wiley

NEWSLETTER

President Trump's Cyber EO Contains Few Surprises, But Portends a Busy Year for Federal Agencies and the Private Sector

May 2017

On May 11, 2017, President Trump signed the long-awaited Cybersecurity Executive Order (Cyber EO). Entitled *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, the Cyber EO has three substantive sections: (1) Cybersecurity of Federal Networks, (2) Cybersecurity of Critical Infrastructure, and (3) Cybersecurity for the Nation. These sections create requirements for a number of reports and assessments by various agencies. These reports will be classified as appropriate. Overall, the Cyber EO contemplates at least 15 reports in the next year, and one report that is required to be updated annually. The Cyber EO picks up on several issues, from botnets to workforce development, that industry and government have been looking at for some time. In the main, it is silent about process and the scope of opportunities for public comment and input.

Section 1, "Cybersecurity of Federal Networks," Focuses on Federal Network Risk Management, the NIST Cybersecurity Framework, and Procurement

The Cyber EO emphasizes the importance of cybersecurity risk management, defining it as "full range of activities undertaken to protect IT and data from unauthorized access and other cyber threats, to maintain awareness of cyber threats, to detect anomalies and incidents ..., and to mitigate the impact of, respond to, and recover from incidents." This section also highlights information sharing, stating that information sharing "facilitates and supports [cybersecurity risk management] activities."

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Practice Areas

Privacy, Cyber & Data Governance

Section 1 mandates that executive branch agencies implement risk management, and creates a series of reports and reviews:

- "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 and data."
- Each agency head **must use NIST's *Cybersecurity Framework*** (or any successor document) to manage agency cybersecurity risk. Each agency head must **provide a risk management report** to the Secretary of Homeland Security and the Director of OMB by **August 9, 2017.** Reports must document risk mitigation and acceptance choices made by agency heads as of May 11, 2017, and detail action plans for implementing NIST's *Cybersecurity Framework*.
- The Secretary of Homeland Security and the Director of OMB **will make determinations** based on the agencies' risk management reports as to whether each agency's risk mitigation and acceptance choices are adequate. Within 60 days of receipt of the reports, the Director of OMB and Secretary of Homeland Security will **submit the determinations and a plan** to the President. The plan must, among other things: "protect the executive branch enterprise, should the determination identify insufficiencies; address immediate unmet budgetary needs ...; establish a regular process for reassessing and, if appropriate, reissuing the determination, and addressing future, recurring unmet budgetary needs..." and align with the NIST *Cybersecurity Framework*.

The EO states that the executive branch must "build and maintain a modern, secure, and more resilient executive branch IT architecture." Agency heads are required to **favor shared IT services** – including email, cloud, and cybersecurity services – in the procurement process. Additionally, this section requires a **report to the President regarding modernization of federal IT**. The report is due **August 9, 2017**, and "shall assess the effects of transitioning all agencies, or a subset of agencies, to shared IT services with respect to cybersecurity."[1]

Section 2, "Cybersecurity of Critical Infrastructure," Initiates Market Transparency Efforts, Orders a Special Effort to Address Botnets, and Directs More Reports on Industries and Sectors

This section draws from President Obama's 2013 EO, *Critical Infrastructure Security and Resilience*, and mandates that the Secretary of Homeland Security, with the Secretary of Defense, the Attorney General, the Director of National Intelligence, the Director of the FBI, appropriate sector-specific agencies, and others shall:

- **"[I]dentify authorities and capabilities** that agencies could employ to support the cybersecurity efforts of critical infrastructure entities."
- **Engage with and solicit input from critical infrastructure entities** to determine how identified authorities and capabilities might be employed, and to identify any obstacles.
- Provide a **report to the President** by **November 7, 2017** that includes authorities and capabilities; results from engagement with critical infrastructure entities, and has findings and recommendations

for supporting critical infrastructure entities' cybersecurity risk management efforts. The report must be **updated annually**.

Section 2 requires the Secretary of Homeland Security, with the Secretary of Commerce, to submit a report on transparency in the marketplace by August 9, 2017. It is to look at "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."

Additionally, Section 2 launches an effort against **botnets and other automated threats**. Specifically, the Secretaries of Commerce and Homeland Security are to lead an "open and transparent process to identify and promote action by appropriate stakeholders 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)." They are to consult with other agency heads, including but not limited to the Chairs of the FTC and the FCC. A **preliminary report on the botnet effort** is to be made publicly available by early **January 2018**, and the **final report** is due to the President on **May 11, 2018**.

Section 2 requires additional industry-specific reports and assessments.

- It requires an **assessment of electricity disruption incident response capabilities**, to be completed by the Secretaries of Energy and Homeland Security, due on **August 9, 2017.**
- The departments of Defense and Homeland Security, along with the FBI, must present to the President, also on **August 9, 2017,** a **report on cyber risks facing the defense industrial base**, including supply chain.

Section 3, "Cybersecurity for the Nation," Addresses Deterrence, Workforce, and International Issues

The Cyber EO states: "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. Further, the United States seeks to support the growth and sustainment of a workforce that is skilled in cybersecurity and related fields as the foundation for achieving our objectives in cyberspace."

Section 3 mandates a number of efforts, including:

- A Deterrence and Protection Report, due August 9, 2017, which should cover the "Nation's strategic options for deterring adversaries and better protecting the American people from cyber threats."
- International Cybersecurity Priorities Reports from various agency heads, in an effort to work with allies to maintain the overarching policy goal stated above. These reports are due June 2017. The Secretary of State is charged with providing a report documenting an engagement strategy for international cybersecurity cooperation 90 days after the initial reports are submitted.

- A domestic and international workforce development effort.
  - First, the Secretaries of Commerce and Homeland Security, with others, must "**jointly assess** the scope and sufficiency of efforts to educate and train the American cybersecurity workforce of the future, including cybersecurity-related education curricula, training, and apprenticeship programs, from primary through higher education; and [**by September 8, 2017**], provide a report to the President ... with findings and recommendations regarding how to support the growth and sustainment of the Nation's cybersecurity workforce in both the public and private sectors."
  - Second, the Director of National Intelligence will review the workforce development efforts of foreign cyber peers; a **report** on this effort is due **July 10, 2017**.
  - Third, the Secretary of Defense will "assess the scope and sufficiency of the United States efforts to ensure that the United States maintains or increases its advantage in national-security-related cyber capabilities, and provide a **report** with findings and recommendations to the President by **October 2017.**

---

[1] For "National Security Systems," the Secretary of Defense and the Director of National Intelligence are in charge. They are charged with submitting a report regarding risk management to the Assistant to the President for National Security Affairs and the Assistant to the President for Homeland Security and Counterterrorism. The report is due in October 2017.