Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

April 7, 2026

Cyber and Artificial Intelligence Provisions in the FY2026 National Defense Authorization Act (NDAA)

The National Defense Authorization Act for Fiscal Year 2026 (FY2026 NDAA; P.L. 119-60) contains numerous provisions regarding cyber-related issues, including artificial intelligence (AI). Title XV organizes Cyberspace-Related Matters into five subtitles: A. Operations; B. Cybersecurity; C. Information Technology and Data Management; D. Artificial Intelligence; and E. Reports and Other Matters. Other titles in the FY2026 NDAA contain provisions directly or indirectly related to cyberspace and AI. This In Focus describes selected elements of these and other selected provisions and potential issues for Congress.

Cyber Operations Provisions

Section 1501 of the FY2026 NDAA requires the Commander of U.S. Cyber Command (USCYBERCOM) to establish processes for planning, programming, and budget coordination for Cyber Mission Force (CMF) operations to ensure the CMF is adequately resourced to sustain its mission.

Section 1502 amends 10 U.S.C. §392a(b) to direct the Senior Military Advisor for Cyber Policy to report to the Assistant Secretary of Defense for Cyber Policy, rather than the Under Secretary of Defense for Policy.

Section 1503 directs the Secretary of Defense (SECDEF) to "develop a technical debt classification that adequately reflects different types of technical debt" and integrate the framework into Department of Defense (DOD) structures "relating to resourcing and programmatic decisions for existing or proposed information technology systems, services, or related programs of record." (DOD is "using a secondary Department of War designation" and the SECDEF is using a secondary title of "Secretary of War" under Executive Order 14347, dated September 5, 2025.) Technical debt is the future cost of relying on suboptimal, expedient choices during software development.

Section 1504 establishes a DOD-wide Data Ontology Governance Working Group to "expand data interoperability, enhance information sharing, and enable more effective decision making throughout the Department."

Section 1505 requires DOD tabletop exercises that develop future force employment concepts and assess different models for command and control of cyberspace operations.

Section 1506 requires the Under Secretary of Defense for Personnel and Readiness and the Under Secretary of Defense for Policy to coordinate an initiative to understand and address the behavioral health challenges and work-related stresses faced by the CMF.

Section 1507 prohibits the SECDEF from eliminating certain "cyber assessment capabilities or red teams" that support operational tests and evaluations for DOD programs without providing a specified certification to Congress.

Section 1508 contains a prohibition on availability of funds to modify the authorities of the Commander of USCYBERCOM.

Section 1509 limits the availability of funds for the Combined Joint All-Domain Command and Control initiative until the SECDEF provides a framework for guiding investments and measuring progress.

Cybersecurity Provisions

Section 1511 requires cybersecurity requirements in contracts for secure mobile phones and related telecommunications services provided to senior officials and personnel performing sensitive national security functions in DOD. These requirements must include encryption, persistent identifier mitigation or obfuscation, and continuous monitoring capabilities.

Section 1512 requires DOD, in coordination with other agencies, to establish a comprehensive cybersecurity and governance policy for all AI and machine learning systems used within DOD. The policy must address risks such as counterfeit parts, data poisoning, jailbreaks, and unauthorized access—among other related elements—and is to be implemented as an extension or augmentation to existing cybersecurity frameworks.

Section 1513 directs the development of physical and cybersecurity procurement requirements to mitigate risk of use for covered DOD AI and machine-learning systems.

Section 1514 directs the SECDEF to establish a collaborative cybersecurity educational program with academic institutions to develop cybersecurity competencies at those institutions.

Section 1515 requires the incorporation of AI considerations into DOD cybersecurity training for DOD personnel.

Information Technology and Data Management Provisions

Section 1521 amends DOD's Authorization to Operate (ATO) processes to include "mandatory timelines for activities performed by authorizing officials with respect to an [ATO] for cloud-hosted platforms, services, and applications."

Section 1522 requires an annual report on DOD's ongoing unified datalink strategy.

AI Provisions

Section 1531 modifies Section 1532 of the FY2025 NDAA (P.L. 118-159) on the high performance computing roadmap to require the SECDEF to ensure that data centers to be installed on military installations consider energy and usage requirements.

Section 1532 prohibits DOD from using or acquiring covered AI systems—including those from DeepSeek and High Flyer—or systems from covered nations—including the Democratic People's Republic of Korea, the People's Republic of China, the Russian Federation, and the Islamic Republic of Iran—or AI companies. The SECDEF may grant a case-by-case waiver for research, training, and evaluation or military activities supporting national security functions such as counterterrorism or counterintelligence.

Section 1533 directs the SECDEF to establish a cross-functional team for AI model assessment and oversight. The team is to develop a DOD-wide assessment framework regarding the development and procurement of AI, to include standards for performance of AI models, testing procedures, security requirements, and compliance with DOD's ethical AI principles.

Section 1534 directs the SECDEF to create a task force to develop and deploy AI sandboxes—isolated and controlled computing environments—to support DOD's experimentation with and training and development of AI. The task force is to create standard requirements for AI sandbox environments across DOD.

Section 1535 directs the SECDEF to create an AI Futures Steering committee to shape DOD's advanced AI strategy, analyze the development and effects of associated technologies, and identify resource requirements.

Reports and Other Matters

Section 1541 modifies an existing certification requirement for military recruiting contracts to ensure DOD does not "rate or rank news or information sources for the factual accuracy of their content; provide ratings or opinions on news or in formation sources regarding misinformation, bias, adherence to journalistic standards, or ethics; or acquire or use any service that provides any ratings, rankings, or opinions ... from any other person."

Section 1542 directs that the annual assessments and reports on the assignment of certain budget control responsibility to the Commander of USCYBERCOM include a review of investments in AI capabilities, including their alignment with the milestones of DOD's roadmap and implementation plan for cyber adoption of AI.

Section 1543 requires a study on increasing the cost of and reducing incentives for cyberattacks on defense critical infrastructure.

Section 1544 requires a study on the appropriate "framework for structuring and organizing, including training and preparing, the reserve component personnel and units to be employed within the [CMF] for cyberspace operations."

Section 1545 requires an annual report on Mission Assurance Coordination Board activities, to include cybersecurity risks to covered assessments (as defined in DOD Instruction 3020.45).

Other Cyber- and AI-Related Provisions

Section 5301 authorizes a Post Data Pilot Program to "[cultivate] a data and AI culture at diplomatic posts globally, including data fluency and data collaboration" and promote data integration at the Department of State (DOS).

Section 5302 requires DOS to issue internal guidelines to track the use of commercial cloud enclaves deployed in overseas commercial clouds.

Section 5303 requires detailed reports to Congress on technology transformation projects within DOS.

Section 5304 expresses the sense of Congress of a need for "responsible procurement and application" of commercial spyware capabilities and notes that the growing market for these capabilities has enhanced the abilities of "state and non-state actors" to target journalists, human rights groups, and other members of civil society. It also notes that the United States will, as a matter of policy, "oppose the misuse of commercial spyware" to target vulnerable populations.

Section 6601 directs the Director of the National Security Agency to develop security guidance to defend AI against theft or sabotage by nation-state adversaries by identifying vulnerabilities in the cybersecurity and AI supply chain.

Section 6602 instructs the intelligence community's (IC) Chief Information Officer and Chief AI Officer to identify commonly used AI systems or functions within the IC that could be repurposed for other IC elements and adopt supporting policies and contractual terms.

Section 6603 addresses the use of publicly available AI models in classified environments and directs the creation of policies for AI testing standards that evaluate "performance, efficacy, safety, fairness, transparency, accountability, appropriateness, lawfulness, and trustworthiness" for common AI use cases.

Section 6604 instructs the Director of National Intelligence to create guidelines that require the removal of DeepSeek, or its successors, from IC and IC-related systems.

Issues for Congress

Congress may conduct oversight of DOD's implementation of these provisions and consider the implications of related reporting requirements for future defense authorizations and appropriations.

Congress currently is considering reauthorization of the Cybersecurity Information Sharing Act of 2015 (CISA; P.L. 114-113), which established a voluntary information-sharing process between private sector and federal government entities for cyberthreat indicators and defensive measures. As amended by Section 106 of P.L. 119-37, the act expired on January 30, 2026; its reauthorization was not included in the FY2026 NDAA.

Catherine A. Theohary, Specialist in National Security Policy, Cyber and Information Operations
Kelley M. Sayler, Specialist in Advanced Technology and Global Security

Disclaimer