The FY 2026 National Defense Authorization Act

Client Alert | 22 min read | 12.23.25

On December 18, 2025, the Fiscal Year 2026 National Defense Authorization Act (FY 2026 NDAA) (P.L. 119-60) was signed into law. The **Act** makes significant changes to defense acquisition, sourcing restrictions, and interactions between the Defense Industrial Base (DIB) and the Department of Defense (DOD).

Streamlining Acquisition Process and Collaborating With Industry

Government contractors should pay close attention to the acquisition reforms in this year's NDAA. Most notably, the FY 2026 NDAA overhauls the DOD acquisition lifecycle and requirements process for major systems, shifting to a new portfolio-based acquisition model with product support management built in. As part of the effort to support lifecycle sustainment for major systems and other DOD acquisition programs, the NDAA expands preferences for commercial products and services, recognizing that commercial innovation may be rapid and that more flexible acquisition models may allow DOD to access cutting-edge technology with each iteration of improvement. On the flipside, while the final compromise legislation does not include "right to repair" language pushed by some members of Congress, the NDAA's focus on increasing interoperability of major systems may lead to increased requirements for a modular open systems approach (MOSA), and more collaborative development efforts, as Congress pressures DOD to break up contracts into smaller increments to allow more companies to participate in designs. Contractors may also face DOD requests to purchase government-purpose data rights even for commercial products or services.

The most significant reforms in the FY 2026 NDAA are the changes to DOD's acquisition process for major systems, which in turn drive the Department's other contracting processes. Congress redefined the goals of the acquisition system, including by redefining "best value" for acquisition as the "optimal combination of cost, quality, technical capability or solution quality, and delivery schedule" (Section 1801). To deliver on these new objectives, the NDAA creates the "portfolio acquisition executive" role, responsible for leading "capability portfolios" that, among other things, prioritize commercial products and services (Section 1802), and the product support manager role, responsible for life-cycle sustainment of covered systems, including intellectual property management and authority over "critical readiness items" that could impact sustainment (Section 1803).

Keeping with the goal of better aligning military needs with the pace of technology evolution, Section 1811 modifies the mission of the Joint Requirements Oversight Council (JROC) to focus on addressing gaps and identifying advances in technology, including for "innovative commercial solutions." The JROC's requirements development must now consider end user input as well as industry input on "commercially available technology to address joint operational problems or gaps in military capabilities." These considerations seek to make the defense acquisition process agile enough to facilitate rapid adoption.

The FY 2026 NDAA streamlines the acquisition process by repealing and amending existing laws, particularly for nontraditional defense contractors (Sections 811 and 812). In addition, Section 1804 raises the threshold for mandatory submission of certified cost or pricing data (also known as the TINA threshold) from $2.5

million to $10 million for defense contracts entered after June 30, 2026. Section 1806 raises the thresholds which trigger contractors to comply with Cost Accounting Standards (CAS) and requires implementing regulations within 180 days, as follows: (1) the threshold for full CAS coverage is increased from $50 million to $100 million; and (2) the threshold for CAS applicability for a contract is increased from $2.5 million to $35 million.

The NDAA also seeks to enhance DOD supply chain resiliency and increase the availability of qualified secondary sources for critical readiness items by amending the Expedited Acceptance and Qualification process established in Section 865 of the FY 2025 NDAA. Under Section 832, DOD must now allow expedited acceptance and qualification of critical readiness items, establish in each military department Expedited Qualification Panels to review requests, and accept as qualifications any parts certifications issued by civil aviation authorities. And under Section 1846, DOD must also use the Expedited Acceptance and Qualification Process to approve entire advanced manufacturing processes as part of overarching guidance DOD must issue on standardizing advanced manufacturing approvals and standards across military departments.

Finally, several provisions in the FY 2026 NDAA lower the barrier to market entry and the compliance burden for nontraditional defense contractors. Under Section 824, DOD must issue guidance on allowing past performance references from commercial contracts and using "alternative methods of evaluation other than past performance" when a requirement has little to no precedent.

Section 1826 stipulates that nontraditional defense contractors are exempt from specific statutory and DFARS requirements related to certified cost or pricing data, FAR Part 31 cost principles, and certain business systems. DOD can waive that exemption (in whole or part) but only with *both* a determination by the head of the contracting activity and congressional notice, suggesting that waivers will be rare.

Commercial Contracting

The FY 2026 NDAA directs DOD to increase its use of commercial contracting and streamline requirements for commercial contractors and subcontractors. These efforts include requiring DOD to develop a list of defense-unique contract clauses based on statutes, executive orders, and acquisition policies applicable to DOD contracts for commercial products and services and commercially available off-the-shelf items (Section 1821), as well as prohibiting DOD from designating clauses not on that list as mandatory flow-downs for commercial subcontracts (Section 1824).

Congress is also taking further steps toward making commercial designations mandatory and making it more difficult to determine the non-availability of commercial products or services. In particular, Section 1822 requires DOD to establish processes for determining that commercial products or commercial services are not available, including market research, and requires that such market research include senior DOD personnel. Section 1823 broadens DOD's authority to award sole-source follow-on production contracts if the original contract was awarded "through a competitive selection of proposals resulting from a general solicitation and a peer review, technical review, or operational review (as appropriate);" the authority now covers all commercial products, commercial services, and non-developmental items, not just "innovative" commercial products or services. DOD must still follow justification requirements.

Section 1828 requires DOD to conduct a "comprehensive review" of its approach to commercial products and services procurements and, within 180 days of the enactment of the NDAA, report to Congress on its findings,

improvement actions, response to any identified noncompliance with statutory or regulatory requirements, and legislative recommendations.

Bid Protests

Section 875 requires the Secretary of Defense to revise the DFARS to establish procedures for contracting officers to withhold up to 5% of the amount earned by an incumbent DOD contractor as a result of a stay prohibiting award of the contract during the pendency of its Government Accountability Office (GAO) protest and for the incumbent contractor to forfeit those amounts if GAO dismisses the protest "based on a lack of any reasonable legal or factual basis."

Data Rights

While the final compromise NDAA did not include significant "right to repair" provisions that both the House and Senate had initially included, the NDAA requires DOD to inventory its existing data rights and data rights contractual requirements, including requirements that DOD may not always invoke. In particular, Section 805 requires DOD to (1) establish a digital system for tracking, managing, and assessing "covered data" (i.e., technical data and computer software required to enable DOD and repair contractors to perform depot-level maintenance and to repair or maintain a core logistics capability) related to "covered systems" (i.e., major defense acquisition programs and programs or projects using rapid prototyping or rapid fielding acquisition pathways meeting certain dollar thresholds) and (2) verify contractor and subcontractor compliance with technical data contract requirements for covered systems. It also requires DOD to review requirements in contracts for each covered system, including requirements for data deliverables and data otherwise accessible by DOD on a non-deliverable basis.

Congress further instructed DOD to (1) review requirements related to covered data and describe the location of that data in the possession of DOD or method by which DOD accesses the data, (2) evaluate whether delivered covered data comply with marking and rights requirements and the requirements of 10 U.S.C. Chapter 275, and (3) describe the rights in technical data granted to DOD in data deliverables. These findings will be recorded in the aforementioned digital system.

With this information, DOD must identify areas where covered data are insufficient in a way that negatively impacts effective operation and maintenance of a covered system in a cost-effective manner. If delivery of or access to covered data was required under the contract but deliveries or access are insufficient or data rights markings are incorrect, then DOD must address the issue with the contractor. For covered data where delivery or access was not required by the contract, DOD is directed to request options from the contractor to address the insufficiency in the covered data. DOD is also instructed to consider using escrow agreements and similar arrangements under a specifically negotiated license for required covered data for covered systems.

Where there is an insufficiency in covered data for a commercial product, DOD must verify pricing and terms are commensurate with commercial practices and, to the extent DOD needs access to technical data, software, or other information in a manner that differs from the contractor's customary commercial practice, DOD must then seek to negotiate a customized commercial license for such access.

Finally, DOD is directed to ensure that all technical data, software, contract files, and related records acquired or generated in connection with a covered system are retained and managed by DOD until DOD has divested from the covered system.

Acquisition Reform Regarding Special Circumstances

Multiyear Procurement Authority. Section 804 authorizes multiyear procurement authority (MYP) for certain munitions, including:

- Standard Missile-3 (SM-3),
- Standard Missile-6 (SM-6),
- Tomahawk Cruise Missile,
- Advanced Medium-Range Air-to-Air Missile (AMRAAM),
- Joint Air-to-Surface Standoff Missile (JASSM), Long Range Anti-Ship Missile (LRASM),
- Terminal High Altitude Area Defense (THAAD), Patriot Advanced Capability-3 (PAC-3),
- Family of Affordable Mass Munitions (FAMM),
- Extended-Range Attack Munition (ERAM),
- Enterprise Test Vehicle (ETV), and
- low-cost hypersonic strike systems.

This expansive use of MYP authorities indicates that Congress may continue to relax the MYP environment, which could in turn create a steady government demand signal necessary for the industrial base to make critical capital investments, attract and retain workers, and exercise more control over margins.

Undefinitized Contractual Actions. Section 814 amends 10 U.S.C. § 3374(a) to add two new categories of increased cost risk that must be included in the government's calculations when determining profit on undefinitized contractual actions (UCAs): (1) costs incurred prior to the award of a UCA, when such costs would have been directly chargeable to the contract if incurred after the award of the contract and were incurred to meet anticipated delivery schedules or government price targets under required acquisition strategies; and (2) costs arising from negotiations that last more than 180 days from the contractor's submission of a qualifying proposal to definitize the UCA. DOD must amend the DFARS within 120 days of the NDAA's enactment to incorporate these changes.

Supply Chain Restrictions

Critical Minerals. Congress restricted DOD's ability to procure critical minerals from non-allied foreign nations, most notably China, while also appearing to concede that DOD needs more information about the supply chains for those critical minerals. The FY 2026 NDAA codifies DFARS 252.225-7052, which prohibits sourcing critical minerals — including components or elements — that are mined, refined, or separated in non-allied foreign nations (Section 848). This restriction will take effect five years after the date of enactment, which may show Congress recognizes the commercial realities of the critical minerals supply chain by giving contractors time to adapt to this new environment. Congress also added molybdenum, gallium, and germanium to the list of critical minerals that cannot be sourced from non-allied foreign nations (Section 844) and harmonized the processes to obtain waivers from both the prohibition against procurement from non-allied foreign countries and the requirement to procure from domestic or allied sources (Section 843).

Despite these new restrictions, Congress also appeared to understand the need for a more realistic approach to new sourcing restrictions. By Section 837, Congress mandated that DOD expedite qualification of compliant sources of critical minerals, consistent with recommendations from the forum to address challenges to and limitations of the defense industrial base that Congress created in Section 1844. The NDAA requires DOD to assess its own dependence on foreign entities of concern (FEOC) for critical infrastructure that DOD owns, extending to a risk assessment related to the supply chains and supply chain redundancy (Section 838).

Congress also directed DOD to provide greater specificity in reports under the Strategic and Critical Materials Stock Piling Act to require greater specificity (Section 1411). Congress directed DOD to expand critical minerals recycling programs, especially for optical grade germanium, and report to Congress regarding stockpile shortfalls, program barriers, and best practices (Section 1412).

Outbound Investment. The FY 2026 NDAA codifies and expands current outbound investment restrictions by amending the Defense Production Act (DPA) to create a mandatory notification obligation for certain investments in China or in Chinese-controlled entities relating to advanced technologies. The provision also authorizes, but does not require, the prohibition of those investments, defined as an equity interest in an entity in, or subject to the control or ownership of, a foreign country of concern, regarding a "prohibited technology," defined as a range of advanced technology, including activities involving integrated circuits, artificial intelligence, semiconductors, and quantum computing. Treasury must issue regulations outlining these requirements, which include both mandatory notification for non-prohibited but "notifiable technologies" and potential exemptions in limited national security cases, subject to congressional notification. Penalties for violations of the prohibited investment provision would include civil penalties of $250,000 or twice the value of the violative transaction; a requirement to divest of the prohibited investment; and enforcement by the Attorney General.

Supply Chain Illumination. The FY 2026 NDAA also requires DOD to continue implementation of the Supply Chain Illumination program established in the FY 2025 NDAA, under which major systems contractors must submit information about their supply chains. The NDAA incentivizes contractors to make disclosures based on information captured through that system by authorizing DOD to provide, on an interim basis through January 1, 2028, "national security waivers" when contractors promptly disclose noncompliant sources under specific sourcing requirements that were identified by their supply chain illumination systems (Section 833). DOD's national security waivers require a written determination, which must also be sent to Congress within five days of issuance, suggesting that Congress intended for the waivers to be used sparingly.

Congress directed DOD, through Section 836, to create and maintain a publicly available online database, in which offerors may submit information related to the compliance of certain products (mostly major systems or components thereof) with specific sourcing requirements. While an earlier version of Section 836 required DOD to expedite payments for contractors that register in advance, the final compromise version walks that back, requiring DOD to establish policies to incentivize contractors' advance registration, including a suggestion that DOD could implement national security waivers beyond the interim ones provided under Section 833.

Item-Specific Restrictions. While Congress did not expand restrictions on specific items as extensively as in the past, the FY 2026 NDAA includes restrictions on optical glass, computer displays, concessions contracts in military exchanges, advanced batteries, photovoltaic modules, and computers and printers. The NDAA also expands certain existing prohibitions. In particular:

- Sections 834 and 835, covering optical glass and computer displays, require DOD to develop strategies for future limits on optical glass and computer displays and to end its "dependence" on Chinese sources by 2040. DOD must brief Congress on implementation of the strategies by March 15, 2027, and must implement the strategies by January 1, 2030. For computer displays, the provision explicitly limits applicability of the restriction to computer displays acquired as end items. Earlier versions of these provisions would have made the restrictions immediately effective, but the final compromise bill's phased approach indicates a recognition of the supply chain challenges.

- Section 841 requires DOD to review long-term concessions agreements and terminate any such agreements with contractors that are controlled by a covered foreign nation and operate in a physical location on a military installation.

- Section 842 limits DOD procurement of batteries from foreign entities of concern (FEOC), i.e., companies located in, or subject to the control of, China, Russia, Iran, or North Korea. This is another example of the final FY 2026 NDAA adopting a less restrictive provision than the original because it permits exemptions that keep some FEOCs in the supply chain and extends the implementation timeline to January 1, 2028, for new contracts; January 1, 2029, for standard batteries; and January 1, 2031, for existing acquisition programs.

- Section 847 bars DOD from using funds authorized by this NDAA for photovoltaic modules and inverters from FEOCs but explicitly excludes contracts involving third-party financing arrangements.

- Section 849 bars DOD from purchasing advanced manufacturing machinery from entities on the Consolidated Screening List, effective one year after the date of enactment.

- Section 850 addresses DoD acquisition of computers or printers manufactured by a "Covered Chinese Entity," requiring that at least 10% of computers or printers acquired in FY 2026 are not from such entities, increasing to 100% of computers or printers acquired from other-than "Covered Chinese Entities" by FY 2029. "Covered Chinese Entity" is defined as an entity on the 1260H List or the Non-SDN CCMIC List; or an entity that is both (i) domiciled in or controlled by China, and (ii) on the Entity or Denied Persons Lists.

- Several provisions also relate to the 1260H List, first created under the FY 2021 NDAA. These provisions prohibit grants to 1260H List entities (Section 845), expand the 1260H list to include entities operating inside or outside China under specific government ownership or control (Section 1262), require an annual review of other U.S. government lists to identify additional entities for inclusion on the 1260H List (Section 1263), and prohibit the intelligence community from purchasing from entities on the 1260H List (Section 6703).

BIOSECURE Act. Congress also used the NDAA as the vehicle to enact the BIOSECURE Act, a government-wide ban on contracts with and financial assistance for biotechnology companies of concern, defined as any entity that "is to any extent involved in the manufacturing, distribution, provision, or procurement of any biotechnology equipment or service," and that is either (a) identified in the 1260H List; (b) subject to the control of a government of a foreign adversary; or (c) deemed to pose a risk to U.S. national security based on its connection to a foreign adversary. The Office of Management and Budget (OMB) must issue a list of companies identified as biotechnology companies of concern within one year.

The BIOSECURE Act bars any federal agency from procuring biotechnology equipment or services from a biotechnology company of concern or contracting with an entity that uses or will use biotechnology

equipment or services from such an entity during contract performance. That prohibition will take effect after the Federal Acquisition Regulation is amended to include the restriction. The BIOSECURE Act also applies those same prohibitions to federal grants and loans, barring agencies and grant recipients from contracting with or using services or products from a biotechnology company of concern.

Export Controls Under AUKUS. The FY 2026 NDAA amended export control laws to exempt transfers under the Australia-U.K.-U.S. (AUKUS) trilateral defense agreement from certain notification and consent requirements (Section 1085). Congress instead requires a report on the expedited licensing processes and updates to the Excluded Technology List. Further, the NDAA requires DOD to develop a framework, within 180 days, to reform technology transfer and foreign disclosure policies, including balancing technology protection with sharing requirements for emerging and advanced defense technologies, stakeholder engagement, transparency improvements, process streamlining, and annual audits of denied license applications, with ongoing industry feedback and congressional reporting.

Defense Industrial Base and Economic Investments

The 2026 NDAA includes various terms addressing U.S. government investments in domestic industry by both reauthorizing a cornerstone for government investment — the Defense Production Act — through September 30, 2026; and providing DOD with new authorities to support certain sectors within the defense industrial base.

Most significantly, Section 867 amends the Industrial Base Fund (IBF) statute, 10 U.S.C. § 4817, to identify the specific defense supply chain applications for IBF authorities. The provision also amends 10 U.S.C. § 4817 to specifically authorize DOD to use certain types of arrangements for the domestic industrial base, including contracts, grants, other transaction agreements, private sector incentives, third-party awards for investments in businesses with a defense interest, and subsidies to address market manipulation. However, Congress limited Section 867 by requiring DOD to use specifically appropriated funding to carry out the new IFB authorities and sunsetting those new authorities on December 31, 2035, which combined may limit DOD to shorter-term agreements using its new IFB authorities.

Section 865 expressly approves certain investments into the domestic textile and footwear industrial base. Though not providing express investment authority, Section 1844 requires the creation of one or more consortia to serve as collaborative forums to address defense industrial base challenges and limitations, and Section 1845 requires that members of the Section 1844 collaborative forum are sponsored for facility clearances.

The NDAA also includes the DFC Modernization and Reauthorization Act of 2025, making another significant update to federal economic investment. Among other things, those provisions expand the scope of authorized investments for the Development Finance Corporation.

Drones/Unmanned Air Systems (UAS)

In the wake of rising national security threats posed by unauthorized drone usage and as significant, large-scale events draw near, Congress enacted a range of provisions designed to improve and expand counter-drone authorities, along with coordination, training, and oversight provisions.

Section 912 creates Joint Interagency Task Force 401, the Director of which will report to the Deputy Secretary of Defense. The Task Force will have a range of responsibilities, including coordinating small-UAS-related

procurement efforts, maintaining a counter small-unmanned aerial systems (sUAS) strategic plan, approving counter-sUAS systems for Department use, and maintaining a list of approved systems (with limited waivers available). The Director must establish an acquisition division to operationalize counter-sUAS capabilities. The provision requires a number of reports, including annual reports on Task Force activities and a report focusing on differences in interpretations of existing counter-UAS (c-UAS) authorities among the armed services within 180 days of enactment.

Section 914 directs the Deputy Secretary of Defense to establish the "Small-UAS Industrial Base Working Group" by January 15, 2026, to analyze the supplier base for sUAS and recommend strategic investments to, for example, remediate supply chain fragility or limited availability of domestic suppliers. The section includes opportunities for public-private partnerships, including an authorization and conditions for establishment of the SkyFoundry program to rapidly scale up drone manufacturing, joint operations of certain facilities and sites, and opportunities to incubate and innovate sUAS technologies. The Working Group must submit an initial report by April 1, 2026, and biannual reports once every 180 days thereafter.

Section 1707 expands c-UAS authorities to encompass more military installations, including permitting the Department to authorize certain contractors to mitigate UAS threats. The provision expands the definition of covered facilities to include additional sites deemed critical to the national defense and — notably — assistance to federal, state, or local officials responding to certain national security incidents. Multiple provisions seek to address potential concerns arising from expanded c-UAS authorities, including requirements regarding civil aviation safety, privacy and civil liberties, and records retention. The semiannual briefing requirement has been replaced with a public reporting requirement on all detection and mitigation activities during the preceding year, with specific data requirements. The provision also creates an interagency committee to conduct ongoing review of the section's implementation with an annual reporting requirement on its activities.

Sections 8601-8606 implements the SAFER SKIES Act, which expands Department of Justice and Department of Homeland Security c-UAS authorities to "enforce the law, protect the public, or mitigate a credible threat" posed by UAS or unmanned aircraft. Subject to training, certification, notification, and oversight requirements, the provisions authorize c-UAS activities by certain state, local, Tribal, or territorial entities. The provisions also authorize the use of grant funds for UAS and c-UAS systems to benefit public safety. Multiple provisions govern penalties for UAS-related misuse, including violations of defense airspace, transportation of contraband, and unauthorized c-UAS use, including enhanced penalties for use of UAS to commit certain crimes. Within 180 days of enactment, the Departments of Homeland Security, Justice, and Transportation must develop and publish regulations governing c-UAS authorities for state, local, Tribal, and territorial agencies and correctional agencies, including FAA coordination to ensure aviation safety.

Cyber and AI

The FY 2026 NDAA directs several important initiatives to strengthen the cybersecurity posture of defense and intelligence enterprises and both promotes the deployment of AI and imposes important safeguards to protect its use in critical areas.

The FY 2026 NDAA's cybersecurity and AI provisions continue with the overall theme of streamlining requirements, while also addressing an evolving understanding of AI. To streamline, Section 866 requires DOD to harmonize cybersecurity requirements across the defense industrial base, reduce bespoke cyber

requirements, identify and eliminate duplicative requirements, and centralize approval of any sub-regulatory cybersecurity requirements. Similarly, Section 1515 requires DOD to revise its mandatory cybersecurity training within one year to include content on AI-related cybersecurity challenges, and Section 1533 requires DOD to establish a cross-functional team to create a standardized framework for evaluating, procuring, and overseeing DOD AI models, including department-wide guidelines for testing, documentation, ethics, and security.

Congress also used the bill to create multiple requirements for DOD to streamline its guidance or create new teams to do so for emerging issues.

- Section 1521 requires DOD to develop mandatory department-wide timelines for granting cloud Authorizations to Operate (ATO), and it mandates that DOD issue guidance within 180 days on expedited ATO processes and a process for appeals for expedited review. The provision also requires reports to Congress on both implementation and activities under the streamlined ATO process, signaling Congress's interest in DOD reforms.

- Section 1512 directs DOD to develop, within 180 days, a department-wide policy for cybersecurity and governance of AI and machine learning (AI/ML) systems, addressing AI/ML-specific threats, lifecycle cybersecurity measures, industry frameworks, governance standards, and workforce training. DOD must also report to Congress by August 31, 2026, with an assessment of current practices, identified security gaps, and recommended enhancements. In the Joint Explanatory Statement, Congress clarified that the DOD policies concerning software bills of materials (SBOM) should also apply, where feasible, to AI systems used, developed, or acquired by DOD, suggesting that future DOD regulations may require contractors to provide SBOMs for those items.

- Section 1513 requires DOD to develop a framework for cybersecurity and physical security standards for AI/ML technologies and to amend the DFARS to incorporate the requirements. The framework must cover workforce risks, supply chain risks, adversarial tampering, and security monitoring, drawing on the NIST SP 800 series cybersecurity requirements and augmenting the Cybersecurity Maturity Model Certification (CMMC) program.

- Section 1534 requires the secretary of defense, not later than April 1, 2026, to establish a task force on AI sandbox environments to allow for the isolated testing and training of AI.

- Section 1535 directs the establishment, by April 1, 2026, of a steering committee to direct the long-term AI strategy, analyze the trajectory of advanced and emerging AI and enabling technologies, including those that could "enable artificial general intelligence," and develop a strategy for "risk-informed adoption" of AI, among other duties.

- Section 1531 expands an FY 2025 NDAA provision that established a DOD testing program for AI, to direct DOD to create a roadmap of high-performance computing capability to consider both DOD-owned computing assets and commercially procured cloud services and infrastructure-as-a-service providers. This reflects Congress's focus on commercial resources and acknowledges that DOD's computing assets are often contracted.

Congress also used this NDAA to direct DOD to conduct certain cybersecurity and AI-focused exercises and direct continued use of certain cyber capabilities. Section 1505 requires DOD to conduct cybersecurity

tabletop exercises by September 1, 2026, and it requires those exercises to (a) experiment with doctrine, organization, training, and policy for non-kinetic cyber actions outside the current Cyber Mission Force Approach and (b) assess command and control models for integrating cyber forces into non-cyber units. DOD must also develop future operational employment concepts for planned cyber capabilities, with a report due January 1, 2027. Under Section 1507**,** Congress prohibited DOD from divesting from or changing NSA-certified cyber assessment capabilities or red teams supporting operational testing, absent a certification by the Defense Secretary. In Section 1543, Congress required DOD to submit a comprehensive study and report to Congress by December 1, 2026, examining how military capabilities can deter adversaries from targeting U.S. defense-critical infrastructure in cyberspace. The study must also assess adversary capabilities, identify ways to impose costs, evaluate required investments, and examine integration with federal agencies, allies, and industry.

Finally, the FY 2026 NDAA includes provisions with strict sourcing requirements. Section 1511 requires DOD to acquire, within 90 days of enactment, mobile phones with encryption and other security capabilities for senior officials performing sensitive national security functions under contracts requiring enhanced cybersecurity protections. Similarly, Section 1532 requires, within 30 days of enactment, exclusion and removal of AI developed by DeepSeek, High Flyer, or associated entities from DOD systems, as well as prohibiting contractors from using such AI, with limited waivers. The exclusion and removal requirements extend to contractors as well — prohibiting contractors from using DeepSeek or High Flyer (and affiliates) "with respect to the performance of a contract with" DoD. The provision also requires DOD to determine whether to issue guidance excluding AI from companies domiciled in covered nations, subject to unmitigated foreign control, and on Department of Commerce screening lists, and makes contractors subject to that guidance. Waivers are limited to research, national security analysis, and mission-critical functions. Section 6604 of the Intelligence Authorization Act applies these same restrictions to the Intelligence Community.

The Intelligence Authorization Act (FY 2026 IAA), which was included with the FY 2026 NDAA, also addresses many of the same AI and cybersecurity concerns as to the intelligence community. Section 6601 amends the AI Security Center within the NSA, as established under the FY 2025 IAA. Among its provisions, it directs the development of AI Security Guidance to defend AI technologies from technology theft by nation-state adversaries.

- In a bid to promote cost-effective adoption of AI technologies, Section 6602, directs the Intelligence Community (IC) to identify "commonly used" AI systems or functions that IC elements can reuse without significant medication, and create "model contract terms" for AI systems. These requirements ultimately mirror the preference for interoperability that appears throughout the FY 2026 NDAA.

- Section 6603 directs the IC to draft policies and standards for assessing the appropriateness of hosting publicly available AI models on classified computer systems. The rules of construction specify that the provision does not "authorize an officer or employee of the intelligence community to direct a vendor or prospective vendor to alter a model to favor a particular viewpoint."

Contacts

Alexandra Barbee-Garrett
Counsel

She/Her/Hers

Washington, D.C. D | +1.202.508.8918
abarbee-garrett@crowell.com

Olivia Lynch
Partner
Washington, D.C. D | +1.202.624.2654
olynch@crowell.com

Jonathan M. Baker
Partner
Washington, D.C. D | +1.202.624.2641
jbaker@crowell.com

Laura J. Mitchell Baker
Counsel
Washington, D.C. D | +1.202.624.2581
lbaker@crowell.com

Caroline E. Brown
Partner
Washington, D.C. D | +1.202.624.2509
cbrown@crowell.com

Jacob Canter
Counsel
He/Him/His

San Francisco D | +1.415.365.7210
jcanter@crowell.com

Adelicia R. Cliffe
Partner
She/Her/Hers

Washington, D.C. D | +1.202.624.2816
acliffe@crowell.com

Christian N. Curran
Partner
Washington, D.C. D | +1.202.624.2543
ccurran@crowell.com

Sharmistha Das
Partner
Washington, D.C. D | +1.202.624.2557
sdas@crowell.com

Riley Delfeld
Associate
Washington, D.C. D | +1.202.624.2743
rdelfeld@crowell.com

Matthew F. Ferraro
Partner
Washington, D.C. D | +1.202.624.2610
mferraro@crowell.com

Rina M. Gashaw
Counsel
She/Her/Hers

Washington, D.C. D | +1.202.624.2827
rgashaw@crowell.com

Emily P. Golchini
Associate
She/Her/Hers

Washington, D.C. D | +1.202.624.2741
egolchini@crowell.com

Kate M. Growley
Partner, Crowell Global Advisors Senior Director
Washington, D.C. D | +1.202.624.2698

Washington, D.C. (CGA) D | +1 202.624.2500
kgrowley@crowell.com

Michael G. Gruden
Partner
Washington, D.C. D | +1.202.624.2545
mgruden@crowell.com

Jacob Harrison
Associate
He/Him/His

Washington, D.C. D | +1.202.624.2533
jharrison@crowell.com

Brittany Kouroupas
Associate
Washington, D.C. D | +1.202.624.2777
bkouroupas@crowell.com

Skye Mathieson
Partner
Washington, D.C. D | +1.202.624.2606
smathieson@crowell.com

Adina Nelson
Associate
She/Her/Hers
Washington, D.C. D | +1.202.624.2596
adnelson@crowell.com

Vanessa A. Perumal
Associate
Chicago D | +1.312.379.4283
vperumal@crowell.com

Kate Robb
Crowell GovCon Strategies President
Washington, D.C. D | +1.202.688.3434
krobb@crowellgcs.com