, New York, NY 10019-6099. Our telephone number is (212) 728-8000 and our fax number is (212) 728-8111. Our website is located at www.willkie.com.

May 18, 2017