Bloomberg Law

Privacy and Security Law Report®

Cybersecurity Executive Order

President Donald Trump's long-awaited ''Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, calls for a government-wide review and analysis of federal information technology infrastructure, including known risks and vulnerabilities, as well as consideration of the U.S.'s cybersecurity capabilities in relation to the rest of the world, the authors write.

Presidential Executive Order on Cybersecurity: No More Antiquated IT

BY JONATHAN MEYER, JOHN CHIERICHELLA, AND TOWNSEND BOURNE

On May 11, President Donald Trump issued his long-awaited Executive Order on cybersecurity, the ''Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.'' It had been in the works since early in the administration, and its release had been announced (and drafts leaked) several times, only to be pulled back and reworked further. The Executive Order calls for a government-wide review and analysis of federal information technology infrastructure, including known risks and vulnerabilities, as well as consideration of the U.S.'s cybersecurity capabilities in relation to the rest of the world.

The Order begins by stating explicitly that ''[t]the President will hold accountable heads of executive departments and agencies (Agency Heads) for managing cybersecurity risk to their enterprises.'' It then goes on to state the government's intention to ''manage cybersecurity risk as an executive branch enterprise.'' While neither of these statements are groundbreaking, they send a strong message to government leaders that cybersecurity is now a high priority and that the White House will be looking to government leaders to focus on this issue and coordinate appropriately with others in government.

The Order also speaks of cybersecurity in terms of risk management, calling on Agency Heads to approach cybersecurity based on the ''risk and magnitude of the harm that would result from unauthorized access, use, disclosure, disruption, modification or destruction of IT and data.'' Addressing cybersecurity as risk management is an approach growing in acceptance today and one that the Obama Administration utilized in recent years. This is one of a number of indications in this Order that, unlike other areas of policy, we can expect intragovernment cybersecurity policy to show continuity with the prior administration.

Also of note, but not surprising, the Order requires each Agency Head to utilize the National Institute of Standards' Framework for Improving Critical Infrastructure Cybersecurity (NIST Framework) to manage his or her agency's cybersecurity risk. This NIST Framework has become a leading standard for cybersecurity policy not only in government, but across the economy.

The Order also clarifies cybersecurity responsibilities across the government. While giving roles to many officials, it taps the Secretary of Homeland Security and the Director of the Office of Management and Budget as the primary assessors of each civilian agency's cybersecurity efforts. For national security systems, that role will be played by the Secretary of Defense and the Director of National Intelligence. Recent years have wit-

Jonathan Meyer is a partner at Sheppard Mullin Richter & Hampton LLP in Washington.

John Chierichella is a partner at Sheppard Mullin Richter & Hampton LLP in Washington.

Townsend Bourne is an associate at Sheppard Mullin Richter & Hampton LLP in Washington.

 ISSN 1538-3423

nessed some behind-the-scenes power struggles over who is in charge of cyber. This Order should help bring some resolution to those issues.

The Order will be of particular interest not only to government agencies, but to companies that do business with the government. They should pay attention to its emphasis on the modernization of IT and the stated policy for ''Agency heads [to] show preference in their procurement for shared IT services, to the extent permitted by law, including email, cloud, and cybersecurity services.'' Thus, government contractors with far-reaching solutions that can be easily adapted for multiple agencies stand to benefit from the Executive Order if implemented as the President clearly intends. The Executive Order also mandates review of the supply chain for the defense industrial base, suggesting contractors serving the military may be more heavily scrutinized in the future (if that is even possible).

Addressing cybersecurity as risk management is an approach growing in acceptance today and one that the Obama Administration utilized in recent years.

The Order requires preparation of myriad reports by personnel throughout the government, many of which are due within a 90 day period—meaning we could see a shift in implementation of federal cybersecurity policy as well as new proposed regulations well before the end of the calendar year. The reports required by the Order shed some light on the areas of review, and the cyber threats, the President deems most critical.

■ The Head of each Executive department must submit a risk management report within 90 days of the Order (*i.e.*, by Aug. 9, 2017) describing the agency's approach and plan for risk mitigation as well as any known unmitigated risks. Risk management measures are to be in accordance with the NIST Framework.

■ Following receipt of the reports, the Director of OMB has 60 days to make a determination regarding the adequacy of the risk management reports provided by Agency heads, as well as a plan for cybersecurity for the executive branch enterprise. This includes a reconciliation of *all* policies, standards, and guidelines issued by *any agency* related to information security under 44 U.S.C. Chapter 35, Subchapter II as well as issuance of new policies, standards, or guidelines if necessary. It is probably safe to regard this 60-day timeline as ''aspirational.''

■ The Director of the American Technology Council must submit a report within 90 days addressing the modernization of Federal IT as well as the technical and budgetary considerations associated with transitioning agencies to (a) ''one or more consolidated network architectures''; and (b) ''shared IT services, including email, cloud, and cybersecurity services.''

■ The Secretary of Defense and Director of National Intelligence must report within 150 days of the Order (*i.e.*, by Oct. 8, 2017) on the implementation of the plans and strategies provided in the above-mentioned reports.

■ The Secretary of Homeland Security must issue a report, within 180 days of the Order, identifying ways better to protect our critical infrastructure entities from cyberattacks (as described in Executive Order 13636 (Feb. 12, 2013)).

■ The Secretary of Homeland Security must issue a report within 90 days regarding the adequacy of existing policies and practices ''to promote appropriate market transparency of cybersecurity risk management practices by critical infrastructure entities, with a focus on publicly traded critical infrastructure entities.''

■ The Secretaries of Commerce and Homeland Security are jointly tapped to lead a process to ''improve the resilience of the Internet and communications ecosystem'' to reduce the threats posed by automated and distributed attacks, such as botnets (*i.e.*, armies of infected computers and devices controlled remotely and used to attack particular targets). They are to submit a preliminary report within 240 days, and a final version within one year.

■ The Secretaries of Energy and Homeland Security are, within 90 days of the Order, to provide an assessment regarding ''the potential scope and duration of a prolonged power outage associated with a significant cyber incident'' as well as the ability of the United States to manage such an incident, including any gaps in capabilities.

■ Within 90 days of the Order, the Secretaries of State and Homeland Security and the Federal Bureau of Investigation Director are to issue a potentially classified report on ''cybersecurity risks facing the defense industrial base, including its supply chain, and United States military platforms, systems, networks, and capabilities,'' including recommendations to mitigate these risks.

■ A group of eight Agency Heads and White House officials must issue a report on ''strategic options for deterring adversaries and better protecting the American people from cyber threats'' within 90 days of the Order.

■ Within 45 days of the Order, reports are to be provided by multiple Agency Heads on ''international cybersecurity priorities.'' Within 90 days of submission of these reports, the Secretary of State is required to issue a report on ''an engagement strategy for international cooperation in cybersecurity.''

  PVLR ISSN 1538-3423

■ The Secretaries of Commerce and Homeland Security are ordered to provide findings and recommendations ''regarding how to support the growth and sustainment of the Nation's cybersecurity workforce in both the public and private sectors'' within 120 days of the Order.

■ Within 60 days of the Order, the Director of National Intelligence is to report on foreign workforce development efforts ''likely to affect long-term United States cybersecurity competitiveness.''

■ Within 150 days of the Order, the Secretary of Defense must report on the ''scope and sufficiency of United States efforts to ensure that the United States maintains or increases its advantage in national-security-related cyber capabilities.''

It will be interesting to see just how many of these reporting deadlines are actually met with meaningfully substantive reports. Regardless, many government personnel will be busy over the next few months scrutinizing the U.S.'s cyber capabilities and risks and identifying solutions for strengthening the nation's ability to prevent, detect, and respond to threats. As they do so, contractors and other companies that interact with the government can expect more collaboration among agencies in implementing protective measures, as well as an increased emphasis on cybersecurity from their government customers and interlocutors.

It is to be hoped that the intra-governmental focus on cybersecurity as risk management will carry over to the relationship of the government with contractors in this area and that the complex regulatory schemes imposed by recent changes to the government's procurement rules will not be transmuted by the government into a ''free fire zone'' for overly zealous attacks on contractors. After all, the government has not been terribly successful in preventing cyber intrusions into its systems. Holding contractors to a higher standard, with more significant consequences, hardly seems fair.