Trump Administration Cyber Executive Order Revises Prior Administrations' Requirements

Client Alert | 4 min read | 06.10.25

On June 6, 2025 President Trump signed an **Executive Order**, *Sustaining Select Efforts to Strengthen the Nation's Cybersecurity and Amending Executive Order 13694 and Executive Order 14144* (the "Trump Cyber EO"). The Trump Cyber EO rescinds and modifies select Biden administration guidance from EO 14144 covering several cybersecurity regimes, including digital identity verification, artificial intelligence, and secure software development practices, and it amends Obama administration guidance from EO 13694 authorizing sanctions on persons involved in malicious cyber activities. We have provided a summary of significant changes made by the Trump Cyber EO below.

Notable Trump Cyber EO Changes to EOs 14144 and 13694

- **CISA SSDF Attestation Requirements Are in Limbo.** EO 14144 built on prior Biden Administration Cybersecurity and Infrastructure Security Agency (CISA) Secure Software Development Framework (SSDF) guidance in EO 14028 and OMB Memorandums **M-22-18** and **M-23-16**—which require federal agencies to collect **SSDF attestation forms** from their software suppliers—by directing Federal Acquisition Regulation (FAR) amendments to standardize and enhance enforcement of the SSDF attestation process. The Trump Cyber EO removes the portions of EO 14144 requiring the SSDF FAR amendments but does not rescind EO 14028 or the relevant OMB Memorandums, leaving the future of SSDF attestation requirements unclear. The Trump Cyber EO does retain EO 14144 language requiring the National Institute of Standards and Technology (NIST) to update SSDF practices and relevant security standards, including NIST Special Publication 800-218, which may indicate that SSDF attestations are not being abolished entirely.

- **Post-Quantum Cryptography Requirements are Stripped Down.** EO 14144 directed several activities to encourage federal government adoption of products that support post-quantum cryptography (PQC). The Trump Cyber EO preserves EO 14144 mandates requiring CISA to compile a list of PQC-enabled products and for agencies to support Transport Layer Security protocol 1.3 (or a successor version) by 2030, but the Trump Cyber EO eliminates provisions directing the inclusion of PQC requirements in solicitations for certain products, agency PQC key establishment, and efforts to encourage key foreign partners to adopt NIST-standardized PQC algorithms.

- **Cyber Trust Mark and Machine-Readable Cyber Standard Requirements Remain in Place.** Trump's Cyber EO leaves intact two key technical measures from EO 14144, including the requirement to amend the FAR so that, by January 4, 2027, federal vendors of consumer IoT products must display the U.S. Cyber Trust Mark—a certification program launched by the previous administration to improve cybersecurity transparency and build consumer confidence. The order also preserves the directive to develop, within one year, a pilot program for a rules-as-code approach to develop machine-readable versions of cybersecurity policy and guidance issued by OMB, NIST, and CISA.

- **Reduced AI Cyber Defense and Threat Response Activities.** The Trump Cyber EO rescinds several provisions from Section 6 of EO 14144, aiming to refocus "AI cybersecurity efforts towards identifying and managing vulnerabilities, rather than censorship." Revoked measures include a pilot program to explore AI applications for securing critical infrastructure in the energy sector, a mandate for the Department of Defense to adopt advanced AI models for cyber defense, and the prioritization of federal research into secure AI design, the security of AI-generated code, and AI-assisted incident response. Notably, two Biden-era directives remain in place, including the release of existing federal cyber defense datasets to the broader research community and the incorporation of AI vulnerability management into DHS, DoD, and the Director of National Intelligence agency cybersecurity frameworks.

- **Digital Identity Verification Efforts are Scrapped.** Section 5 of EO 14144 proposed various measures to encourage adoption of and to standardize digital identity documentation to address "the use of stolen and synthetic identities by criminal syndicates to systemically defraud public benefits programs." The Trump Cyber EO removes Section 5 in its entirety.

- **EO 13694 Sanctions for Malicious Cyber Activity are Limited to "foreign persons" Only.** EO 13694 allowed the federal government to impose economic sanctions on "any person" it determined had engaged in cyber-enabled malicious activities, including misappropriation of trade secrets or other activities representing a serious threat to the United States' national security or economic health. The Trump Cyber EO limits the scope of EO 13694 sanctions to "any *foreign* person." The Trump Administration explained in a Fact Sheet that this change is intended to "prevent[] misuse against domestic political opponents and clarify[] that sanctions do not apply to election-related activities."

Key Takeaways

The Trump Cyber EO rescinds or modifies portions of previous administrations' EOs while leaving their overall frameworks mostly intact. As a result, it may take impacted federal agencies some time to parse which initiatives have been canceled and which remain in effect. Federal government software suppliers should pay close attention to updates from CISA and their customer agencies regarding the future of SSDF attestations, as the Trump Cyber EO rolls back select SSDF activities but does not appear to terminate the attestation process altogether.

Contacts

Michael G. Gruden
Partner
Washington, D.C. D | +1.202.624.2545
mgruden@crowell.com

Kate M. Growley
Partner, Crowell Global Advisors Senior Director
Washington, D.C. D | +1.202.624.2698
Washington, D.C. (CGA) D | +1 202.624.2500
kgrowley@crowell.com

Jacob Harrison
Associate
He/Him/His

Washington, D.C. D | +1.202.624.2533
jharrison@crowell.com

Caitlyn Weeks
Crowell Global Advisors Associate Consultant
Washington, D.C. (CGA) D | +1.202.654.2762
cweeks@ccrowellglobaladvisors.com

