ROPES & GRAY

ALERT

Privacy & Data Security

May 16, 2017

Trump Issues First Executive Order on Cybersecurity: While Goals Are Ambitious, Timelines Are Tight

Attorneys
Heather Egan Sussman
James S. DeGraw
Rohan Massey
Douglas H. Meal
Seth C. Harrington
David M. McIntosh
Mark P. Szpak
Michelle Visser
Paul D. Rubin
Marc P. Berger
Laura G. Hoey
David T. Cohen
Daniel Freshman

On May 11, 2017, President Donald J. Trump signed an executive order addressing cybersecurity risk management across three key areas: (1) federal government networks, (2) critical infrastructure, and (3) cybersecurity for the nation as a whole (Order). The Order builds upon Presidential Policy Directive 21, issued by the prior administration on February 12, 2013, and orders agency heads and leaders across the executive branch to undertake a period of cybersecurity risk assessment, planning and reporting.

Taken together, the Order and its mandates aim to jump-start cybersecurity risk management activities within the federal government and establish concrete steps toward solving the aging federal information technology infrastructure – an area longcited as needing modernization. But while the Order's requirements are substantial, the reporting deadlines are relatively short, and many experts in the field query whether impacted agencies – many of which already are facing budget constraints – can undertake meaningful risk assessments and required planning activities on such important topics within these tight timelines.

Embedded within the heap of reporting requirements were several new policy declarations on cybersecurity for the Trump administration:

- Risk Allocation: Heads of executive departments and agencies shall be directly accountable for managing cybersecurity risks for their organizations;
- NIST Cybersecurity Framework Alignment: Agencies must follow the NIST Cybersecurity Framework for its cybersecurity risk management, and the executive branch plans to align existing cybersecurity and policy regulations with the Framework; and
- Shared / Consolidated Services: Agencies must "show preference" for shared IT services (including e-mail, cloud and cybersecurity services), and the executive branch aims to transition all agencies to using shared IT services, where feasible.

In all events, we can expect a flurry of activity across the federal government over the next few months as stakeholders work to meet the requirements of this ambitious Order. Here is a breakdown of those requirements.

Cybersecurity of Federal Networks

The Order establishes that it is "the policy of the United States to manage cybersecurity risk as an executive branch enterprise" and that "the President will hold heads of executive departments and agencies (agency heads) accountable for managing cybersecurity risk to their enterprises."

In particular, the Order provides that agency heads will be held accountable 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"; and
- Ensure "that cybersecurity risk management processes are aligned with strategic, operational, and budgetary planning processes."

Toward that end, the Order directs all agencies to use the NIST Framework for Improving Critical Infrastructure Cybersecurity (known as the "Cybersecurity Framework") to manage each agency's particularly cybersecurity risk. Notably, NIST released a proposed updated version of the Cybersecurity Framework earlier this year, adding a number of proposed improvements including important supplier controls.

90-Day Agency Reports

In addition, within 90 days of the executive order, all federal agencies must submit a cybersecurity "risk management report" to the Department of Homeland Security (DHS) and the Office of Management and Budget (OMB), documenting:

"(A) the risk mitigation and acceptance choices made by each agency head as of the date of this order, including:

(1) the strategic, operational, and budgetary considerations that informed those choices; and

(2) any accepted risk, including from unmitigated vulnerabilities; and

(B) describe the agency's action plan to implement the Framework."

The goal of part (A) is to document a baseline of the agency's current risk profile with relevant considerations, and the goal of part (B) is to outline the agency's proposed steps for how to map and align that baseline to the Cybersecurity Framework.

Special rules and timing requirements apply to any National Security Systems.

60-Day Determination and Plan

After receiving the risk management reports from the agency heads, the Order then directs DHS and OMB, along with other stakeholders, to submit a report to the President within 60 days that assesses each agency report and makes a determination as to "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 (the determination)." That 60-day report must also establish a plan to:

- mitigate any identified risks to the executive branch;
- address immediate unmet budgetary needs;
- establish a regular process for reassessing these risks and future recurring budgetary needs;
- revise all policies, standards, and guidelines issued by any agency necessary to meet the objectives of the Order, consistent with law; and
- align such policies, standards, and guidelines with the Cybersecurity Framework.

Preference for Shared Services

The Order establishes a policy "to build and maintain a modern, secure, and more resilient executive branch IT architecture." Toward that end, the Order directs agency heads to "show preference in their procurement for shared IT services, to the extent permitted by law, including email, cloud, and cybersecurity services." This mandate brings the federal government more in line with the private sector trend in this same direction.

The Order also directs the American Technology Council to coordinate a report with relevant stakeholders within 90 days of the Order for how to modernize federal information technology systems. This report must outline the considerations relevant to transitioning federal agencies to consolidated network architecture and shared IT services. The Order directs agency heads to supply "information concerning their current IT architectures and plans as is necessary to complete this report on time."

Cybersecurity of Critical Infrastructure

The second part of the Order focuses on using the executive branch's "authorities and capabilities to support the cybersecurity risk management efforts of the owners and operators of the Nation's critical infrastructure ... as appropriate." The term "critical infrastructure" is defined in 42 USC s. 5195c(e) as "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."

This portion of the Order directs the DHS and relevant stakeholders to identify critical infrastructure at greatest risk of "attacks that could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security (section 9 entities)" and, within 180 days, to provide a report to the President with findings and recommendations for how to support the cybersecurity risk management activities of such critical infrastructure. The Order calls for an updated report to the President annually thereafter.

The Order then directs DHS and other relevant stakeholders to:

- Within 90 days of the order, produce a report examining the "sufficiency of existing federal 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"
- Lead an "open and transparent process" to identify ways "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 (e.g., botnets)" producing a preliminary report of recommendations within 240 days and a final report due to the President one year from the date of the Order.

As for the energy sector, within 90 days of the Order, the Secretary of Energy, in collaboration with other stakeholders, must assess the "potential scope and duration of a prolonged power outage" that could stem from a significant cyberincident, the nation's readiness to deal with such an outage, and any "gaps in assets or capabilities" necessary to address such an incident.

And finally, for the defense sector, within 90 days of the Order, the Secretary of Defense working with relevant stakeholders must report to the president 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."

Cybersecurity of the Nation

The third and final substantive part of the Order focuses on cybersecurity of the nation as a whole and establishes that in order to "ensure that the internet remains valuable for future generations, it is the policy of the executive branch to promote an open, interoperable, reliable, and secure internet that fosters efficiency, innovation, communication, and economic prosperity, while respecting privacy and guarding against disruption, fraud, and theft."

This portion of the Order focuses on deterrence and protection and international cooperation. In particular, it directs more reports to be prepared and submitted to the President:

- Within 90 days, the Secretary of State, in collaboration with other stakeholders including trade representatives, must submit a report to the President "on the Nation's strategic options for deterring adversaries and better protecting the American people from cyber threats."
- Within 45 days, the Secretaries of State, Treasury, Defense, Commerce, and Homeland Security, in coordination with the Attorney General and the Director of the FBI, "shall submit reports to the President on their international cybersecurity priorities, including those concerning investigation, attribution, cyber threat information sharing, response, capacity building, and cooperation."
- Within 90 days, the Secretary of State must, in collaboration with the other Secretaries, provide a report to the President, "documenting an engagement strategy for international cooperation in cybersecurity."

The Order closes its substantive directives by requiring a series of additional reports designed to identify and assure the development of a workforce to support the nation's growing cybersecurity needs, and to ensure the United States "maintains a long-term cybersecurity advantage."

Conclusion

As the Trump administration's first executive action on cybersecurity, the Order calls for a thorough review of the federal government's cybersecurity practices, but imposes minimal immediate consequences on the private sector or the marketplace.

At several points across the past three months, previously circulated drafts of the executive order did not allocate direct cybersecurity responsibility to agency heads, nor did it include the Federal Bureau of Investigation in its infrastructure review; both features are now included in the signed Order. By including defense and intelligence agencies in the infrastructure review, the executive order also allocates more responsibility to the military for federal cybersecurity, which had been previously resisted by the Obama administration.

Beyond the Order's reporting and review requirements, the Order does signal the growing importance of the NIST Cybersecurity Framework on both the public and private sectors. The NIST Cybersecurity Framework was originally published in 2014 as a voluntary set of guidelines for federal agencies. Increasingly, regulators have referenced the NIST Cybersecurity Framework in their industry guidance and enforcement actions in an effort to guide companies toward its adoption. Now entities conducting business with federal agencies, directly or indirectly, should anticipate that government agencies will expect that those with whom those agencies do business will have adopted and be operating under the NIST Cybersecurity Framework or a widely recognized alternative. Moreover, the emphasis the Order places on consolidation of services should lead more service providers to consider the benefits of becoming FEDRAMP-certified.

For more information regarding the May 11 executive order or to discuss cybersecurity issues more generally, please contact Heather Egan Sussman, Jim DeGraw, Rohan Massey, Doug Meal, Seth Harrington, David McIntosh, Mark

Szpak, Michelle Visser, Paul Rubin, Marc Berger, Laura Hoey, David Cohen, Dan Freshman, or another member of Ropes & Gray's leading privacy & data security team.