President Trump Issues Cybersecurity Executive Order

MAY 12, 2017

On May 11, President Trump signed his long-awaited Executive Order on "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure."[1] Much of the Order mandates efforts to improve the government's own information technology (IT) and cybersecurity practices, but several directives focus on the private sector: (i) a report to the President within 90 days on whether publicly-traded companies operating critical infrastructure should have to make fuller public disclosures concerning their cybersecurity practices; (ii) a report to the President within 90 days on the electric sector's ability to respond to and mitigate an attack leading to a prolonged outage; (iii) a report to the President within 90 days on cyber threats confronting defense industrial base (DIB) companies and their supply chains; and (iv) a requirement that agencies conform their cybersecurity guidance documents to the National Institute of Standards and Technology's (NIST) Cybersecurity Framework, which may lead to new requirements for government contractors. The Order also calls for reports on the government's ability to assist and defend companies operating critical infrastructure systems at greatest risk, deterring cyber threats from abroad, building more effective defenses against botnets, international cybersecurity priorities, and cyber workforce development.

Cybersecurity of Critical Infrastructure

To support the risk management efforts of the owners and operators of critical infrastructure (CI), the Order requires various designated agencies to report to the President, within 90 days:

- Whether Federal policies and practices are sufficient "to promote appropriate market transparency of cybersecurity risk management practices" by CI entities, focusing on publicly-traded CI entities.[2] This suggests that the Trump Administration may be exploring the possibility of creating new requirements for companies, particularly those that are publicly-traded, to report their cybersecurity risk management practices to investors. In the event that this assessment leads to more extensive requirements or more aggressive enforcement by the Securities and Exchange Commission, publicly-traded companies should consider reviewing their securities disclosures to confirm that cybersecurity risks and risk management practices are appropriately disclosed to investors.
- Regarding the potential scope and duration of a prolonged power outage associated with a

significant cyber incident, the country's readiness to manage the consequences of such an incident, and any gaps or shortcomings in assets or capabilities.[3] The specific focus on the electric sector may signal cybersecurity priorities for the Trump Administration going forward, and companies in this sector in particular should seek opportunities to engage with Administration officials as they conduct the assessments and reporting required by the Order.

- Regarding the cybersecurity risks facing the DIB, including its supply chain, and the US military platforms, systems, networks, and capabilities, as well as recommendations for mitigating those risks.[4]

The Order also requires designated agencies to:

- Identify authorities and capabilities to support cybersecurity efforts of CI entities at greatest risk,[5] and engage and solicit input from those entities to evaluate whether and how the identified authorities and capabilities might be employed to support cyber risk management efforts, and any obstacles for doing so[6]; and
- Engage in an "open and transparent process," with appropriate stakeholders, to identify and promote action to improve internet and communications systems' resilience and collaboration to reduce threats from automated and distributed attacks, such as botnets.[7]

Cybersecurity of Federal Networks

The majority of the Executive Order focuses on improving IT security at Executive Branch agencies. However, defense and civilian agency contractors may see downstream effects from the Order's requirements for their agency customers.
Specifically, the Order:

- Requires agency heads to implement the NIST Cybersecurity Framework.[8] Contractors that have not yet implemented the NIST Cybersecurity Framework may see such a requirement imposed by agencies working to implement the Framework pursuant to the Order.
- Declares that agency heads will be held accountable by the President for "implementing 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 data," and for "ensuring that cybersecurity risk management processes are aligned with strategic, operational, and budgetary planning processes" in accordance with the Federal Information Security Management Act.[9]
- Directs agency heads to show procurement preference for shared IT services, to the extent permitted by law, including email, cloud, and cybersecurity services. Contractors for IT services may face a changing business landscape in light of this preference, such as increased focus on General Services Administration IT Schedule contracts.

---

[1] The Executive Order (the Order).

[2] Id. § 2(c).

[3] Order § 2(e). The assessment may be classified in whole or in part.

[4] Order § 2(e). The report may be classified in whole or in part.

[5] The Order explicitly references the process described in Section 9 of President Obama's Cybersecurity Executive Order (Executive Order 13,636 (Feb. 12, 2013)), and would not create a new designation process.

[6] Order § 2(b). The agencies must report their findings to the President within 180 days, and update their findings annually thereafter.

[7] Order § 2(d). The agencies must provide a preliminary report on this effort within 240 days, to be followed by a final report within one year.

[8] Order § 1(c)(ii).

[9] Order § 1(c)(i).

Authors

Benjamin A. Powell

PARTNER

Co-Chair, Cybersecurity and Privacy Practice

Co-Chair, Artificial Intelligence Practice

benjamin.powell@wilmerhale.com

+1 202 663 6770