Congressional Research Service
Informing the legislative debate since 1914

INSIGHT

FY2026 Department of Defense Cyber Budget Request

November 24, 2025

Introduction

The "cyber budget," as it is known colloquially, of the U.S. Department of Defense (DOD)—which is "using a secondary Department of War designation" under Executive Order 14347 dated September 5, 2025—is the aggregate of defense programs and activities related to cyberspace. The Senate Armed Services Committee-reported version of the National Defense Authorization Act for Fiscal Year 2026 (NDAA; S. 2296) generally refers to these programs in Title XVI as "Cyberspace-Related Matters," as does the House Armed Services Committee-reported version (H.R. 3838) in Title XV. Some provisions containing the word "cyber" or "cybersecurity" that may be part of the cyber budget appear elsewhere in these bills (e.g., H.R. 3838, Titles VI, XII). Other programs that relate to cyberspace such as information assurance, artificial intelligence, or information operations, although they lack the "cyber" header, may also be part of the overall cyber budget. Details of cyberspace-related programs, such as program elements, may be classified; budget requests for these programs are historically submitted in a classified annex. Both classified and unclassified programs are included in totals for the DOD cyber budget. The cyber budget submission combines the non-cyber President's Information Technology Budget for the Department of Defense. Information on DOD, as well as civilian agencies' information technology budgets, are available at the General Services Administration's IT Dashboard.

Cyber Activities for FY2025

DOD's FY2025 budget request for information technology and cyberspace activities shows that the latter, at approximately $14.5 billion, is less than a quarter of the budget compared to non-cyber information technology, at approximately $49.6 billion. The figure for cyberspace activities comprises three portfolios: cybersecurity (much of which is related to information assurance), cyberspace operations, and research and development. The cyberspace operations budget is further delineated between funding for the Cyber Mission Force (CMF) and United States Cyber Command Headquarters (CYBERCOM), as well as "all other" cyberspace operations. DOD requests funds for CYBERCOM and its programs in budget justification documents associated with multiple Defense-Wide accounts: Operations and

Congressional Research Service
https://crsreports.congress.gov
IN12616

Maintenance (O&M); Procurement; and Research, Development, Test, and Evaluation (RDT&E). Each of the military services provides a budget request for cyberspace activities along with defense-wide cyberspace activities. DOD components with significant cyber responsibilities, such as the Defense Threat Reduction Agency and the Defense Information Systems Agency, submit their own budget justifications.

Cyber Activities for FY2026

The cyberspace activities request for FY2026 is approximately $15.1 billion, or 4.1% more than the previous year's request. The FY2026 budget request overview states that this request will "defend and disrupt the efforts of advanced and persistent cyber adversaries, accelerate the transition to Zero Trust cybersecurity architecture, and increase defense of U.S. critical infrastructure and defense industrial base partners against malicious cyber attacks." It further states that this budget request aligns with the classified 2025 Interim National Defense Strategic Guidance priorities and the 2023 DOD Cyber Strategy.

Cybersecurity

The FY2026 budget request includes $9.1 billion for cybersecurity. Programs under this header include information assurance, operational technologies including weapons systems, defense critical infrastructure, supply chain risk management, defense industrial base security, and cryptographic modernization. Particular initiatives include mitigating DOD's cyber risk by working towards a "zero trust" model, which assumes that intruders are already present on DOD information networks, and resourcing the Cybersecurity Maturity Model Certification program for the defense industrial base.

Cyberspace Operations

The FY2026 budget requests $5.4 billion for cyberspace operations. Approximately $2.6 billion of the cyberspace operations budget is designated for CYBERCOM resources, including $314 million for CYBERCOM headquarters and $1.3 billion for the command's operational arm, the Cyber Mission Force. Approximately $2.8 billion is for the military services, the Joint Staff, the Defense Intelligence Agency, the Defense Threat Reduction Agency, the National Security Agency, and the Office of the Under Secretary of Defense, Research and Engineering. Investment areas include cyber training and readiness, offensive and defensive cyberspace operations, DOD's Hunt Forward Operations (HFO), and cyber operations capability development.

Research and Development

The $611.9 million DOD cyber research and development (R&D) was requested to resource the deployment and modernization of existing capabilities and technologies that advance "next generation" cybersecurity and cyberspace operations programs. Additionally, the department requested R&D investments to support "developing the computing, networking, and cyber defense technologies needed to protect DOD information infrastructures and mission-critical information systems." CYBERCOM's artificial intelligence initiatives across the DOD enterprise outline six areas of focus: vulnerabilities and exploits; network security, monitoring, and visualization; modeling and predictive analytics; persona and identity; permeability and agility across domains; and infrastructure and transport.

Cyberspace and the Pacific Deterrence Initiative

Cyberspace activities are a priority under the DOD's Pacific Deterrence Initiative, which seeks to deter threats from China in the Indo-Pacific area of operations. DOD's Indo-Pacific Command (INDOPACOM)

is undergoing a technology modernization effort as part of CYBERCOM's Joint Cyber Warfighting Architecture (JCWA) Integration and Innovation program. There are six elements of the JCWA: Cyber Weapons and Tools, Data and Sensors, Robust Infrastructure, Cloud and Unified Platform, Persistent Cyber Training Environment, and Cyber Command and Control. Of the six elements, the Data and Sensors element is of particular relevance to the PDI. The Data and Sensors program budget for $62.5 million under CYBERCOM's procurement budget activity would fund HFO, Enhanced Sensing and Mitigation, Deployable Mission Support Systems kits, Joint Cyber Hunt Kits, and investments in other sensors used to support the CMF. According to the budget justification, the enhanced sensing efforts are components of the PDI to reduce vulnerabilities, strengthen defenses in key networks and improve the overall defensive posture in the INDOPACOM region, with a near-term focus on Guam.

The Senate passed its version of the National Defense Authorization Act for Fiscal Year 2026 on October 9, 2025 and was sent to the House of Representatives on November 10, 2025, where it is being held at the desk as of November 12, 2025. Previously, the House of Representatives version passed on September 10, 2025. The House passed the Department of Defense Appropriations Act, 2026 on July 18, 2028. The Senate version has not received a vote.

Author Information

Catherine A. Theohary
Specialist in National Security Policy, Cyber and
Information Operations

Disclaimer