EXECUTIVE ORDER
14412
- - - - - - -

SECURING THE NATION AGAINST ADVANCED CRYPTOGRAPHIC ATTACKS

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered:

Section 1. Background and Policy. The advent of large-scale quantum computers, particularly in the hands of adversaries, will pose a significant threat to widely used cryptographic security systems. Ongoing cyber activity against our Nation also presents the risk of adversaries collecting United States information now, and decrypting it later once large-scale quantum computers are operational. In light of these threats, the United States must take steps to strengthen cryptographic protections for the Nation's sensitive data, critical infrastructure, and digital economy.

It is the policy of the United States to safeguard national security and maintain technological leadership by responsibly and effectively executing the transition of Federal information systems to National Institute of Standards and Technology (NIST)-approved Federal Information Processing Standards (FIPS) for Post-Quantum Cryptography (PQC), and to assist critical infrastructure owners and operators with their transitions.

Sec. 2. Definitions. For purposes of this order:

(a) the term "agency" has the same meaning as it has in 44 U.S.C. 3502(1);

(b) the term "critical infrastructure" has the same meaning as it has in section 1016(e) of the USA Patriot Act of 2001 (42 U.S.C. 5195c(e));

(c) the term "high impact system" means an information system in which at least one security objective (i.e.,

confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of "high";

(d) the term "high value asset" or "HVA" means Federal information or a Federal information system designated as a high value asset under Office of Management and Budget (OMB) Memorandum M-19-03, "Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program," or any successor document;

(e) the term "information systems" has the same meaning as it has in 6 U.S.C. 650(14);

(f) the term "National Security Systems" has the same meaning as it has in 44 U.S.C. 3552(b)(6);

(g) the term "post-quantum cryptography" or "PQC" means those cryptographic algorithms or methods that are designed to be resistant to attack by both a quantum computer and a classical computer;

(h) the term "PQC migration lead" means the agency employee or detailee who reports to the agency's chief information officer and is responsible for overseeing agency-wide cryptographic inventory management, developing a prioritized PQC migration plan, and coordinating cross-agency efforts in PQC;

(i) the term "Cryptographic Module Validation Program" has the same meaning as it has in FIPS 140-3, "Security Requirements for Cryptographic Modules," or any successor policy;

(j) the term "digital signature" has the same meaning as it has in FIPS 186-5, "Digital Signature Standard (DSS)," or any successor policy; and

(k) the term "key establishment" has the same meaning as it has in FIPS 203, "Module-Lattice-Based Key-Encapsulation Mechanism Standard," or any successor policy.

Sec. 3. Coordinating the PQC Transition. (a) The Director of OMB and the National Cyber Director, in consultation with the Assistant to the President for National Security Affairs and the Administrator of the Office of Electronic Government, OMB, shall lead the strategic coordination and oversight of the national PQC migration policy and strategy set forth in this order, ensuring its alignment with broader cybersecurity goals.

(b) The Secretary of Commerce, through the Director of NIST, and in consultation with the Director of the National Security Agency (NSA) and the Secretary of Homeland Security, through the Director of the Cybersecurity and Infrastructure Security Agency (CISA), shall provide agencies on an ongoing basis with comprehensive technical guidance on PQC implementation, including best practices in implementation and risk management strategies.

Sec. 4. Accelerating the PQC Transition. (a) Within 30 days of the date of this order, each agency head shall identify its PQC migration lead and provide the name and contact details of the PQC migration lead to the Director of OMB and the National Cyber Director.

(b) Within 90 days of the date of this order, the Director of OMB shall, in consultation with the Secretary of Homeland Security through the Director of CISA and the National Cyber Director, and consistent with 6 U.S.C. 1526(c), issue guidance requiring each agency to:

(i) review their inventory of HVAs and high impact systems, excluding National Security Systems;

(ii) transition all HVAs and high impact systems to use PQC for key establishment by December 31, 2030;

(iii) transition all HVAs and high impact systems to

use PQC for digital signatures by December 31, 2031; and

(iv) develop and submit to the Director of OMB and the National Cyber Director a plan to accomplish this directive.

(c) Within 180 days of the date of this order, the Secretary of Commerce, through the Director of NIST, shall initiate a pilot project for PQC migration on an appropriate subset of information systems owned or operated by NIST, to be completed no later than December 31, 2027.

Sec. 5. Leading the PQC Transition. (a) All agencies that serve as Sector Risk Management Agencies, as defined by the National Security Memorandum 22 of April 30, 2024 (Critical Infrastructure Security and Resilience) or its successor, shall work with the Department of Homeland Security through the Director of CISA to assist critical infrastructure owners and operators in developing their PQC migration plans.

(b) The Secretary of State shall work with the Director of NIST, the Secretary of Homeland Security, the National Cyber Director, the Secretary of War, and the Director of National Intelligence (DNI) to identify and engage foreign governments and industry groups in key countries to encourage their transition to PQC algorithms standardized by NIST.

(c) Within 180 days of the date of this order and annually thereafter until PQC migration is complete, the Director of the NSA, in his capacity as the National Manager for National Security Systems, shall submit a report to the President, through the Committee on National Security Systems, on the status of PQC migration for agencies that own or operate National Security Systems.

(d) Within 270 days of the date of this order, the

Secretary of Homeland Security, through the Director of CISA, and in coordination with the Director of NIST, shall release public guidance describing the agencies' considered view as to the minimum elements for a cryptographic bill of materials. These elements shall enable the automated assessment of the cryptographic assets utilized by a hardware or software element.

Sec. 6. Procurement. (a) The Director of OMB, the Secretary of War, the Administrator of National Aeronautics and Space Administration, and the Administrator of General Services, in consultation with the Secretary of Homeland Security, the DNI, and the Director of NIST, shall coordinate efforts to identify cost-saving opportunities in implementing the national PQC migration policy and strategy, such as migration of cloud-based technologies, shared procurement of PQC tools, joint training programs, and centralized technical support.

(b) Within 180 days of the date of this order, the Secretary of Commerce, through the Director of NIST, shall, to the extent appropriate and consistent with applicable law, revise the processes used by the Cryptographic Module Validation Program to accelerate validations of cryptographic modules.

(c) Within 180 days of the date of this order, the Federal Acquisition Regulatory Council (FAR Council), in consultation with the Secretary of Homeland Security through the Director of CISA and the Director of NIST, shall publish a proposed rule amending the Federal Acquisition Regulation (FAR) to require covered contractors to comply by December 31, 2030, with NIST's FIPS, including all applicable FIPS incorporating PQC compliant algorithms.

(d) Within 270 days of the date of this order, the FAR Council, in consultation with the Secretary of Homeland Security through the Director of CISA and the Director of NIST, shall

publish a proposed rule amending the FAR requirements and contract clauses for contractor vulnerability disclosure programs to ensure that covered contractors implement vulnerability disclosure policies (VDPs), consistent with NIST guidelines, and that VDPs incorporate reports of cryptographic vulnerabilities, including testing for lack of encryption and the use of non-FIPS approved algorithms.

Sec. 7. 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 the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(b) This order shall be implemented 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 Commerce.

THE WHITE HOUSE,

June 22, 2026.

[FR Doc. 2026-12909 Filed: 6/24/2026 11:15 am; Publication Date: 6/25/2026]