
June 12, 2025

Trump's New Cyber Executive Order Preserves Many Cyber Initiatives, Rolls Back Security Requirements for Contractors, and Changes Cyber Sanctions Regime

On June 6, 2025, President Trump issued a new executive order that amends prior directives to “refocus[]” and “reprioritize[]” federal cybersecurity efforts.¹ Federal contractors and software vendors will be the most immediate beneficiaries of the new order’s shift away from regulatory expansion, including by rescinding certain software attestation requirements.

While the new order represents a significant departure from many elements of Executive Order 14144—which the Biden administration issued in its final days—it stops short of repealing the prior order in its entirety, in contrast to the Trump administration’s approach in other contexts.²

Instead, many provisions of the prior order remain in effect, and the blunt assessment of the threat environment remains largely the same: “The People’s Republic of China presents the most active and persistent cyber threat to United States Government, private sector, and critical infrastructure networks,” and “[m]ore must be done to improve the Nation’s cybersecurity against these threats.”³

Rolling Back Security Requirements for Government Contractors

The new order slashes many of the efforts in the prior order to use the federal procurement process to enhance software security—efforts that the Trump administration characterizes as “[i]mposing unproven and burdensome software accounting processes that prioritized compliance checklists over genuine security investments.”⁴

While maintaining the industry-friendly directive for NIST to collaborate with industry to develop guidance based on the Secure Software Development Framework, the new order eliminates provisions that would have required federal contractors to submit “secure software development attestations,” as well as plans for CISA and the National Cyber Director to verify those attestations, publish the results of those reviews, and, in the case of discrepancies, refer companies to the Department of

¹ The White House, *Fact Sheet: President Donald J. Trump Reprioritizes Cybersecurity Efforts to Protect America* (Jun. 6, 2025), available [here](#) (the “Fact Sheet”).

² See Paul, Weiss Client Alert: *White House Releases Executive Order to Strengthen and Promote Cybersecurity Innovation* (Jan. 17, 2025), available [here](#).

³ The White House, *Sustaining Select Efforts to Strengthen the Nation’s Cybersecurity and Amending Executive Order 13694 and Executive Order 14144*, § 2(a) (Jun. 6, 2025), available [here](#) (the “Order”); see Executive Order 14144 of January 16, 2025, 90 Fed. Reg. 6755, at § 1 (Jan. 17, 2025), available [here](#).

⁴ Fact Sheet.

Trump's New Cyber Executive Order Preserves Many Cyber Initiatives, Rolls Back Security Requirements for Contractors, and Changes Cyber Sanctions Regime

Justice.⁵ The new order also strikes a provision that would have required federal contractors to “follow applicable minimum cybersecurity practices” to be identified by NIST.⁶

Other Cuts: AI and Quantum Security, Digital IDs, and Federal Agency Security Requirements

The new order cuts many of the provisions related to the use of AI to bolster security, including testing AI to improve critical infrastructure cyber defenses, prioritizing federal research regarding the secure design of AI systems, and directing the Secretary of Defense to develop a program to use “advanced AI models for cyber defense.”⁷ However, in one area of continuity with the prior order, the new order requires NIST to work with other agency heads to, by November 1, 2025, “incorporate management of AI software vulnerabilities and compromises into their respective agencies’ existing processes and interagency coordination mechanisms for vulnerability management, including through incident tracking, response, and reporting, and by sharing indicators of compromise for AI systems.”⁸

The new order also cuts the previous administration’s efforts to accelerate the government’s adoption of post-quantum cryptography by requiring agencies and vendors to adopt quantum-resistant encryption; however, the directive leaves a requirement that CISA maintain “a list of product categories in which products that support post-quantum cryptography (PQC) are widely available.”⁹

Moreover, the new order strikes a provision in the prior order that encouraged the creation and adoption of digital identity documents to access public benefits programs that require identity verification.¹⁰ The order explains that the deleted provisions “risked widespread abuse by enabling illegal immigrants to improperly access public benefits” and, more broadly, constituted “inappropriate measures outside of core cybersecurity focus.”¹¹

Finally, the new directive rolls back several other requirements for federal agencies, including certain provisions regarding testing phishing-resistant authentication technologies, internet routing security, and email encryption.¹²

Narrowing Cyber Sanctions

The new order also narrows the cyber sanctions regime established in 2015 in Executive Order 13694 and that the prior order expanded.¹³ Specifically, the new order explicitly limits sanctions for cyber attacks on critical infrastructure to *foreign* persons, not domestic entities.¹⁴ According to the White House, these limitations are aimed at “preventing misuse against domestic political opponents,” as well as “clarifying that sanctions do not apply to election-related activities.”¹⁵

Cyber Trust Mark Program Survives

Of the Biden-era initiatives that are preserved under the new order, one of the more significant for the private sector is the FCC-administered U.S. Cyber Trust Mark program—a voluntary cybersecurity labeling program for “Internet of Things” products designed to help Americans make more informed choices about the cybersecurity of products they bring into their homes.

Conclusion

The June 6 executive order marks one of the Trump administration’s first major efforts to define its cybersecurity strategy. The order prioritizes technical rigor over policy expansion, refocuses sanctions on external threats, and retreats from federal digital identity initiatives. Even without secure software attestations and other regulatory requirements, however, NIST and other

⁵ Order at § 1(a); *see* Executive Order 14144 at § 2(a)–(b).

⁶ Order at § 2(f); *see* Executive Order 14144 at § 7(c)(i).

⁷ Order at § 2(e); *see* Executive Order 14144 at § 6.

⁸ Order at § 2(e); *see* Executive Order 14144 at § 6(e).

⁹ Order at § 2(d); *see* Executive Order 14144 at § 4(f).

¹⁰ Order at § 1(h); *see* Executive Order 14144 at § 5.

¹¹ Fact Sheet.

¹² *See* Order at § 1(c), (f), (g); *see* Executive Order 14144 at §§ 3(a)–(b), 4(b)(iv), 4(d)(ii)–(iii).

¹³ *See* Executive Order 13694 of April 1, 2015, 80 Fed. Reg. 18077 (Apr. 2, 2015), available [here](#); Executive Order 14144 at § 9.

¹⁴ Order at § 3.

¹⁵ Fact Sheet.

Trump's New Cyber Executive Order Preserves Many Cyber Initiatives, Rolls Back Security Requirements for Contractors, and Changes Cyber Sanctions Regime

federal agencies must still take dozens of actions, including developing updated guidance and standards to protect against foreign cyber threats. Organizations should keep abreast of evolving federal cyber policy and expect additional developments in this space as the administration fills key cyber leadership positions, including those of the National Cyber Director and CISA Director.

Trump's New Cyber Executive Order Preserves Many Cyber Initiatives, Rolls Back Security Requirements for Contractors, and Changes Cyber Sanctions Regime

* * *

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content. Questions concerning issues addressed in this memorandum should be directed to:

John P. Carlin

+1-202-223-7372

jcarlin@paulweiss.com

Katherine B. Forrest

+1-212-373-3195

kforrest@paulweiss.com

Roberto J. Gonzalez

+1-202-223-7316

rgonzalez@paulweiss.com

Anna R. Gressel

+1-212-373-3388

agressel@paulweiss.com

Elizabeth Hanft

+1-212-373-3664

ehanft@paulweiss.com

Mitchell D. Webber

+1-202-223-7359

mwebber@paulweiss.com

Peter Carey

+1-202-223-7485

pcarey@paulweiss.com

Audrey M. Paquet

+1-212-373-2397

apaquet@paulweiss.com

Associates Matthew J. Disler and Emily S. Shah contributed to this Client Memorandum.