JENNER & BLOCK

Client Alert: White House Narrows and Refocuses Biden Executive Order on Strengthening Federal Cybersecurity

Publications

June 12, 2025
By: Aaron R. Cooper, Shoba Pillay, Matt Pearl, Philip J. Chertoff

On June 6, 2025, President Donald J. Trump signed a new executive order on "Sustaining Select Efforts to Strengthen the Nation's Cybersecurity and Amending Executive Order 13694 and Executive Order 14144"[1] ("Trump Cyber EO"), which significantly narrows the scope and ambition of a Biden administration executive order focused on raising federal cybersecurity standards among federal vendors. However, the order retains certain key provisions raising internal cybersecurity standards within federal agencies and directing updated voluntary standards, guidance, and best practices for industry. Organizations doing business with the federal government should take note of these updates.

As noted by Jenner & Block in its prior analysis,[2] EO 14144 ("Biden Cyber EO") directed various parts of the federal government to adopt a laundry list of cybersecurity standards and contract requirements, ranging from enabling encrypted Domain Name System ("DNS") and communications systems to adopting products using post-quantum cryptography, and prioritized the acquisition of artificial intelligence cybersecurity tools and digital authentication methods.

The Trump Cyber EO adopts a tailored approach to amending the Biden Cyber EO, removing certain sections, revising others, and leaving some untouched.

Scaling Back Secure Software Development Practices, Advancing Federal Cloud and Civilian Space System Cybersecurity

- The Biden Cyber EO laid out a detailed process for developing new guidance on the secure software development practices outlined in NIST Special Publication 800–218 ("Secure Software Development Framework" or "SSDF") and established a new program for federal software providers to submit—in machine-readable format—attestations of their use of SSDF, and provide technical evidence of their compliance with these practices. While the accompanying fact sheet asserts that the Trump Cyber EO "directs the Federal government to advance secure software development,"[3] the Trump Cyber EO scraps the new attestation process in its entirety (though the

pre-existing process for submitting written attestations of compliance established under Biden administration EO 14028, Improving the Nation's Cybersecurity, remains intact).

- The Trump Cyber EO also terminates requirements to further incorporate updates to the SSDF into "the requirements of OMB Memorandum M-22-18 (Enhancing the Security of the Software Supply Chain through Secure Software Development Practices) or related requirements," thereby walking back prior efforts to mandate federal vendors' SSDF practices.

- The Trump Cyber EO nonetheless retains the directive to NIST to, in collaboration with an industry consortium, develop guidance on the "implementation of secure software development, security, and operations practices" based on the SSDF, update NIST Special Publication 800-53 to provide guidance on "how to securely and reliably deploy patches and updates," and develop and publish a preliminary update to the SSDF.

- The Trump Cyber EO continues several of the Biden Cyber EO's efforts to further mature cybersecurity for FedRAMP and federal cloud infrastructure. It retains the directive to the Director of FedRAMP to, in collaboration with CISA and NIST, "develop FedRAMP policies and practices to incentivize or require cloud service providers in the FedRAMP Marketplace 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." It also continues the tasking of NIST and CISA to develop guidelines for the secure management of access tokens and cryptographic keys used by cloud service providers; the FedRAMP Director to develop updated FedRAMP requirements incorporating these access token and cryptographic key guidelines; and the OMB Director to require FECB agencies to "follow best practices concerning the protection and management of hardware security modules, trusted execution environments, or other isolation technologies for access tokens and cryptographic keys used by cloud service providers in the provision of services to agencies."

- The Trump Cyber EO also continues the Biden Cyber EO efforts to advance civilian space system cybersecurity, retaining requirements for the Under Secretary of Commerce for Oceans and Atmosphere, the Administrator of the National Oceanic and Atmospheric Administration, and NASA Administrator to review "civil space contract requirements in the FAR [Federal Acquisition Regulations]," recommend to the FAR Council updates to civil space cybersecurity requirements and relevant contract language, and for the NCD to submit to OMB a study of space ground systems owned by civilian agencies and OMB to take steps to ensure these systems comply with its cybersecurity requirements.

Focuses Cybersecurity Defense and Sanctions Authorities on Foreign Adversaries

- The Trump Cyber EO reinforces the Biden Cyber EO's policy directive on hardening American defenses against foreign adversaries. The Biden EO generally described a need for enhanced defense against foreign adversarial countries and criminals and specifically called out the People's

Republic of China as the "most active and persistent" cyber threat to U.S. networks; the policy section of the Trump Cyber EO expands this list of threats to include Russia, Iran, and North Korea. The language about Russia is particularly significant, given conflicting reports in recent months about whether the Trump administration was treating Russia as a cyber threat actor.

- Notably, the Biden Cyber EO amended certain sanctions authorities granted to designate actors for malicious cyber-enabled activities, including unauthorized access or disruption to critical infrastructure or critical infrastructure-supporting computer networks, interference in election institutions and processes, ransomware, misappropriated intellectual property and confidential information, cyber-enabled intrusions, and sanctions evasion. While the Trump Cyber EO generally retains these authorities, it separately amends Executive Order 13694 to limit designation authority to only *foreign persons* (by replacing use of the terms "any person" with "any foreign person"). The fact sheet advises that this change "limits the application of cyber sanctions only to foreign malicious actors, preventing misuse against domestic political opponents and clarifying that sanctions do not apply to election-related activities."

Scales Back US Government Investment in Emerging Technologies and Novel Security Measures

- Despite the administration's public support for the adoption of, and investment in, artificial intelligence, the Trump Cyber EO similarly scales back pilot programs for the creation and government adoption of AI. The Trump EO retains requirements that existing datasets for cyber defense research be made maximally available to AI developers, and that agencies incorporate management of AI software vulnerabilities and compromises into existing vulnerability management practices. However, it drops the Biden Cyber EO's requirements that the Departments of Defense and Homeland Security launch a pilot for use of AI to enhance cyber defense of critical infrastructure in the energy sector, establish a program for use of AI models for cyber defense, support research on certain AI cybersecurity topics, and prioritize funding for the development of aforementioned large scale labeled datasets.

- The Trump Cyber EO also restricts efforts to advance the adoption of post-quantum cryptography ("PQC") within the federal government by canceling directives to begin solicitation and implementation of PQC algorithms, as well as efforts to begin outreach to foreign nations to adopt NIST-standardized algorithms. However, the Trump Cyber EO maintains the requirement for CISA to release a list of product categories with widely available products supporting post-quantum cryptography, as well as the directive to Defense and OMB to issue requirements to agencies to adopt Transport Layer Security Protocol version 1.3 or a successor.

- Citing fraud concerns and privacy risks, the new Trump Cyber EO similarly rescinds the Biden Cyber EO directives aimed at investing in and developing improved authentication and identity technologies and encouraging the adoption of digital identification documents and new validation services. It also eliminates requirements from the Biden EO for the federal civilian agencies to

begin using commercial phishing-resistant standards, and to expand use of authenticated transport-layer encryption between email services.

Generally Retains Efforts to Enhance Cybersecurity Practices at Federal Civilian Agencies

- The Trump Cyber EO retains, in its entirety, the Biden Cyber EO directive to OMB, NIST, and the Federal Acquisition Security Council to require agencies to comply with NIST Special Publication 800-161 (Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (SP 800-161 Revision 1)) and provide annual updates to OMB on its implementation. It also maintains the Biden Cyber EO's requirement that CISA, OMB, and the GSA issue joint recommendations to agencies on "the use of security assessments and patching of open-source software and best practices for contributing to open-source software projects."

- The Trump Cyber EO also retains the Biden Cyber EO's direction to agencies to comply with NIST-issued guidance on adopting cybersecurity supply chain risk management (*Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations* (SP 800–161 Revision 1)) and recommendations to agencies jointly issued by DHS and OMB "on the use of security assessments and patching of open source software and best practices for contributing to open source software projects."

- The Trump Cyber EO scales back the Biden Cyber EO's efforts to align investments and priorities in network visibility and security controls. The Trump Cyber EO retains the mandated issuance of guidance on federal information architecture and revisions to OMB Circular A-130 (Managing Information as a Strategic Resource), a pilot program of a "rules-as-code" approach for machine-readable versions of OMB, NIST, and CISA cybersecurity policies and guidance, and directed amendment of the FAR to require federal government contractors to carry United States Cyber Trust Mark labeling for their products. However, it cancels requirements for NIST to "identify minimum cybersecurity practices" based on common practices and control outcomes across industry, international standards bodies, and other risk management programs and to amend the FAR to require federal government contractors to follow these "minimum cybersecurity standards."

- Finally, the Trump EO cancels certain one-off directives, such as requirements to update guidance on Border Gateway Protocol (BGP) security.

Key Takeaways

- The Trump Cyber EO scraps one of the Biden Cyber EO's most consequential initiatives to require federal contractors to not just attest to compliance with secure software development practices, but provide proof, as well as other regulatory and contractual requirements to raise the cybersecurity standards of federal contractors. While federal software providers may be relieved of the near-term deadline to comply with these practices, overall industry trends, and recent False

Claims Act litigation related to failures to satisfy federal cybersecurity regulatory requirements, suggest it is likely prudent for federal contractors to continue to adopt and integrate federal secure software development practices and federal cybersecurity requirements, especially contractors operating in the federal cloud space.

- The Trump Cyber EO's removal of key provisions expanding investment and adoption of artificial intelligence for cyber defense and post-quantum cryptography is a dramatic turn from the administration's strong embrace of these emerging technologies as both national security and economic priorities. However, considering the administration is in the process of drafting a new action plan on AI, the rescission may also be an effort to clear out the previous administration's policymaking in these areas before issuing new policies and guidance on these topics to federal agencies.

- The administration's decision to retain key provisions requiring federal agencies to adopt cybersecurity best practices and technologies in a number of areas suggests that federal cybersecurity procurement will continue to be a growing business area for federal contractors, especially those involving the adoption of emerging technologies like artificial intelligence and quantum computing.

- Further, in some cases, the Trump Cyber EO's elimination of security requirements on departments and agencies may reflect a preference for being less operationally prescriptive in executive orders, rather than a directive to departments and agencies that they should not implement such practices. This is particularly relevant for technical requirements that federal contractors did not previously identify as burdensome, and that the administration did not associate with ideological priorities. Thus, federal software providers should thoughtfully examine instances in which they should continue offering products that would comply with the prior requirements in the Biden Cyber EO to the federal government.

Jenner & Block's pioneering Critical and Emerging Technologies Practice continues to monitor new developments regarding the regulation of artificial intelligence, quantum computing, and other critical and emerging technologies and is available to counsel clients on a broad range of related issues.

Aaron Cooper is founding co-chair of the firm's Critical and Emerging Technologies Practice, co-chair of the Cybersecurity and Data Privacy Practice, and a partner in the Investigations, Compliance, and Defense Practice. Shoba Pillay is co-chair of the Cybersecurity and Data Privacy Practice, co-chair of the National Security and Crisis Practice, and a partner in the Investigations, Compliance, and Defense Practice. Matt Pearl is of counsel in the Critical and Emerging Technologies Practice and the Communications, Internet, and Technology Practice. Philip Chertoff is an associate in the Critical and Emerging Technologies Practice and National Security and Crisis Practice.

Footnotes

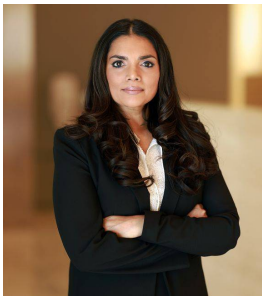
[1] Executive Order, *Sustaining Select Efforts to Strengthen the Nation's Cybersecurity and Amending Executive Order 13694 and Executive Order 14144*, (June 6, 2025), https://www.whitehouse.gov/presidential-actions/2025/06/sustaining-select-efforts-to-strengthen-the-nations-cybersecurity-and-amending-executive-order-13694-and-executive-order-14144/.

[2] Executive Order, *Executive Order on Strengthening and Promoting Innovation in the Nation's Cybersecurity*, (Jan. 16, 2025), https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2025/01/16/executive-order-on-strengthening-and-promoting-innovation-in-the-nations-cybersecurity/.

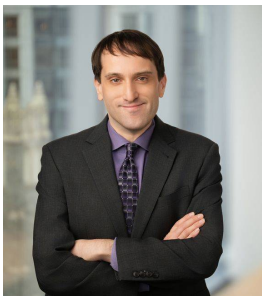
[3] Fact Sheet, *Fact Sheet: President Donald J. Trump Reprioritizes Cybersecurity Efforts to Protect America*, (June 6, 2025), https://www.whitehouse.gov/fact-sheets/2025/06/fact-sheet-president-donald-j-trump-reprioritizes-cybersecurity-efforts-to-protect-america/.

Related Attorneys

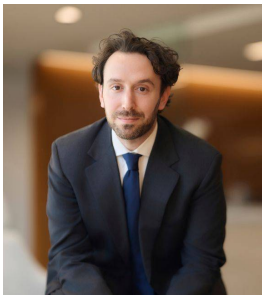
Aaron R. Cooper
Partner
acooper@jenner.com
+1 202 637 6333



Shoba Pillay
Partner
spillay@jenner.com
+1 312 923 2605



Matt Pearl
Of Counsel
mpearl@jenner.com
+1 202 639 6086



Philip J. Chertoff
Associate
pchertoff@jenner.com
+1 202 637 6346

Related Capabilities

Critical and Emerging Technologies

Data Privacy and Cybersecurity

National Security and Crisis

Stay Informed →