wiley

ALERT

President Trump's Cyber Mandate: Analysis of Executive Order on Strengthening U.S. Cybersecurity

June 13, 2025

Below are links to the key topics covered in this alert:

President Trump issued a cybersecurity Executive Order, "Sustaining Select Efforts to Strengthen the Nation's Cybersecurity" (Trump EO), along with a corresponding Fact Sheet on June 6, 2025. The Trump EO clears some of the regulatory overhang from Biden Administration cybersecurity policies, streamlining updates on the security of software, federal communications, post-quantum cryptography (PQC), and artificial intelligence (AI) for federal agencies.

The Trump EO amends the Biden Administration Executive Order "Strengthening and Promoting Innovation in the Nation's Cybersecurity" (Biden EO 14144), released on January 16, 2025, and Obama Administration Executive Order 13694, "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Sydney M. White
Special Counsel
202.719.3425
swhite@wiley.law

Alissa Lynwood
Associate
202.719.4527
alynwood@wiley.law

Teresita Regelbrugge
Associate
202.719.4375
rregelbrugge@wiley.law

Practice Areas

AI Executive Order

Cyber and Privacy Investigations, Incidents & Enforcement

Privacy, Cyber & Data Governance

Activities" (Obama EO or Obama EO 13694), released on April 1, 2015, which established sanctions for persons involved with malicious cyber-enabled activities.

The Trump EO also modifies lines of effort started under President Biden's EO 14028, Executive Order on Improving the Nation's Cybersecurity (Biden EO 14028) released on May 12, 2021 and further detailed in the *National Cybersecurity Strategy* released on March 23, 2023, and the *National Cybersecurity Strategy Implementation Plans V.1 and V.2* released in July 2023 and May 2024 respectively. Much like Biden EO 14144, the Trump EO responds to cybersecurity threats from adversarial countries including China, Russia, Iran, and North Korea. The Trump EO directs actions to defend digital infrastructure and secure services and capabilities vital to the digital domain. The Trump EO reins back the scope of Biden EO 14144 by exempting National Security Systems and designated debilitating impact systems, with the exception of provisions on PQC. Overall, the Trump EO is less prescriptive than either Biden EO 14028 or EO 14144, consistent with calls from Congress for a more moderate approach to cybersecurity.

Takeaways on Cybersecurity Priorities

- The Trump EO identifies China as the biggest threat to U.S. cybersecurity and outlines measures where the government will enhance secure technology practices.
- Lines of effort on secure software development and secure Internet routing are continued from the Biden Administration.
- Agency transitions to PQC remain on the 2035 schedule established during the Biden Administration.
- Consistent with previous Trump Executive Orders, this order frames AI advances as being driven by private sector innovation, provides for greater agency adoption of AI, and incorporates AI vulnerabilities into interagency coordination on vulnerability management.

Software Supply Chains

Executive departments and agencies are tasked with several key actions to bolster software security, primarily spearheaded by the National Institute of Standards and Technology (NIST) under the U.S. Department of Commerce. Specifically, the Trump EO "directs the Federal government to advance secure software development" by establishing new practices, procedures, controls, and implementation examples for the secure development and delivery of software.

Building on Biden EO 14144, the Trump EO leverages NIST's work and takes a broad strategic approach to enhancing the software supply chain and directs NIST to establish a consortium with industry at the National Cybersecurity Center of Excellence by August 1, 2025. This consortium's goal is to develop guidance for implementing secure software development, security, and operations practices based on existing NIST Special Publication 800-218 version 1.1 *Secure Software Development Framework* (SSDF). The Trump EO keeps the requirement updates to the SSDF based on the consortium guidance and NIST Special Publication 800-53, *Security and Privacy Controls for Information Systems and Organizations*, to incorporate guidance on secure patching and updates.

The Trump EO keeps requirements related to the SSDF for agencies to require government contractors providing software to the government to confirm their compliance with secure software practices in the SSDF through a common attestation form. However, the Trump EO strikes the requirement in Biden EO 14144 for those government contractors to submit the common attestation form to a repository established by the Cybersecurity and Infrastructure Security Agency (CISA) and for CISA to validate the attestations.[1]

Improving the Cybersecurity of Federal Systems

The Trump EO preserves the prioritization of strengthening CISA's threat hunting capability across Federal Civilian Executive Branch (FCEB) agencies. Under Biden EO 14144, the Director of CISA, in coordination with the Federal Chief Information Officer Council and the Federal Chief Information Security Officer Council, is required to develop a "concept of operations" by December 3, 2025 for the "timely access to required data" from agency endpoint detection and response (EDR) solutions and agency security operation centers to identify coordinated cyber campaigns and coordinate government-wide information gathering and analysis on cyber incidents. Biden EO 14144 lays out a process for CISA to develop EDR technical controls for implementation in FCEB agencies, which do not disrupt CISA's threat hunting activities or agencies' "mission-critical operations."

If CISA is accessing "agency data that is subject to statutory, regulatory, or judicial restrictions," CISA is directed to comply with agency procedures and "work with the agency to develop an appropriate administrative accommodation … so that data is not subject to unauthorized access or use."

Cloud Services

As for the Federal Risk and Authorization Management Program (FedRAMP), the Trump EO intends "to incentivize or require" cloud service providers "to produce baselines with specifications and recommendations for agency configuration of agency cloud-based systems in order to secure Federal data based on agency requirements." This information is intended to help agencies address difficulties surrounding configuration of cloud services.

The Trump EO continues to prioritize addressing identity and access management to strengthen cloud security by directing the development of guidelines for secure management of access tokens and cryptographic keys used by cloud service providers.

Space Systems

The Trump EO preserves obligations under Biden EO 14144 to update civil space cybersecurity requirements in the Federal Acquisition Regulation. The Trump EO directs that requirements must be risk-based, apply using a tiered approach, and apply at a minimum to on-orbit and link segments. Higher-tier requirements will include encryption; methods to detect, report, and recover from anomalous network or system activity; and use of the SSDF. National Cyber Director (NCD) will evaluate space ground systems owned by FCEB agencies and recommend improvements to cyber defenses, which will be applied by OMB to FCEB agencies.

Securing Federal Communications

The Trump EO amends Section 4 of Biden EO 14144 by striking the statement that Internet routing using Border Gateway Protocol "is vulnerable to attack and misconfiguration." Although this change does not alter federal policy, it seems to recognize the educational efforts of the Internet routing community during the Biden Administration. The Trump EO preserves the requirements in Biden EO 14144 related to the protection of federal government communications from adversarial nations. Under the Biden EO, FCEB agencies are required to take steps to have all their Internet protocol (IP) address blocks and Autonomous System Numbers covered by a Registration Services Agreement with the American Registry for Internet Numbers or other regional registry. Agencies are required to update these registry records on an annual basis. Having federal agencies follow these best practices was a recommendation in the Office of the National Cyber Director's *Roadmap to Enhancing Internet Routing Security*, released in September 2024.

Under the Biden EO, NCD is required to recommend contract language to the Federal Acquisition Regulatory (FAR) Council to require Internet service providers deploy secure Internet routing technologies, including by publishing Route Origin Authorizations and validating Internet routes' Route Origin Validation. By October 15, 2025, the FAR Council is required to consider amending the FAR to adopt similar requirements. Pending that amendment, agencies "are encouraged to include such requirements in future contracts."

The Trump EO also preserves the requirement for FCEB agencies to encrypt Domain Name System (DNS) traffic. The Director of CISA was required to publish template contract language by April 15, which the FAR Council is required to use to amend the FAR. These requirements were still outstanding on June 6, 2025.

Encryption for Agency Communications

The Trump EO preserves the Biden requirement for the federal government to adopt the latest encryption protocols for email messages in transit. The Trump EO leaves in place the mandate that FCEB agencies enforce encrypted and authenticated transport for all connections between the agency's email clients and their email servers by May 16, 2025. It also leaves in place the directive for OMB to establish a requirement for expanded use of authenticated transport layer encryption between email servers used by FCEB agencies and for voice and video by July 15, 2025. Ninety days after that requirement is established, CISA is required to begin implementing directives and providing guidance to help FCEB agencies meet the requirement.

Post-Quantum Cryptography

The Trump EO "directs department and agency level actions on post-quantum cryptography to ensure protection against threats that may leverage next generation compute architectures." It builds on the Biden Administration National Security Memorandum 10 of May 4, 2022, *Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems* (NSM 10), which "directed the Federal Government to prepare for a transition to cryptographic algorithms that would not be vulnerable to a [Cryptanalytically Relevant Quantum Computer (CRQC)]."

Similar to the Biden EO, the Trump EO requires the NSA and CISA by December 1, 2025, to produce and "update a list of product categories in which products that support … PQC are widely available." The Trump EO maintains the requirement for agencies to support "Transport Layer Security protocol version 1.3 or a successor version" for National Security Systems (NSS) and non-NSS by January 2, 2030.

The Trump EO strikes requirements under the Biden EO for agencies to "implement PQC key establishment or hybrid key establishment … as soon as practicable" and for contract solicitations to include products that support PQC. However, the Trump EO preserves the goal of 2035 established by NSM 10 for the transition of cryptographic systems to PQC.

Artificial Intelligence

The Trump EO builds on previous Executive Orders on AI issued by President Trump, including the "Initial Rescissions of Harmful Executive Orders and Actions," which repealed the Biden AI EO of 2023, and "Removing Barriers to American Leadership in Artificial Intelligence" (Trump AI EO), which seeks to advance U.S. AI and economic competitiveness and national security. The Trump EO builds on the Administration's efforts to reframe AI policy around private sector innovation and further the adoption of AI within the federal government. Specifically, it refocuses AI "cybersecurity efforts towards identifying and managing vulnerabilities" and "automating cyber defense." It also seeks to "ensure existing datasets for cyber defense research have been made accessible to the broader academic research community" to the extent feasible.

By November 1, 2025, the Trump EO requires the Secretary of Defense, the Secretary of Homeland Security, and the Director of National Intelligence to work in coordination with the Office of Science and Technology Policy, the NCD, and the Director of OMB "to incorporate management of AI software vulnerabilities and compromises into … interagency coordination for vulnerability management through incident tracking, response, and reporting, and by sharing indicators of compromise for AI systems."

Aligning Policy to Practice

Consistent with Biden EO 14144, in consultation with the NCD, agencies are required to align investments with cybersecurity priorities to reduce cyber risk. By June 2028, the Director of OMB is required to "issue guidance … to address critical risks and adopt modern practices and architectures across Federal information systems and networks." Such guidance will include any necessary updates to OMB Circular A-130 *Managing Information as a Strategic Resource*.

Among the initiatives to be launched under Biden EO 14144 that were stricken by the Trump EO was high level direction on the use of digital identities, reflecting the Trump Administration's concerns over their use for public benefit fraud.

IoT Cyber Trust Mark

The Trump EO also maintains the June 6, 2026, deadline under Biden EO 14144 for the FAR Council to take steps to amend the FAR to require agencies to adopt a requirement for consumer Internet of Things (IoT) products to carry the Cyber Trust Mark label by January 4, 2027. Complying with the labeling deadline may be challenging for device manufacturers selling to agencies, due to delays in the Federal Communications Commission labeling program.

Sanctions to Combat Significant Malicious Cyber-Enabled Activities

To combat significant malicious cyber enabled activities, the Trump EO amends the Obama Administration EO 13694, "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities," and a series of subsequent orders. Such orders addressed the national emergency and threats to U.S. national security, foreign policy, and economic health and authorized the Treasury Department to impose economic sanctions on individuals and entities engaging in cyber activities that cause harm to critical infrastructure. The Trump EO redirects these orders at foreign persons rather than specific individuals to limit the application to foreign nationals and criminals that conduct cyber campaigns against the United States.

***

Overall, the Trump EO strikes significant portions of the lengthy narratives in Biden EO 14144, including some of the more prescriptive mandates. Although it does not make dramatic changes to U.S. cybersecurity policy, it terminates some Biden Administration lines of effort that the Trump Administration has deprioritized.

---

[1] Biden EO 14028 originally established the requirement for software attestations. OMB Memorandum M-22-18 *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices* (Sept. 14, 2022) established the requirement for a CISA Software Bill of Materials repository.

To stay informed on announcements from the Trump Administration, please visit our dedicated resource center below.

Wiley's Trump Administration Resource Center