

Executive Order 14306—Sustaining Select Efforts To Strengthen the Nation's Cybersecurity and Amending Executive Order 13694 and Executive Order 14144
June 6, 2025

By the authority vested in me as President by the Constitution and the laws of the United States of America, including the International Emergency Economic Powers Act (50 U.S.C. 1701 *et seq.*), the National Emergencies Act (50 U.S.C. 1601 *et seq.*), section 212(f) of the Immigration and Nationality Act of 1952 (8 U.S.C. 1182(f)), and section 301 of title 3, United States Code, it is hereby ordered:

Section 1. Amendments to Executive Order 14144. Executive Order 14144 of January 16, 2025 (Strengthening and Promoting Innovation in the Nation's Cybersecurity), is hereby amended by:

- (a) striking subsections 2(a)–(b) and redesignating subsections 2(c), 2(d), and 2(e) as subsections 2(a), 2(b), and 2(c), respectively;
- (b) striking the first sentence of subsection 2(e);
- (c) striking subsections 3(a)–(b) and redesignating subsections 3(c), 3(d), and 3(e) as subsections 3(a), 3(b), and 3(c), respectively;
- (d) striking from subsection 3(c) the phrase "In Executive Order 14028, I directed the Secretary of Defense and the Secretary of Homeland Security to establish procedures to immediately share threat information to strengthen the collective defense of Department of Defense and civilian networks.";
- (e) striking from subsection 3(c)(i)(A) the word "novel";
- (f) striking subsection 4(b)(iv);
- (g) striking subsections 4(d)(ii)–(iii);
- (h) striking section 5 and redesignating sections 6, 7, 8, 9, 10, and 11 as sections 5, 6, 7, 8, 9, and 10, respectively; and
- (i) striking from subsection 8(c) the phrase "in the areas of intrusion detection, use of hardware roots of trust for secure booting, and development and deployment of security patches.".

Sec. 2. Further Amendments to Executive Order 14144. Executive Order 14144 is hereby amended by:

- (a) striking section 1 and inserting, in lieu thereof, the following:

"Section 1. Policy. Foreign nations and criminals continue to conduct cyber campaigns targeting the United States and Americans. The People's Republic of China presents the most active and persistent cyber threat to United States Government, private sector, and critical infrastructure networks, but significant threats also emanate from Russia, Iran, North Korea, and others who undermine United States cybersecurity. These campaigns disrupt the delivery of critical services across the Nation, cost billions of dollars, and undermine Americans' security and privacy. More must be done to improve the Nation's cybersecurity against these threats. I am ordering additional actions to improve our Nation's cybersecurity, focusing on defending our digital infrastructure, securing the services and capabilities most vital to the digital domain, and building our capability to address key threats.";

(b) striking subsection 2(c) and inserting, in lieu thereof, the following:

"(c) Relevant executive departments and agencies (agencies) shall take the following actions:

(i) By August 1, 2025, the Secretary of Commerce, acting through the Director of NIST, shall establish a consortium with industry at the National Cybersecurity Center of Excellence to develop guidance, informed by the consortium as appropriate, that demonstrates the implementation of secure software development, security, and operations practices based on NIST Special Publication 800–218 (Secure Software Development Framework (SSDF)).

(ii) By September 2, 2025, the Secretary of Commerce, acting through the Director of NIST, shall update NIST Special Publication 800–53 (Security and Privacy Controls for Information Systems and Organizations) to provide guidance on how to securely and reliably deploy patches and updates.

(iii) By December 1, 2025, the Secretary of Commerce, acting through the Director of NIST, in consultation with the heads of such agencies as the Director of NIST deems appropriate, shall develop and publish a preliminary update to the SSDF. This preliminary update shall include practices, procedures, controls, and implementation examples regarding the secure and reliable development and delivery of software as well as the security of the software itself. Within 120 days of publishing the preliminary update, the Secretary of Commerce, acting through the Director of NIST, shall publish a final version of the updated SSDF.";

(c) striking from subsection 4(b) the phrase "The security of Internet traffic depends on data being correctly routed and delivered to the intended recipient network. Routing information originated and propagated across the Internet, utilizing the Border Gateway Protocol (BGP), is vulnerable to attack and misconfiguration." and inserting, in lieu thereof, the following:

"Relevant agencies shall take the following actions:";

(d) striking subsection 4(f) and inserting, in lieu thereof, the following:

"(f) A quantum computer of sufficient size and sophistication—also known as a cryptanalytically relevant quantum computer (CRQC)—will be capable of breaking much of the public-key cryptography used on digital systems across the United States and around the world. National Security Memorandum 10 of May 4, 2022 (Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems), directed the Federal Government to prepare for a transition to cryptographic algorithms that would not be vulnerable to a CRQC.

(i) By December 1, 2025, the Secretary of Homeland Security, acting through the Director of the Cybersecurity and Infrastructure Security Agency (CISA), and in consultation with the Director of the National Security Agency, shall release and thereafter regularly update a list of product categories in which products that support post-quantum cryptography (PQC) are widely available.

(ii) By December 1, 2025, to prepare for transition to PQC, the Director of the National Security Agency with respect to National Security Systems (NSS), and the Director of OMB with respect to non-NSS, shall each issue requirements for agencies to support, as soon as practicable, but not later than January 2, 2030, Transport Layer Security protocol version 1.3 or a successor version.";

(e) striking former section 6 (newly designated section 5) and inserting, in lieu thereof, the following:

"Sec. 5. Promoting Security with and in Artificial Intelligence. Artificial intelligence (AI) has the potential to transform cyber defense by rapidly identifying vulnerabilities, increasing the scale of threat detection techniques, and automating cyber defense.

(a) By November 1, 2025, the Secretary of Commerce, acting through the Director of NIST; the Secretary of Energy; the Secretary of Homeland Security, acting through the Under Secretary for Science and Technology; and the Director of the National Science Foundation shall ensure that existing datasets for cyber defense research have been made accessible to the broader academic research community (either securely or publicly) to the maximum extent feasible, in consideration of business confidentiality and national security.

(b) By November 1, 2025, the Secretary of Defense, the Secretary of Homeland Security, and the Director of National Intelligence, in coordination with appropriate officials within the Executive Office of the President, to include officials within the Office of Science and Technology Policy, the Office of the National Cyber Director, and the Director of OMB, shall 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.";

(f) striking section 7 and inserting, in lieu thereof, the following:

"Sec. 7. Aligning Policy to Practice. Agencies' policies must align investments and priorities to improve network visibility and security controls to reduce cyber risks. In consultation with the National Cyber Director, agencies shall take the following actions:

(a) Within 3 years of the date of this order, the Director of OMB shall issue guidance, including any necessary revision to OMB Circular A–130, to address critical risks and adapt modern practices and architectures across Federal information systems and networks.

(b) Within 1 year of the date of this order, the Secretary of Commerce, acting through the Director of NIST; the Secretary of Homeland Security, acting through the Director of CISA; and the Director of OMB shall establish a pilot program of a rules-as-code approach for machine-readable versions of policy and guidance that OMB, NIST, and CISA publish and manage regarding cybersecurity.

(c) Within 1 year of the date of this order, agency members of the FAR Council shall, as appropriate and consistent with applicable law, jointly take steps to amend the FAR to adopt requirements for agencies to, by January 4, 2027, require vendors to the Federal Government of consumer Internet-of-Things products, as defined by 47 CFR 8.203(b), to carry United States Cyber Trust Mark labeling for those products."; and

(g) striking subsection 8(a) and inserting, in lieu thereof, the following:

"(a) Except as specifically provided for in subsection 4(f) of this order, sections 1 through 7 of this order shall not apply to Federal information systems that are NSS or are otherwise identified by the Department of Defense or the Intelligence Community as debilitating impact systems."

Sec. 3. Amendments to Executive Order 13694. Executive Order 13694 of April 1, 2015 (Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities), as amended by Executive Order 13757 of December 28, 2016 (Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities), Executive Order 13984 of January 19, 2021 (Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities), and Executive Order 14144, is hereby further amended by:

(a) striking from subsection 1(a)(ii) the phrase "any person" and inserting in lieu thereof "any foreign person"; and

(b) striking from subsection 1(a)(iii) the phrase "any person" and inserting in lieu thereof "any foreign person."

Sec. 4. General Provisions. (a) Nothing in this order shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department or agency, or the head thereof; or

(ii) the functions of the Director of OMB relating to budgetary, administrative, or legislative proposals.

(b) This order shall be implemented in a manner consistent with applicable law and subject to the availability of appropriations.

(c) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

(d) The costs for publication of this order shall be borne by the Department of Homeland Security.

DONALD J. TRUMP

The White House,
June 6, 2025.

[Filed with the Office of the Federal Register, 11:15 a.m., June 10, 2025]

NOTE: This Executive order was published in the *Federal Register* on June 11.

Categories: Executive Orders : Cybersecurity, strengthening efforts.

Subjects: Artificial intelligence and other emerging technologies; Cybersecurity and Infrastructure Security Agency; Cybersecurity, strengthening efforts; Director of National Intelligence; National Institute of Standards and Technology; National Science Foundation; National Security Agency; Office of Management and Budget; Office of Science and Technology Policy; Secretary of Commerce; Secretary of Defense; Secretary of Energy; Secretary of Homeland Security; Under Secretary of Homeland Security for Science and Technology.

DCPD Number: DCPD202500669.