New Executive Order Modifies Cybersecurity Requirements to Be Imposed on Federal Contractors and Subcontractors

JUNE 13, 2025

On June 6, 2025, President Donald Trump issued Executive Order (E.O.) 14306 to scale back a range of cybersecurity requirements and government-wide approaches implemented by the Biden Administration. The associated Fact Sheet (June 6 Fact Sheet) can be found here. Although E.O. 14306 rescinds certain Biden-era cybersecurity policies pertaining to federal contractors and subcontractors, several key restrictions remain in place.

Most important, the Defense Federal Acquisition Regulations requiring that defense contractors comply with 110 National Institute of Standards and Technology (NIST) security requirements for controlled unclassified information remain in effect. Moreover, the Department of Defense has nearly finalized an acquisition rule that will trigger implementation for the new Cybersecurity Maturity Model Certification (CMMC) Program published as a final rule last year. As described in prior WilmerHale alerts, here and here, this new CMMC program will require companies to assess (or in some cases have third parties assess) certain cybersecurity standards at progressively advanced levels depending on the type and sensitivity of the information they process, store or transmit.

As the Trump Administration continues to forge its approach to cybersecurity policies and standards, requirements affecting federal contractors and subcontractors may continue to change. E.O. 14306 signals what that approach is likely to be: removing requirements perceived as barriers to private sector growth and expansion while preserving key requirements that protect the U.S. government's own systems against cyber threats posed by China and other hostile foreign actors. These policy developments will require careful monitoring by government contractors and subcontractors to understand which requirements remain in place and how they are being monitored and enforced. This client alert outlines key changes made by E.O. 14306 to E.O. 13694 and E.O. 14144, and the implications for federal government contractors and subcontractors. Even though major removals include reversals on seeking government contractor attestations on cybersecurity standards and the implementation by agencies of digital identity verification technologies, certain technical requirements as implemented by agencies for federal government contractors still remain in place, such as requirements pertaining to internet protocol (IP) address blocks, Domain Name System (DNS) resolver systems and mandatory cybersecurity labeling.

I. Background

E.O. 14306 amends two prior orders: E.O. 13694, as previously amended, and E.O. 14144. E.O. 13694, which was signed by President Barack Obama on April 1, 2015, authorized sanctions on certain actors engaging in malicious cyber-related activities, such as harming or limiting critical infrastructure; certain commercial or economic crimes; or causing disruptions to the availability of computer networks. It was subsequently amended by several E.O.s, including E.O. 14144. On January 16, 2025, President Joe Biden issued E.O. 14144 directing agency heads to impose new requirements on federal contractors and subcontractors. Most notably, E.O. 14144 directed (1) agency heads to require software developers to attest to their cybersecurity practices for the Cybersecurity and Infrastructure Security Agency's (CISA) approval through CISA's Repository for Software Attestation and Artifacts (RSAA), (2) the Secretary of Homeland Security to regularly update a list with product categories supporting post-quantum cryptography (PQC) and (3) the director of the Office of Management and Budget (OMB) to issue federal government-wide guidance to align cybersecurity priorities among agencies.

E.O. 14306 significantly alters E.O. 14144, repealing portions of it, changing others and leaving still others in place.

II. Scaling Back E.O. 14144 and Modifying E.O. 13694

Described as a "reprioritizing" of cybersecurity efforts, E.O. 14306 revokes key provisions of E.O. 14144, which the Trump Administration characterized in its June 6 Fact Sheet as "micromanag[ing] technical cybersecurity decisions better handled at the department and agency level."

Key removals include:

- *Attestations and Artifacts Requirements*: E.O. 14306 removed the Biden-era requirement for federal contractors and subcontractors providing computer software to submit validated attestations and artifacts regarding secure development practices, in line with NIST Special Publication 800-218 (Secure Software Development Framework (SSDF)), through CISA's RSAA. Whereas E.O. 14144 also required updates to the SSDF to be incorporated into OMB Memorandum M-22-18 (Enhancing the Security of the Software Supply Chain through Secure Software Development Practices), E.O. 14306 calls only for a preliminary update to the SSDF, while retaining the original directive to establish a consortium with industry at the National Cybersecurity Center of Excellence to develop the guidance updates. The June 6 Fact Sheet explains that the attestations were "[i]mposing unproven and burdensome software accounting processes that prioritized compliance checklists over genuine security investments." Overall, this reorientation appears intended to put industry more in the lead in developing software validation practices rather than the federal government.
- *Digital Identity Verification Systems*: E.O. 14144 directed federal agencies to encourage the acceptance of digital identity documents to access public benefits programs that require identity verification. The requirement's stated purpose was to address "[t]he use of stolen and synthetic identities by criminal syndicates to systematically defraud public benefits programs[.]" However, according to the June 6 Fact Sheet, the Trump Administration said

the “digital identity mandat[e]” risks “widespread abuse by enabling illegal immigrants to improperly access public benefits” and consequently struck this section entirely. Similarly, provisions requiring the prioritization of investments in “innovative identity technologies,” including pilot programs using commercial phishing resistant standards such as WebAuthn, are removed.

Certain other provisions from E.O. 14144 are scaled back or modified. For example, the E.O.:

- Modifies the policy statement to expressly name the People’s Republic of China as the “most active and persistent threat to United States Government, private sector, and critical infrastructure networks” as well as identify the “significant threats” emanating from “Russia, Iran, North Korea, and others who undermine United States cybersecurity”;
- Removes references to presidential direction of agency use of Border Gateway Protocol (BGP) security methods for routing information and security;
- Retains some standards for technical enforcement of encrypted and authenticated transport for electronic communications, while removing provisions directing requirements for agencies to expand the use of authenticated transport layer encryption;
- Retains the requirement for federal agencies to update a list of product categories containing products that support PQC, but removes requirements for such products to be included in solicitations;
- Modifies the section on promoting security with and in artificial intelligence (AI) to remove prioritization of the use of AI for the development of cyber defense, including by eliminating a pilot program involving collaboration with private-sector critical infrastructure entities on the use of AI to enhance cyber defense of critical infrastructure in the energy sector; a directive to the Secretary of Defense to establish a program to use advanced AI models for cyber defense; and a directive to prioritize AI research on defensive cyber analysis, security of AI coding assistance, and methods of designing secure AI systems. However, directives on sharing information on existing cyber defense research remain, as does a directive for interagency coordination for management of AI software vulnerability. The Trump Administration characterized this re-prioritization in the June 6 Fact Sheet as refocusing AI cybersecurity efforts “towards identifying and managing vulnerabilities, rather than censorship”; and
- Scales back details for what should be included in guidance revisions to OMB Circular A-130 to address critical risks and adopt modern practices and architectures across federal information systems and networks. The new E.O. also removes a requirement for NIST to evaluate common cybersecurity practices across industry sectors, international standards bodies and other risk management programs to issue minimum cybersecurity practices guidance and subsequently establish a requirement for contractors and subcontractors to follow those applicable minimum cybersecurity practices.

The E.O. notably retains the requirement for the Federal Acquisition Regulation (FAR) Council to amend the FAR to require vendors of the federal government of Internet of Things products to carry US Cyber Trust Mark labeling for those products.

Finally, E.O. 14306 further amends E.O. 13694, which authorized the imposition of sanctions related to malicious cyber-enabled activities originating from, or directed by, persons located outside the United States. Whereas E.O. 13694 originally imposed both asset-blocking sanctions and visa entry restrictions for "any person" determined by the Secretary of the Treasury to meet certain criteria for malicious cyber-related activities, including US citizens, E.O. 14306 amends this authority to be restricted to sanction only "any foreign person"—a notable alteration. The June 6 Fact Sheet framed the change as "preventing misuse against domestic political opponents and clarifying that sanctions do not apply to election-related activities."

III. Non-Modified Requirements and Obligations From E.O. 14144

While several provisions of E.O. 14144 lose their bite following E.O. 14306, several other provisions remain in their original form. Still intact, for example, is E.O. 14144's requirement that federal agencies ensure that assigned internet number resources, such as IP address blocks and Autonomous System Numbers will be covered by a Registration Services Agreement with the American Registry for Internet Numbers or an analogous internet registry. Also unchanged is E.O. 14144's directive that the National Cyber Director recommend contract language to the FAR Council to require contracted providers of internet services to federal agencies to adopt and deploy internet routing security technologies, including publishing Route Origin Authorizations and performing Route Origin Validation filtering.

Similarly without alteration is E.O. 14144's mandate for the Secretary of Homeland Security to publish template contract language requiring any system acting as a DNS resolver for the federal government to support encrypted DNS. Systems acting as a DNS allow internet routing by authoring IP addresses from domain names. When lacking encryption or proper maintenance to secure them, DNSs are prone to discoverable vulnerabilities.

Also unchanged is E.O. 14144's directive for the federal government to deploy commercial security technologies and architectures, such as hardware security modules, trusted execution environments and other isolation technologies, to protect and audit access to cryptographic keys with extended life cycles.

Finally, the new E.O. does not change existing directives to review and update space system cybersecurity policies, such as on debilitating impact systems.

Conclusion

Although E.O. 14306 has scaled back several notable compliance obligations and requirements that were previously imposed on federal contractors and subcontractors, key standards remain and will continue to affect federal contractors and subcontractors going forward. Notable among the persistent requirements are, in particular, PQC requirements and the requirement for government vendors to label their Internet of Things products with the US Cyber Trust Mark.

More broadly, E.O. 14306 offers a helpful guide for how the federal government's cybersecurity standards are likely to evolve and what contractors and subcontractors should be considering in evaluating their own cybersecurity systems.

Authors

Benjamin A. Powell

PARTNER

Co-Chair, Cybersecurity and Privacy Practice

Co-Chair, Artificial Intelligence Practice

benjamin.powell@wilmerhale.com

+1 202 663 6770

Barry J. Hurewitz

PARTNER

barry.hurewitz@wilmerhale.com

+1 202 663 6089

Joshua A. Geltzer

PARTNER

joshua.geltzer@wilmerhale.com

+1 202 663 6404

Arianna Evers

PARTNER

arianna.evers@wilmerhale.com

+1 202 663 6122

Shervin Z. Taheran

ASSOCIATE

shervin.taheran@wilmerhale.com

+1 202 663 6268

Maria I. Kanevsky

ASSOCIATE

maria.kanevsky@wilmerhale.com

+1 617 526 6298