NATIONAL SECURITY PRESIDENTIAL MEMORANDUM/NSPM-11

June 5, 2026

MEMORANDUM FOR THE SECRETARY OF STATE

THE SECRETARY OF THE TREASURY

THE SECRETARY OF WAR

THE ATTORNEY GENERAL

THE SECRETARY OF ENERGY

THE SECRETARY OF HOMELAND SECURITY

THE DIRECTOR OF THE OFFICE OF MANAGEMENT AND BUDGET

THE DIRECTOR OF NATIONAL INTELLIGENCE

THE DIRECTOR OF THE CENTRAL INTELLIGENCE AGENCY

THE ASSISTANT TO THE PRESIDENT FOR NATIONAL SECURITY AFFAIRS

THE ASSISTANT TO THE PRESIDENT FOR SCIENCE AND TECHNOLOGY

THE ASSISTANT TO THE PRESIDENT FOR POLICY AND HOMELAND SECURITY ADVISOR

THE DIRECTOR OF THE FEDERAL BUREAU OF INVESTIGATION

THE DIRECTOR OF THE OFFICE OF PERSONNEL MANAGEMENT

THE NATIONAL CYBER DIRECTOR

SUBJECT: Artificial Intelligence in the National Security Enterprise

By the authority vested in me as President by the Constitution and the laws of the United States of America, I hereby direct the following:

Section 1. Purpose. Artificial intelligence (AI) will be among the most transformative technologies to national security in the history of the United States. When adopted appropriately, AI can help protect our warfighters during peacetime and on the battlefield, enable precise operations that minimize harm to civilians, and ensure the United States continues to maintain technical overmatch against our adversaries and strategic competitors.

Previous administrations imposed undue bureaucracy that hampered the pace of AI adoption, fostered dangerous dependencies on single vendors, and made it challenging for our warfighters to adopt the most advanced technologies. Meanwhile, our competitors continued to develop and deploy their own AI and sophisticated autonomous technologies for military and intelligence purposes, employing them with little regard for appropriate human oversight or civil liberties.

Under my Administration, the United States can and will responsibly accelerate the use of AI across intelligence and warfighting domains in line with American values. The United States possesses the most effective and moral military in the history of world. It is also among the most trusted institutions in American life. That trust is rooted in an unbroken chain of command and accountability, from our democratic process through civilian and military leadership, to the men and women who carry out the mission.

My Administration will ensure that those who safeguard America and the American way of life are equipped with the most sophisticated and secure AI technologies to perform complex, time-sensitive, and highly-consequential missions, with full confidence that those tools will be available when they matter most. We will streamline the acquisition and deployment of these technologies while maintaining rigorous oversight and building a secure and resilient supply chain that cannot be severed in times of conflict. We will work closely with the private sector and academia to ensure the best technical talent is available to the national security enterprise and that our warfighters are trained to effectively employ advanced AI systems in accordance with guidance. Through these efforts, my Administration will secure a decisive and enduring AI advantage against any and all adversaries while safeguarding the constitutional chain of command.

Sec. 2. Policy. My Administration will accelerate the development and use of AI for national security applications, guided by the following four pillars:

(a) Adoption. The national security enterprise shall accelerate AI adoption by identifying mission areas where AI can enhance operational effectiveness and eliminating unnecessary barriers to rapid deployment. To

this end, the national security enterprise shall maintain deep, proactive partnerships with industry, to make the most advanced frontier models broadly available to national security professionals without delay, ensuring technological overmatch while driving rapid experimentation and validation across potential applications.

(b) Adaptation. The national security enterprise shall adapt commercial or open-source AI technologies, leveraging the most cutting-edge capabilities available from diverse suppliers across the private sector, large and small, while ensuring that AI technologies chosen are optimized for their intended use. In cases where the use of a commercial solution is not appropriate due to security or mission limitations, executive departments and agencies (agencies) may deploy commercially or internally customized AI technologies or develop AI technologies internally. Such technologies shall be made available across the national security enterprise to support multiple missions where possible.

(c) Assurance. The national security enterprise shall assure that all AI technologies adopted are designed to be reliable, robust, steerable, and controllable, and that they operate, in accordance with applicable laws, government policies, and guidance. To protect American warfighters, the national security enterprise shall ensure, through contractual clauses or other means, that no commercial entity or adversary possesses the capability to prevent use of, disable or degrade, or materially modify without Federal Government knowledge and approval, an AI system that our men and women depend on for their missions. In addition, rigorous security and functionality measures, including testing, evaluation, validation, and verification, shall be implemented to assure the appropriate confidentiality, integrity, reliability, availability, and interoperability of AI systems across the national security enterprise.

(d) Accountability. American AI technologies shall neither be developed nor used by the national security enterprise to censor free speech, embed ideological bias, or conduct unauthorized or unlawful surveillance activities. The use of AI by the national security enterprise must always be consistent with United States civil liberties and protections afforded by the Constitution and laws and regulations safeguarding the privacy of American citizens. Commanders, directors, and heads of agencies shall remain responsible and accountable for ensuring that these obligations are met at every level of command, and that such accountability keeps pace with the evolution of AI capabilities and regulations governing the privacy and civil liberties of American citizens.

Sec. 3. Updated Policies and Guidance. (a) Within 90 days of the date of this memorandum, the Secretary of War shall issue an update to DOD Directive 3000.09 on Autonomy in Weapon Systems, to be reviewed annually to account for the rapidly evolving capabilities of AI systems, to ensure the deliberate adoption of AI systems that respect the chain of command and operational authorities, and remain consistent with the policy set forth in section 2 of this memorandum.

(b) Consistent with roles and responsibilities outlined in the Federal Information Security Modernization Act of 2014 (44 U.S.C. 3551 *et seq*.), the Secretary of War for systems described in section 3553(e)(2) of that Act, the Director of National Intelligence (DNI) for systems described in section 3553(e)(3) of that Act, and the heads of relevant agencies for systems described in section 3557 of that Act, shall direct, to the maximum extent permissible by law, termination for default or for convenience contracts with companies that have repeatedly demonstrated a pattern of conduct that is inconsistent with policies laid out in section 2 of this memorandum. This includes contracts under which such companies provide services to the applicable agencies as subcontractors. The heads of these agencies may establish a waiver process to grant limited exceptions of a defined duration, to exceed no longer than 1 year, where such relationships are necessary to responsibly steward United States national security. Exceptions may include operational imperatives, test and evaluation arrangements, threat intelligence sharing, and other mission-critical applications, subject to appropriate risk mitigation measures and enhanced oversight. All exceptions shall be reported to the Assistant to the President for Science and Technology (APST) and the Assistant to the President for National Security Affairs (APNSA) in writing by heads of agencies, without designee, within 30 days of the waiver being granted.

(c) Within 90 days of the date of this memorandum, consistent with policies laid out in section 2 of this memorandum, the Committee on National Security Systems and the Director of the Office of Management and Budget (OMB Director), in coordination with the APST, and in consultation with the heads of relevant IC elements, shall issue an appropriate policy for governance of AI use in national security systems, including implementation and reporting requirements. Such policy should maximize consistency with AI governance requirements for non-national security systems, such as that in OMB guidance OMB memorandum M-25-21, to the extent appropriate.

(d) To address sensitive national security issues, a classified annex will be issued within 90 days of the date of this memorandum.

(e) Following the issuance of the guidance called for in this section, the Secretary of War, heads of agencies within the IC, and the heads of any other agency performing a national security function shall update all relevant policies and guidance to be consistent with the policy set forth in this memorandum. Each such agency head shall review and, as necessary, further update such guidance on an annual basis to reflect the evolving state of AI technology.

(f) This memorandum hereby rescinds and replaces National Security Memorandum-25 and associated guidance.

Sec. 4. Advancing National Security Capabilities. (a) Within 120 days of the date of this memorandum, the Secretary of War, the DNI, and the heads of agencies with IC elements shall review and update procurement processes to ensure the rapid onboarding of the most advanced AI models from multiple vendors, closing the capability gap between what is available to the public and to our national security workforce.

(b) Within 90 days of the date of this memorandum, the APST and the OMB Director, in coordination with the Secretary of War, the Secretary of Energy, the DNI, and the Director of the National Security Agency (NSA Director), and in consultation with other agencies as appropriate, shall jointly develop a roadmap to ensure that all elements of the national security enterprise have adequate access to advanced computing resources. The roadmap should include the commissioning of advanced AI computing facilities with the appropriate high security requirements, to support next-generation AI systems operating at scale, and should include the establishment of an AI test range for national security use cases, subject to the availability of appropriations.

(c) Within 120 days of the date of this memorandum, the Secretary of War, the Secretary of Energy, the DNI, and the NSA Director, through the AI Security Center, in consultation with the APST, shall develop partnerships with willing private-sector companies to help secure America's most cutting-edge AI technologies, including from malicious distillation attacks. Such partnerships may include sharing threat intelligence, conducting joint AI red-team exercises, assisting with personnel vetting, supporting joint security research and development (R&D) that the private sector cannot undertake alone, enhancing the physical and cyber security of our Nation's data centers, and providing technical support similar to that given to Defense Industrial Base partners. Agencies shall coordinate and deconflict engagements with industry partners when practicable.

(d) The Secretary of Energy shall work with relevant agencies through the Genesis Mission to develop capabilities for applying AI to national security missions, including through partnerships with the private sector.

(e) The DNI, in coordination with IC elements, shall prioritize the collection and analysis of foreign AI technologies, across the AI technology stack, AI applications and uses, and AI governance and policies that pose a threat to United States national security, economic security, and strategic competitiveness. In consultation with the DNI, the Secretary of State shall develop a strategy to engage with allies and partners and share findings from the DNI's analysis, as appropriate, to address these threats.

(f) Within 120 days of the date of the memorandum, consistent with applicable authorities, the DNI, the Secretary of War, the Secretary of Energy, and the NSA Director, under his National Manager authorities, shall initiate joint AI data and model exchanges, accessible across multiple enclaves, for mission applications common to the national security enterprise.

Sec. 5. Building Capacity for AI Adoption. (a) Agencies are directed to utilize special hiring and pay authorities, as well as novel talent programs from the Office of Personnel Management (OPM) and other relevant agencies, to accelerate the hiring of technical AI talent into the Federal Government.

(b) Within 120 days of the date of this memorandum, the OPM Director, in coordination with the Secretary of Homeland Security, and in consultation with the DNI, the Secretary of War, the Secretary of Energy, the OMB Director, the APST, and the APNSA, the Homeland Security Advisor, and relevant IC elements, shall initiate efforts to establish an AI National Security Strategic Reserve of non-governmental AI talent to provide support to Federal efforts to address AI national security issues, as needed.

(c) Within 120 days of the date of this memorandum, the DNI and the Secretary of War, in coordination with the OMB Director and IC elements, shall develop and implement an AI for National Security Curriculum, coordinated with existing Federal AI and cyber training programs. This initiative shall ensure that relevant personnel across the national security enterprise are trained to employ AI systems in accordance with applicable guidance and maintain literacy on the current AI frontier, including its capabilities, limitations, and implications for national security.

(d) Agencies shall prioritize the R&D of technologies that enable AI reliability, robustness, steerability, and controllability in fulfillment of mission requirements, including constitutional protections. They shall also develop

capabilities and best practices to maintain the leadership of the national security enterprise in this domain, subject to the availability of appropriations.

(e) Within 120 days of the date of this memorandum, to ensure the confidentiality, integrity, and availability of America's most critical AI systems, the DNI, the Secretary of War, and the NSA Director, under his National Manager authorities, in coordination with the Secretary of Homeland Security, the Secretary of Energy, and the Secretary of the Treasury, shall develop a joint strategy for AI risk management and assurance and implementation guidance that establishes baseline AI security practices for the national security enterprise, to be submitted to the APST, the OMB Director, the National Cyber Director, and the APNSA for review prior to publication.

(f) Within 120 days of the date of this memorandum, the Secretary of War, through the NSA Director, and the DNI shall submit standardized AI national security Test, Evaluation, Verification, and Validation methodologies, including for conformity verification and sustainment of high-security AI systems, at appropriate classification levels, to the APST and the National Cyber Director for review prior to publication, where appropriate.

Sec. 6. Definitions. For the purposes of this memorandum:

(a) "Artificial intelligence" or "AI" has the meaning set forth in 15 U.S.C. 9401(3);

(b) "AI incident response" means the preparation, detection, analysis, remediation, and recovery from intentional or unintentional performance degradation or data loss or spillage of AI systems, including technical malfunctions and adversarial attacks;

(c) "AI security" means the application of appropriate protection mechanisms across the AI technology stack to ensure the confidentiality, integrity, and availability of AI systems, from design through deployment;

(d) "AI technology stack" means the layers that enable the development and deployment of AI technologies, including AI-optimized hardware and related infrastructure, including chips, servers, accelerators, data center storage, cloud services, networking, etc.; data pipelines and labeling systems; AI models and systems; security and cybersecurity measures for AI models and systems; and AI applications for sector-specific or functional use cases;

(e) “Chain of command” means the properly designated succession of individuals through which authority, direction, and control is exercised to accomplish a lawful objective;

(f) “Controllability” means the ability to monitor the operation and outcomes of a system and take corrective action as needed.

(g) “Intelligence Community” has the meaning given the term in section 3003 of title 50, United States Code;

(h) “National security enterprise” means the Department of War, the Intelligence Community, and other agencies that develop, deploy, or use national security systems or otherwise serve a national security role;

(i) “Reliability” means the ability of a system to perform as required, without failure, under given conditions;

(j) “Robustness” means the ability of a system to maintain a level of performance under a variety of circumstances, including outside intended operating conditions; and

(k) “Steerability” means the ability to shape the internal behavior of a system to pursue a given set of objectives.

Sec. 7. General Provisions. (a) Nothing in this memorandum 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.

DONALD J. TRUMP