

National Security Presidential Memorandum on National Policy for the Cybersecurity of National Security Systems

June 12, 2026

National Security Presidential Memorandum/NSPM–12

Memorandum for the Vice President, the Secretary of State, the Secretary of the Treasury, the Secretary of War, the Attorney General, the Secretary of the Interior, the Secretary of Agriculture, the Secretary of Commerce, the Secretary of Labor, the Secretary of Health and Human Services, the Secretary of Housing and Urban Development, the Secretary of Transportation, the Secretary of Energy, the Secretary of Education, the Secretary of Veterans Affairs, the Secretary of Homeland Security, the White House Chief of Staff, the Deputy Chief of Staff for Policy and Homeland Security Advisor, the Director of the Office of Management and Budget, the Director of National Intelligence, the Assistant to the President for Science and Technology, the Assistant to the President for National Security Affairs, the Assistant to the President and Counsel to the President, the Chairman of the Joint Chiefs of Staff, the Director of the Central Intelligence Agency, the Director of the National Security Agency, the Administrator of General Services, the National Cyber Director, the Director of the Cybersecurity and Infrastructure Security Agency

Subject: National Policy for the Cybersecurity of National Security Systems

As President, it is my priority to ensure that the United States can conduct key military and intelligence missions in contested cyber environments and that our personnel have access to the modern, secure technology they need to accomplish these missions. The Department of War (DOW), Intelligence Community (IC), and Federal Civilian Executive Branch (FCEB) Agencies own or operate this technology as National Security Systems (NSS). It shall be the policy of the United States Government that these systems be defended to the greatest extent practicable and that executive department and agency (agency) heads be accountable for this defense through government-wide oversight mechanisms. Therefore, by the authority vested in me by the Constitution and the laws of the United States, including section 3557 of title 44, United States Code, and section 301 of title 3, United States Code, it is hereby ordered:

Section 1. Purpose. (a) This National Security Presidential Memorandum sets forth principles and establishes cybersecurity governance for NSS. It further details the governance structure of the Committee on National Security Systems (CNSS) and the role of the Director, National Security Agency (NSA) as the National Manager for NSS.

(b) This memorandum further sets forth requirements for NSS that are equivalent to or exceed the cybersecurity requirements for other Federal Information Systems set forth within Executive Order 14306 of June 6, 2025 (Sustaining Select Efforts to Strengthen the Nation's Cybersecurity and Amending Executive Order 13694 and Executive Order 14144).

Sec. 2. Policy. (a) National Security Directive 42 (NSD–42) of July 5, 1990 (National Policy for the Security of National Security Telecommunications and Information Systems) and National Security Memorandum 8 (NSM–8) of January 19, 2022 (Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems) are hereby rescinded.

(b) It shall be the policy of the United States Government to foster a proactive, adaptive, and resilient cybersecurity ecosystem for all NSS to better safeguard the Nation against persistent cyber threats from sophisticated adversaries. To this end, this memorandum establishes a clear

structure of authorities, roles, and responsibilities for the governance of NSS as well as accountability for owners and operators of NSS. This memorandum shall:

- (i) enhance national cyber defense governance and accountability and re-establish and designate clear governance roles and scope of authorities for the CNSS;
- (ii) re-establish and empower a National Manager for NSS to identify emerging threats, advise the CNSS, issue emergency directives, provide authoritative minimum requirements for cryptology and cryptographic systems, and, through the CNSS, direct technical solutions for separation of classification levels (whether between systems or on the same system);
- (iii) foster collaboration, standardization, and efficient resource management by promoting coordination and information sharing across agencies, public-private partnerships, and international liaison activities; and
- (iv) promote efficient use of taxpayer funds in securing NSS.

Sec. 3. The Committee on National Security Systems. (a) The Committee on National Security Systems (CNSS) is re-established to enhance accountability and coordination across the DOW, the IC, and FCEB Agencies in implementing necessary cyber defenses on all NSS. The CNSS shall operate under the coordination of a member of the National Security Council (NSC) staff, who shall serve as Chair.

(i) The CNSS members shall consist of:

- (A) the Secretary of War, acting through the DOW Chief Information Officer (CIO);
- (B) the Director of National Intelligence (DNI), acting through the IC CIO;
- (C) the Director of the Office of Management and Budget (OMB), acting through the Federal CIO; and
- (D) the Director of the NSA as National Manager, acting through the Deputy National Manager.

(ii) The following officials may recommend representatives as advisors to the members of the CNSS:

- (A) the Attorney General;
- (B) the Secretary of Commerce;
- (C) the Director of the Central Intelligence Agency (CIA);
- (D) the Assistant to the President for National Security Affairs;
- (E) the Assistant to the President for Science and Technology;
- (F) the National Cyber Director;
- (G) the Chairman of the Joint Chiefs of Staff;
- (H) the Director of the Cybersecurity and Infrastructure Security Agency (CISA); and
- (I) any other advisors as the CNSS deems necessary.

(b) The objectives of the CNSS shall be to:

- (i) establish baseline cybersecurity requirements for all NSS;

- (ii) through the respective statutory and delegated authorities held by the members, hold NSS owners and operators accountable for implementing required security measures;
- (iii) represent the requirements of the NSS ecosystem, owners, and operators in interagency fora, public fora, the Congress, and the Council of Inspectors General on Integrity and Efficiency;
- (iv) coordinate with NSS shared service providers to promote efficient use of secure shared services where practicable; and
- (v) facilitate a shared platform or forum for dissemination and access to CNSS guidance and decisions, NSS requirements, and related policies, accessible by all NSS end-user IC, DOW, and FCEB Agencies.

(c) The CNSS, acting through its members consistent with section 301 of title 3, United States Code, shall issue directives and complementary standards that apply to all NSS, including directives and standards issued under subsections (c)(i) and (c)(ii) of this section. The agencies that own or operate NSS shall comply with all directives and complementary standards issued by the CNSS.

(i) For the purposes of safeguarding NSS from a known or reasonably suspected information security threat, vulnerability, or risk, the CNSS may issue a directive to the head of an agency, through that agency's CIO, Chief Information Security Officer (CISO), or other officer designated by the head of the agency, to take any lawful action with respect to the operation of that NSS for the purpose of protecting the system from, or mitigating, the threat, vulnerability, or risk.

(ii) NSS shall meet or exceed the protection level of cybersecurity standards issued by the National Institute of Standards and Technology (NIST) unless the CNSS provides otherwise.

(A) The CNSS may issue a complementary standard to adapt NIST-prescribed baselines for NSS where appropriate.

(B) CNSS Policy (CNSSP) 15, or successor policy, or interim guidance from the National Manager, will constitute the commercial cryptographic standard for NSS.

(C) Unless specifically stated by the CNSS or a complementary CNSS issuance exists, all relevant standards issued by NIST shall apply as a minimum baseline to secure NSS.

(d) The CNSS shall have a permanent Executive Secretariat composed of personnel provided by the National Manager. The National Manager shall further provide facilities and support as required. Other agencies shall provide facilities and support as requested by the CNSS, consistent with applicable law.

(i) The Secretary of War, through the DOW CIO, in coordination with the DNI, through the IC CIO, shall be responsible for overseeing the activities of the Executive Secretariat.

(ii) The Executive Secretariat shall be responsible for maintaining an authoritative, machine-readable portal of CNSS guidance applicable to NSS as well as a collaborative environment that is accessible by all NSS owners and operators on Unclassified, Secret, and Top Secret/Sensitive Compartmented Information (TS/SCI) systems.

Sec. 4. Policy Coordination Committee. (a) A Policy Coordination Committee (PCC) for NSS shall be formed pursuant to National Security Presidential Memorandum 1 of January 20, 2025 (Organization of the National Security Council and Subcommittees).

(i) The PCC shall be chaired by a member of the NSC staff and shall consist of representatives of the members and advisors from the CNSS.

(ii) Agencies that operate NSS may be invited at the discretion of the PCC chair.

(b) The PCC through the CNSS may request an assessment of the cybersecurity posture of NSS government-wide, to include performance metrics, cybersecurity assessment results, and compliance with current policy. The PCC chair may request that the National Manager conduct such assessment.

Sec. 5. The National Manager for NSS. (a) The Director of the NSA is the National Manager for NSS and will carry out the certain responsibilities in accordance with existing law, Executive Orders, and other Presidential directives. In this capacity the National Manager is responsible for providing technical advice to the CNSS and:

(i) providing recommendations on incident response for security incidents that impact NSS government-wide; and

(ii) as referenced in section 2(b)(ii) of this memorandum, in response to a known or reasonably suspected information security threat, vulnerability, or risk that represents a substantial threat to the information security of NSS, or in response to intelligence of adversary capability and intent to target NSS, the National Manager may issue an emergency directive to the head of an agency, through that agency's CIO, CISO, or officer designated by the head of the agency, to take any lawful action with respect to the operation of that NSS, including such systems used or operated by another entity on behalf of an agency, for the purpose of protecting the NSS from, or mitigating, the threat, vulnerability, or risk.

(b) The National Manager shall serve as the cryptologic authority for NSS. Through this role, the National Manager shall, in accordance with applicable law and policy:

(i) design, build, test, deliver, and protect cryptographic keys and codes capabilities;

(ii) review, approve, and publish standards related to the security of NSS;

(iii) develop, evaluate and approve techniques, systems, products, solutions, and equipment related to the cybersecurity of NSS, provided that nothing in this provision shall restrict agencies from testing cryptography on NSS that they own or operate;

(iv) operate such printing, fabrication, and other facilities as may be required to perform critical functions related to the provisions of cryptographic, identity, key management, and other technical security material or services;

(v) in consultation with the CNSS, prescribe the minimum standards, methods, and procedures for protecting cryptographic and other technical security material, techniques, and information related to NSS; and

(vi) enter into agreements for the procurement of technical security material and other equipment, their provision to agencies, and, where appropriate, government contractors and foreign governments.

(c) The National Manager shall assess the cybersecurity posture of NSS across the United States Government on behalf of the CNSS and serve as a technical advisor to the CNSS and agencies that own or operate NSS, in alignment with provisions set forth in section 9 of this memorandum. Through this role the National Manager shall:

(i) in consultation with the CNSS, develop government-wide performance metrics for the defense of NSS, and coordinate with the CNSS chair and CNSS members and

advisors on any CNSS collection of those metrics on a regular basis from each agency that owns or operates NSS;

(ii) assess the overall security posture of and disseminate information on threats to and vulnerabilities in NSS;

(iii) operate a technical center to evaluate and certify the security of NSS;

(iv) request from the heads of agencies, through an agency's CIO, CISO, or other officer designated by the head of the agency, such information and technical support as may be needed to discharge the responsibilities assigned herein;

(v) conduct, coordinate, or endorse research and development of techniques and equipment to secure NSS;

(vi) upon request, provide cybersecurity services and technical assistance to NSS owners and operators;

(vii) examine NSS and evaluate their vulnerability to foreign interception and exploitation, provided no examination or monitoring shall be performed without advising the CIO of the agency that owns or operates the NSS; and

(viii) conduct foreign cryptographic and cybersecurity liaison relationships, including by providing information, services, and support and by entering into agreements with foreign governments and with international and private organizations regarding NSS. Any liaison conducted with foreign intelligence or security services shall be carried out in coordination with the Secretary of War, the DNI, and the Director of the CIA in accordance with Executive Order 12333 of December 4, 1981 (United States Intelligence Activities), as amended. Any such agreements shall be coordinated with affected agencies.

(d) The National Manager, through the CNSS, shall establish requirements for cross-domain solutions and alternative technical solutions for the separation of security domains for NSS. Through this role, the National Manager shall:

(i) serve as the principal advisor to NSS owners and operators on cross-domain capabilities;

(ii) develop and maintain community outreach programs and fora focused on cross-domain solutions;

(iii) develop and establish improved security solutions, standards, and technologies for cross-domain solutions; and

(iv) perform comprehensive testing for establishment of approved cross-domain solution products.

(e) NSS owned or operated by civilian agencies play an important role in many military and intelligence missions. Additionally, heads of civilian agencies are accountable for protection of classified material that is stored or processed on NSS that are owned or operated by such agencies. The Director of OMB, with support from the National Manager, and acting through the Federal CIO as appropriate, shall oversee compliance of FCEB Agencies with NSS policies and directives with the exception of agencies and agency components that are part of the IC. National Manager support may include:

(i) collection of metrics and direct assessment of the cybersecurity posture of NSS owned or operated by FCEB Agencies;

(ii) provision of technical assistance upon request to NSS owners and operators on the implementation of the NSS policies; and

(iii) consistent with applicable law, assignment of personnel to the Office of the Federal CIO to align and enhance oversight across FCEB Agencies.

(f) The National Manager may partner and collaborate with the heads of other agencies on matters related to cybersecurity, including with the heads of CISA and NIST, as well as the private sector and academia, to carry out the responsibilities assigned herein in accordance with applicable law and policy.

Sec. 6. Implementation. (a) Within 30 days of the date of this memorandum, the CNSS shall revise CNSS Directive 900 of May 2013 (Committee on National Security Systems (CNSS) Governing and Operating Procedures), and any other policies as the CNSS deems appropriate, to incorporate the changes set forth in this memorandum.

(b) The CNSS and the National Manager shall take the following steps to harmonize NSS policies:

(i) within 60 days of the date of this memorandum, the CNSS shall issue a roadmap and policy priority areas for NSS to be applied in the next calendar year;

(ii) within 90 days of the date of this memorandum, the CNSS shall determine which National Manager Binding Operational Directives and other National Manager policies, including those related to NSM-8, with the exception of National Manager Emergency Directives, must be maintained and, where appropriate, incorporate those requirements into CNSS Directives. Upon completion of this process, the National Manager shall take necessary steps to rescind all National Manager Binding Operational Directives and Memoranda related to NSM-8 as appropriate; and

(iii) within 90 days of the date of this memorandum, the CNSS shall review all existing CNSS policies, directives, and instructions to determine which should be rescinded or harmonized. The CNSS shall complete rescission or harmonization of identified policies within 90 days of the completion of this review.

(c) Effective incident reporting for incidents that occur on or impact NSS is essential to minimize risk to the critical missions enabled by these systems and drive accountability for owners and operators, including civilian, defense, and intelligence agencies.

(i) Within 60 days of the date of this memorandum, the National Manager shall recommend to the CNSS new or modified incident reporting standards that enable government-wide awareness of incidents impacting NSS. This recommendation shall include thresholds for required reporting of incidents.

(ii) Within 60 days of the receipt of the National Manager's recommendations, the CNSS shall update applicable CNSS policies to incorporate those recommendations as appropriate.

(iii) Within 60 days of the release of the incident reporting standards described in section 6(c)(i) of this memorandum, agencies shall update their respective incident response policies to incorporate the revised standards, and ensure that all incidents meeting defined thresholds and that occur on or impact NSS are properly reported to the National Manager, IC CIO, DOW CIO, or Federal CIO.

(d) Each agency shall maintain and annually update an inventory of all NSS owned or operated by that agency.

(i) To assist the National Manager in reporting government-wide metrics, agencies shall make inventories available to the National Manager. At a minimum, this inventory must include the number of total information systems, NSS, and non-NSS, owned or operated by the agency.

(ii) Within 60 days of the date of this memorandum, the CNSS shall establish a working group to deconflict the identification and inventory of NSS and non-NSS in FCEB Agencies.

(e) Within 60 days of the date of this memorandum, the National Manager and the Director of OMB, through the Federal CIO, shall develop any memoranda of agreement necessary for the National Manager to assign or detail personnel to the Office of the Federal CIO, consistent with applicable law, to assist in the oversight of NSS owned or operated by FCEB Agencies in accordance with section 5(e) of this memorandum.

Sec. 7. Adaptation of Executive Order 14306 to National Security Systems. (a) Executive Order 14306 required the development of requirements for NSS that are consistent with the requirements set forth in that order as appropriate and consistent with applicable law. This section implements these requirements for NSS.

(i) Consistent with section 3(b) of Executive Order 14144 of January 16, 2025 (Strengthening and Promoting Innovation in the Nation's Cybersecurity), as amended by Executive Order 14306, within 120 days of the date of this memorandum, the CNSS shall request from cloud service providers accredited to host NSS, excluding those supporting compartmented intelligence missions, baselines with specifications and recommendations for agency configuration of agency cloud-based systems in order to secure Federal data based on agency requirements. The CNSS will assess these recommendations and make an independent decision as to whether to recommend them to the National Manager. The treatment of existing commercial cloud services provided by the CIA as a Service of Common Concern shall be subject to negotiation between the CIA and the CNSS.

(ii) Within 90 days of the date of this memorandum, the CNSS, in coordination with the Secretary of State, through the Department of State CIO, the Secretary of Commerce, through the Department of Commerce CIO, the Secretary of Energy, through the CIO of the National Nuclear Security Administration, and the Secretary of Homeland Security, through the Department of Homeland Security CIO, shall issue a report on the provisioning of cloud capabilities, to include recommended secure configuration baselines, at the Secret, Top Secret Collateral, TS/SCI, and Top Secret Controlled and Special Access Program levels for FCEB Agencies. This report shall be drafted in coordination with the roadmap on advanced computing resources tasked in National Security Presidential Memorandum 11 of June 5, 2026 (Artificial Intelligence in the National Security Enterprise).

(iii) Within 90 days of the date of this memorandum, the CNSS will review and identify revisions needed to CNSSP-32 of May 2022 (Policy on Cloud Security), to provide guidance and requirements for the secure hosting of NSS in cloud environments.

(b) Secure unclassified communication among agencies is essential in promoting the security of NSS and the missions that these systems support. Within 90 days of the date of this memorandum, the National Manager will provide recommendations to the CNSS on policy to promote government-wide, secure, interoperable unclassified voice and video communication capabilities for mobile and fixed devices among FCEB Agencies, DOW, and the IC.

Sec. 8. Definitions. For purposes of this memorandum:

(a) The term "agency" has the meaning given to it in 44 U.S.C. 3502(1).

(b) The term "Federal Civilian Executive Branch Agencies" means all agencies except for the Department of War and agencies in the Intelligence Community.

(c) The term "Federal Chief Information Officer" means the Administrator of the Office of Electronic Government appointed pursuant to 44 U.S.C. 3602(b).

(d) The term "National Security System" has the meaning given to that term in 44 U.S.C. 3552(b)(6), 44 U.S.C. 3553(e)(2), and 44 U.S.C. 3553(e)(3).

(e) The term "information system" has the meaning given to it in 44 U.S.C. 3502(8).

Sec. 9. General Provisions. This memorandum shall not be construed to implicitly alter or supersede existing authorities or contravene existing law, Executive Orders, or Presidential Directives to include authorities conferred to ensure the protection of intelligence sources and methods or to confer the authority to interfere with the means and methods necessary to undertake intelligence collection or covert action operations. This memorandum shall be implemented consistent with applicable law and subject to the availability of appropriations. No implementation measures shall impede the conduct or support of DOW or IC activities, or other activities under provisions of law, and all such implementation measures shall be designed to protect intelligence sources and methods.

DONALD J. TRUMP

NOTE: An original was not available for verification of the content of this memorandum.

Categories: Communications to Federal Agencies : National security systems, national policy for cybersecurity, memorandum.

Subjects: Attorney General; Central Intelligence Agency; Committee on National Security Systems; Cybersecurity and Infrastructure Security Agency; Cybersecurity, strengthening efforts; Director of National Intelligence; Joint Chiefs of Staff; National Cyber Director; National Nuclear Security Administration; National Security Adviser; National Security Agency; National security systems, national policy for cybersecurity; Office of Management and Budget; Office of Science and Technology; Research and development; Secretary of Commerce; Secretary of Energy; Secretary of Homeland Security; Secretary of State; Secretary of War.

DCPD Number: DCPD202600402.