NELSON MULLINS

David F. Katz | Partner
404.322.6122
david.katz@nelsonmullins.com

The Feds: Who is Accountable for Managing Cybersecurity Risks?

Introduction

On May 11, 2017, President Donald Trump signed a Presidential Executive Order[1] entitled *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (the "Order"). The Order places accountability for managing cybersecurity risk on the agency heads of each of the executive departments and federal agencies within the executive branch of the federal government. The Order aligns the key departments and resources of the federal government to address the cybersecurity of Federal networks; cybersecurity of critical infrastructure; and cybersecurity for the nation.

Section One of the Order: The Cybersecurity of Federal Networks.

The Order makes it the policy of the United States to manage cybersecurity as an enterprise risk[2] instead of the individual agencies and departments acting independently to manage risks. This shift to enterprise management is significant because it creates a coordinated unified set of objectives under a common design for risk management across all of the executive branch. The Order's findings conclude that the executive branch has "for too long accepted antiquated and difficult-to-defend IT" and calls for "planning so that maintenance, improvements and modernization occur in a coordinated way and with appropriate regularity."[3] The Order finds that "[e]ffective risk management requires agency heads to lead integrated teams of senior executives with expertise in IT, security, budgeting, acquisition, law, privacy and human resources."[4] The acknowledgement of past inability to effectively deal with cyber threats and call for engagement of outside experts to lead these efforts is a strong indicator of the existing skills gaps that exists within the executive branch to address these on-going risks.

The Order requires agencies to use the *Framework for Improving Critical Infrastructure Cybersecurity (*the Framework*)*[5] developed by the National Institute of Standards and Technology to manage the agency's cybersecurity risks. Each agency head is required to provide a risk management report to the Secretary of Homeland Security and Director of Office of

---

[1] Exec. Order No. 13228, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure" (May 11, 2017).
[2] EO, § 1(a).
[3] EO, § 1(b)(ii) and (iii).
[4] EO, § 1(b)(v).
[5] National Institute of Standards and Technology (U.S.). Framework for Improving Critical Infrastructure Cybersecurity. 2014. <http://purl.fdlp.gov/GPO/gpo46587>. The February 2013 Executive Order-Improving Critical Infrastructure on Cybersecurity Section 7 established a baseline Framework to Reduce Cyber Risk to Critical Infrastructure by having the Secretary of Commerce direct the Director of National Institute of Standards and Technology to lead the development of a framework to reduce risk to critical infrastructure.

Management and Budget within 90 days of the Order.[6] The report shall document the risk mitigation and acceptance choices made by each agency head as of the date of the Order. The report must address the strategic, operational and budgetary considerations that informed those choices along with the accepted risk, including from unmitigated vulnerabilities.[7] Lastly, the report must describe the agency's action plan to implement the Framework.[8]

Once this reporting is completed, the Secretary of Homeland Security and the Director of Office of Management and Budget are both required within 60 days of receipt of these reports to submit to the President[9] a determination and plan to:

> (1) adequately protect the executive branch enterprise, should the determination identify insufficiencies;
>
> (2) address immediate unmet budgetary needs necessary to manage risk to the executive branch enterprise;
>
> (3) establish a regular process for reassessing and, if appropriate, reissuing the determination, and addressing future, recurring unmet budgetary needs necessary to manage risk to the executive branch enterprise;
>
> (4) clarify, reconcile, and reissue, as necessary and to the extent permitted by law, all policies, standards, and guidelines issued by any agency in furtherance of federal law establishing the coordination of federal information policy[10], and, as necessary and to the extent permitted by law, issue policies, standards, and guidelines in furtherance of this order; and
>
> (5) align these policies, standards, and guidelines with the Framework.[11]

The Order makes it the policy of the executive branch to "build and maintain a modern, secure, and resilient executive branch IT architecture."[12] Under the Order, IT architecture is defined as the integration and implementation of IT within an agency.[13] Additionally, agency heads are required to show preference in their procurement for shared IT services, to the extent permitted by law, including email, cloud and cybersecurity services. This component of the Order is perhaps the most significant development for information security policy on how the federal government has to date managed information security. Primarily, this provision brings

---

[6] EO, § (1)(c)(ii).
[7] EO, § 1(c)(ii)(A).
[8] EO, § 1(c)(ii)(B).
[9] EO, § 1(c)(iv).
[10] Chapter 35 subchapter II of title 44 U.S.C.
[11] EO, § 1(iv)(A) and (B).
[12] EO, § 1(vi).
[13] EO, § 4(c).

the commercialization of federal IT systems into practice and creates opportunities for private sector companies to more fully support the modernization and protection of Federal IT.

The Director of the American Technology Council is given the task to coordinate a report to the President from the Secretary of Homeland Security, the Director of the Office of Management and Budget and the Administrator of General Services in consultation with the Secretary of Commerce regarding modernization of Federal IT. This report is required within 90 days of the Order and the report shall "describe the legal, policy, and budgetary considerations relevant to -- as well as the technical feasibility and cost effectiveness, including timelines and milestones, of -- transitioning all agencies, or a subset of agencies, to: (aa) one or more consolidated network architectures; and (bb) shared IT services, including email, cloud, and cybersecurity services."[14] Lastly, the agencies are required as part of this reporting to make "recommendations to ensure consistency with section 227 of the Homeland Security Act (6 U.S.C. 148) and compliance with policies and practices issued in accordance with section 3553 of title 44, United States Code."[15] The Order sets forth separate requirements for a National Security Systems as defined in section 3552(b)(6) of title 44, United States Code. The responsibility for National Security Systems is shifted from the Secretary of Homeland Security to the Secretary of Defense. Additionally, the Director of National Intelligence replaces the Office of Management and Budget and reporting is required within 150 days and has to include a justification for any deviation from the requirements of Section 1 (c) of the Order.

Section Two: Cybersecurity of Critical Infrastructure.

The Order sets the policy of the executive branch to “use its authorities and capabilities to support cybersecurity risk management efforts of the owners and operators and the Nation's critical infrastructure.[16]” The Order brings the Secretary of Homeland Security, Secretary of Defense, Attorney General, the Director of National Intelligence and the Director of the Federal Bureau of Investigation together to identify "authorities and capabilities" that could be employed to support the cybersecurity efforts of critical infrastructure that is at greatest risk of attack and could result in catastrophic regional or national effects on public health or safety, economic security, or national security.[17] The Order ominously requires a joint assessment requirement for electricity disruption incident response capabilities.[18] This assessment would require reporting within 90 days and may be classified in full or in part and would include assessment of (1) the potential scope and duration of a prolonged power outage; (2) the readiness of the United States to manage the consequences of such an incident and (3) any gaps or shortcomings in assets or capabilities required to mitigate the consequences of such an

[14] EO, § 1 (vi)(B).
[15] EO, § 1 (vi)(C).
[16] EO, § 2 (a). Critical Infrastructure is defined in section 5195c(e) of title 42 United States Code.
[17] EO, § 2 (b)(i).
[18] EO, § 2(e)(i).

incident.[19] Lastly, the Order focuses on the Department of Defense's warfighting capabilities and industrial base requiring reporting within 90 days by the Secretary of Defense, the Secretary of Homeland Security and the Director of the Federal Bureau of Investigation in coordination with the Director of National Intelligence to report on the cybersecurity risks facing the defense industrial base, including its supply chain, and United States military platforms, systems, networks and capabilities along with recommendations for mitigating these risks.

Section Three: Cybersecurity for the Nation.

Section three of the Order makes the promotion of an open, interoperable, reliable and secure internet and the growth and sustainment of a skilled workforce in cybersecurity the policy of the United States.[20] The Order sets out a 90 day reporting requirement for the Secretary of State, Secretary of the Treasury, the Secretary of Defense, Attorney General, Secretary of Homeland Security and the United States Trade Representative in coordination with the Director of National Intelligence to advise the President on the strategic options for deterring adversaries and better protecting the American people from cyber threats.[21] Section 3 (c) requires the creation of an engagement strategy for international cooperation on cybersecurity.[22] In an effort to further promote a skilled workforce, Section 3 (d) requires the Secretary of Commerce, Secretary of Homeland Security in consultation of the Secretary of Defense, Secretary of Labor and Secretary of Education, and the Director of Office of Personnel Management to jointly assess the scope and sufficiency of efforts to educate and train the cybersecurity workforce of the future.[23] The reporting includes assessment of the sufficiency of cybersecurity related education curricula, training and apprenticeship programs, from primary through higher education. Workforce development includes reporting, within 120 days of the Order, of findings and recommendations to support the growth and sustainment of the Nation's cybersecurity workforce. The Order requires the Director of National Intelligence to review workforce development of foreign cyber peers and how this might affect the United States' cybersecurity competitiveness.[24] Lastly, the Secretary of Defense in coordination with the Secretary of Commerce, Secretary of Homeland Security and Director of National Intelligence to assess the scope of efforts to ensure maintenance or increase of its advantage in national-security-related cyber capabilities and to report on these within 150 days of the Order.[25]

[19] EO, § 2(e)(i)(ii)(iii).
[20] EO, § 3(a).
[21] EO, § 3(b).
[22] EO, § 3(c).
[23] EO, § 3(d).
[24] EO, § 3(d)(ii).
[25] EO, § 3(d)(iii).

Analysis and **Conclusion**

The Trump administration's efforts to hold agency heads accountable for the management of cybersecurity risks deserves real credit and could not have come sooner in light of the ongoing cybersecurity risks to the United States. Through this Order the Trump administration is well-positioned to determine and plan for how best to protect the executive branch enterprise and address budgetary needs necessary to manage cyber risks. By requiring executive agencies and departments to document risk mitigation and implement the Framework, the 2017 Order is a crucial step in advancing cybersecurity risk management. Moreover, the Order's particular focus on evaluating the budgetary needs of the individual agencies and departments combined with the role of the Office of Management and Budget is a strong indicator of the overall seriousness with which the Trump Administration intends to address cybersecurity risk. The Order's focus on support for critical infrastructure and identification of authorities and capabilities to support cybersecurity efforts around critical infrastructure appears to be a more aggressive and proactive measure than the previous Obama administration 2013 Executive Order which calls for a "consultative process" to coordinate improvements to the cybersecurity of critical infrastructure.[26]

In comparing the 2013 and 2017 Executive Orders, it is clear that the 2017 Order communicates a much greater sense of urgency on the part of the executive branch in light of the past four years. Over the last four years the threats posed by hostile nation states, cyber criminals, and other non-state actors has continued to escalate to point where the failure to adequately address the risks is proving to present a clear and present danger to the national security of the United States. Moreover, the shift in focus from individual department risk analysis and remediation to one of enterprise risk management is a significant change. The 2017 Order builds on the foundation created by the previous administration, but places greater accountability on the individual agency heads and departments in the executive branch. Additionally, the Order specifically references risks pertaining to botnets and other automated distributed threats and the need to improve resilience in the face of these threats. Most compelling is the specific mention of threats for electricity disruption and incident response capabilities. The inclusion of these specifically identified risks to cybersecurity infrastructure are a clear indicator that the federal government views these risks as significant. Notable in the 2017 Order is the specific focus on national security as it specifically relates to the Department of Defense's warfighting capabilities and risks in the industrial base and supply chain.

To the extent federal agencies and departments in the Executive Branch are able to comply with the provisions outlined in the Order there could be significant advancements in the ability to effectively mitigate cyber risks to the United States. The administration deserves credit for aggressively setting the agenda for more proactive and specific measures to address these continuing and increasing risks to the nation's security.

---

[26] *See Exec.* Order No. 13636, "Improving Critical Infrastructure Cybersecurity" 3 C.F.R. 217 (2014), at § 6.