# PRATT'S GOVERNMENT CONTRACTING LAW REPORT

**VOLUME 10** **NUMBER 5** **May 2024**



LexisNexis®

## QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please call or email:

Heidi A. Litman at ..... 516-771-2169
Email: ..... heidi.a.litman@lexisnexis.com

For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at . . . . . (800) 833-9844
Outside the United States and Canada, please call . . . . . (518) 487-3385
Fax Number . . . . . (800) 828-8341
LexisNexis® Support Center . . . . . https://supportcenter.lexisnexis.com/app/home/

For information on other Matthew Bender publications, please call

Your account manager or . . . . . (800) 223-1940
Outside the United States and Canada, please call . . . . . (518) 487-3385

Library of Congress Card Number:

ISBN: 978-1-6328-2705-0 (print)
ISSN: 2688-7290

Cite this publication as:

[author name], [article title], [vol. no.] PRATT'S GOVERNMENT CONTRACTING LAW REPORT [page number] (LexisNexis A.S. Pratt).
Michelle E. Litteken, GAO Holds NASA Exceeded Its Discretion in Protest of FSS Task Order, 1 PRATT'S GOVERNMENT CONTRACTING LAW REPORT 30 (LexisNexis A.S. Pratt)

Because the section you are citing may be revised in a later release, you may wish to photocopy or print out the section for convenient future reference.



Editorial Office
230 Park Ave., 7th Floor, New York, NY 10169 (800) 543-6862
www.lexisnexis.com

MATTHEW BENDER

(2024–Pub.4938)

# *Editor-in-Chief, Editor & Board of Editors*

*Pratt's Government Contracting Law Report* is published 12 times a year by Matthew Bender & Company, Inc.  For customer support, please contact LexisNexis Matthew Bender, 9443 Springboro Pike, Miamisburg, OH 45342 or call Customer Support at 1-800-833-9844. Direct any editorial inquiries and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 631.291.5541. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Government Contracting Law Report*, LexisNexis Matthew Bender, 230 Park Ave. 7th Floor, New York NY 10169.

# The Fiscal Year 2024 National Defense Authorization Act: Key Provisions Government Contractors Should Know—Part II

***By Adelicia R. Cliffe, Lorraine M. Campos, Maria Alejandra (Jana) del-Cerro, Olivia Lynch, Robert J. Sneckenberg, Eric Ransom and Michelle D. Coleman****

*The National Defense Authorization Act for Fiscal Year 2024 makes numerous changes to acquisition policy. In this two-part article, the authors discuss the most consequential changes for government contractors. In the first part, which was published in the April 2024 issue of* Pratt's Government Contracting Law Report, *the authors examined acquisition-related matters. In this conclusion, the authors review cyber-related sections of note, artificial intelligence-related sections of note, supply chain-related matters of note and trade-related sections of note, as well as the American Security Drone Act and the Federal Data Center Enhancement Act.*

The National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2024,[1] which President Biden signed into law on December 22, 2023, makes numerous changes to acquisition policy. This article discusses the most consequential changes for government contractors. These include changes that:

(i) Impose a new conflict of interest regime for government contractors with a connection to China;

(ii) Impose new restrictions and requirements;

(iii) Require government reporting to Congress on acquisition authorities and programs, and alter other processes and procedures to which government contractors are subject.

The FY 2024 NDAA also includes the Federal Data Center Enhancement Act, the American Security Drone Act, and the Intelligence Authorization Act for FY 2024.

---

* The authors, attorneys with Crowell & Moring LLP, may be contacted at acliffe@crowell.com, lcampos@crowell.com, mdel-cerro@crowell.com, olynch@crowell.com, rsneckenberg@crowell.com, eransom@crowell.com and mcoleman@crowell.com, respectively. Per David Midboe, Michael E. Samuels, Laura J. Mitchell Baker, Alexandra Barbee-Garrett, Michael G. Gruden, Catherine O. Shames, Rina M. Gashaw, Rachel Schumacher, Alexis Ward, Brittany Kouroupas, Lucy Hendrix, Nayar Islam, Emily P. Golchini, Dilan Wickrema and Jacob Harrison assisted in the preparation of this article.

[1] https://www.congress.gov/bill/118th-congress/house-bill/2670/text.

**CYBER-RELATED SECTIONS OF NOTE**

Section 1502 tasks the Secretary of Defense with developing a Strategic Cybersecurity Program (Program). The members of the Program will identify all systems, infrastructure, kill chains, and processes that comprise:

(1) Nuclear deterrence and strike;

(2) Select long-range strike missions;

(3) Offensive cyber operations; and

(4) Homeland missile defense.

The National Security Agency (NSA) will support the Program by identifying threats to, vulnerabilities in, and remediations for these mission elements. The NSA will also select the Program Manager, who will be responsible for conducting vulnerability assessments, prioritizing remediation efforts, reviewing systems and infrastructure, advising Secretaries of military departments, and ensuring the Program builds upon other DoD cybersecurity efforts.

Section 1507 requires DoD cyber officials to review the status of the implementation of cyber red team requirements from the NDAA for FY 2020. The officials must develop a plan to identify the funding and resources required to develop cyber red team capabilities, as well as the standards and metrics necessary to ensure sufficient training and staffing. The Secretary of Defense must then issue regulations and guidance to implement the developed plan.

Section 1512 tasks the Secretary of Defense with establishing a cross-functional team to develop a threat-driven defense construct for the systems and networks that support the nuclear command, control, and communications (N3) mission. The team will also develop associated plans and milestones. The construct will be based on zero trust architecture, comprehensive endpoint and network telemetry data, and control capabilities that enable rapid investigation and remediation of threats.

Section 1521 allows the Chief Digital and Artificial Intelligence Officer to access and control any data collected, acquired, accessed or used by any component of the DoD. Section 1521 also requires that the Secretary establishes the Chief Digital and Artificial Intelligence Officer Governing Council to provide policy oversight that ensures responsible, coordinated, and ethical employment of data and AI capabilities across the DoD.

Section 1522 requires the executive agent of the DoD-wide cyber data products and services procurement program to evaluate emerging cyber technologies, specifically AI-enabled security tools, for efficacy and applicability to the requirements of DoD.

Section 1523 tasks the Chief Digital and Artificial Intelligence Officer with providing the digital infrastructure and procurement vehicles necessary to

manage data assets and analytics capabilities. These capabilities should enable an understanding of foreign key terrain and relational frameworks to support cyber operation plans, military operation warnings, and strategic competition actions and reactions.

Section 1535 creates a pilot program to contract for services relevant to the Cyber Mission. The pilot program will seek to enter into one or more contracts under which skilled personnel will provide support for critical work within the Cyber Mission Force to enhance readiness and effectiveness of the Cyber Mission Force. Over a three-year period, the Commander of the United States Cyber Command will determine whether to extend the pilot program, transition the program to a permanent program, or terminate the program.

Section 1552 requires that, within one year of enactment, DoD must review and implement the recommendations from the February 2023 DoD Inspector General report on managing mobile applications titled "Management Advisory: The DoD's Use of Mobile Applications."[2] This section also requires that, within 120 days of enactment, DoD must brief the congressional defense committees on compliance efforts relating to existing DoD policy that prohibits (1) the installation and use of "covered applications" (i.e., TikTok, or other apps developed by ByteDance Limited or its affiliates) on federal government devices, and (2) the use of such covered applications on the DoD Information Network on personal devices.

**AI-RELATED SECTIONS OF NOTE**

Section 1541 requires the Under Secretary of Defense for Acquisition and Sustainment, within thirty days of enactment, to prepare a plan regarding the exercise of the acquisition authority provided to the Joint Artificial Intelligence Center in the FY 2021 NDAA. In addition, within 90 days of enactment, the Chief Digital and Artificial Intelligence Officer (CDAIO) must provide a demonstration of operational capability under the acquisition authority. This demonstration must include how the CDAIO may use the acquisition authorities of DoD and other federal entities to further DoD's data and artificial intelligence objectives.

Section 1542 requires the CDAIO, within 180 days after enactment of the NDAA, to develop a bug bounty (ethical hacking) program for "foundational artificial intelligence models"—defined as adaptive generative models that are trained on a broad set of unlabeled data sets that may be used for different tasks with limited fine-tuning—that are integrated into DoD's missions and operations. Notably, the section states that neither the use of foundational artificial

[2] Report No. DODIG-2023-041.

intelligence models nor the implementation of the bug bounty program is required in DoD's missions and operations.

Section 1543 requires DoD to establish a Generative AI Detection and Watermark Prize Competition, open to federally funded research and development centers, the private sector, the defense industrial base, institutions of higher education, federal departments and agencies, and others. The competition will be designed to evaluate technology, tools, and models for generative AI detection and generative AI watermarking to facilitate the research, development, testing, evaluation, and competition of the technologies to support military warfighting requirements and to transition these types of technologies, including technologies developed under pilot programs, prototype projects, or other research and development programs, from prototype to production. The prize competition must be established within 270 days of enactment, and expires on December 31, 2025.

Section 1544 requires the Secretary of Defense within 120 days of the NDAA's enactment to establish policies and guidance for the adoption and use of AI, including plans for identifying commercially available large language models and make them available on classified networks, where appropriate. This section also requires creation of a policy for contracting officials to protect the intellectual property of commercial entities that provide artificial intelligence algorithms.

Section 1545 requires the Secretary of Defense to complete a study within one year of enactment to assess the functionality, research and development needs, and vulnerabilities to privacy, security, and accuracy of AI enabled military applications.

**SUPPLY CHAIN-RELATED MATTERS OF NOTE**

Section 804 prohibits DoD from entering into a contract with any person or entity that has fossil fuel business operations with an entity that is greater than 50% owned by either an authority of the government of the Russian Federation or a fossil fuel company that operates in the Russian Federation.

Section 805 prohibits DoD from entering into a contract for the procurement of goods and services from an entity on the 1260H list (Entity Prohibition) or contracting for goods and services that include goods or services produced or developed by an entity on the 1260H list or any entity subject to the control of an entity on the 1260H list (Goods and Services Prohibition).

The prohibitions do not extend to purchases of goods, services, or technology that connect goods or services to third party services (e.g., interconnection) or to components, defined broadly as an item supplied to the federal government as part of an end item or of another component. The

provision requires DoD to issue rules implementing the provision within 180 days of enactment for the Entity Prohibition and 545 days of enactment for the Goods and Services Prohibition. Section 805 becomes effective on June 30, 2026 for the Entity Prohibition and June 30, 2027 for the Goods and Services Prohibition.

Section 825 contains two prohibitions designed to curb the use of the LOGINK logistics software used in the People's Republic of China. The provision prohibits DoD from entering into contracts with entities that provide data to "covered logistics software," defined as LOGINK or any national transportation logistics information platform provided or sponsored by a foreign adversary or a commercial entity controlled by the government of an adversary. The provision also prohibits the Department of Transportation from providing federal grant funding to port authorities that use covered logistics software.

Section 833 amends 10 U.S.C. § 4863 to narrow the qualifying country exception for specialty metals. Under the provision, any specialty metal that is procured as a mill product or incorporated into a component must be melted or produced in the United States, the country where mill product or procurement is procured, or another qualifying country. In addition, the supplier of components or systems made of aerospace-grade metals—those that require provenance-tracking to comply with flight safety regulations—must inform DoD if any of the materials were known to be manufactured or processed in China, Iran, North Korea, or Russia.

Section 834 amends 10 U.S.C. § 4872(c) to narrow the non-availability exemption for specialized materials to require DoD to identify a specific end item for which a specific covered material cannot be procured as- and when-needed at a reasonable price. The provision also limits non-availability waivers to 36 months.

Section 856 requires DoD to establish and carry out a pilot program to analyze, map, and monitor key U.S. Indo-Pacific Command system supply chains for up to five covered weapons platforms identified in FY 2021 NDAA § 1251(d)(1), to identify impediments to production and opportunities to expand production of components, identify potential risks and vulnerabilities, and identify critical suppliers. The pilot program must be established within 90 days of enactment. To carry out the pilot program, the provision allows DoD to use a combination of commercial tools and other tools available to it, including AI and machine learning tools.

## TRADE-RELATED SECTIONS OF NOTE

### Matters Relating to the AUKUS Partnership

Sections 1331 through 1352 relate to the AUKUS Partnership. Section 1352 authorizes the president to transfer up to three Virginia Class submarines to the government of Australia on a sale basis and enables the president, with certain requirements, to determine what shipyard in the United States, Australia, or the United Kingdom can perform any repair or refurbishment of a United States submarine involved in AUKUS.

In addition to the submarine transfer, Section 1331 requires the Secretary of State to designate a senior advisor to coordinate the department's internal and diplomatic efforts related to the AUKUS initiative. Section 1331 also requires the Department of State (DoS) to establish an AUKUS Industry Forum and to provide reports to Congress on, among other topics:

(1) Processing times for Direct Commercial Sales (DCS) and Foreign Military Sales (FMS) authorizations to Australian and UK persons;

(2) The number of applications for transfers to Australian and UK persons that were denied or approved with provisos;

(3) Voluntary disclosures resulting in a violation of the International Traffic in Arms Regulations (ITAR), or involving U.S. arms embargoed countries, by Australian or the UK persons;

(4) The adoption of a U.S. classification category relating to any anticipatory disclosure policy for Australia and the United Kingdom; and

(5) Whether regulatory changes to exemptions under the Arms Export Control Act are likely or necessary within the next year.

Section 1333 mandates that the president submit to Congress the text of any non-binding instruments relating to the AUKUS partnership and a report that includes information regarding, but not limited to: (1) progress made on achieving the Optimal Pathway established for Australia's development of conventionally armed, nuclear-powered submarines, and (2) progress made on Pillar Two of the AUKUS partnership.

Section 1341 mandates that the president institute policies to expedite the review of Letters of Request related to AUKUS and to create an anticipatory release policy and an expedited decision-making process for the transfers of technologies associated with AUKUS to Australia, the United Kingdom, and Canada through FMS and DCS that are not covered by an exemption under the ITAR.

Section 1343 requires, within 120 days of the NDAA's enactment, the president to determine and certify in writing to Congress whether Australia or the United Kingdom has implemented: (1) a system of export controls comparable to those of the United States, and (2) a comparable exemption from its export controls for the United States. If there is a determination that the comparability standards have been met, the president is required to exempt transfers of defense articles and defense services between the United States and that country or countries from the approval requirements. If the comparability standards are not met, the president must reassess the requirements every 120 days. Any of the three countries can exclude transfers from eligibility for the exemption, and certain items—largely nuclear, missile, or chemical proliferation related—are also excluded, as well as transfers involving persons not approved by three countries. The president also has the power to suspend an exemption under specified circumstances. Any exemption specified under this provision has a sunset of 15 years which can be renewed by the Secretary of State for five years.

Section 1344 mandates that the Secretary of State initiate a rulemaking to establish an expedited decision-making process, classified or unclassified, for applications to export between and among Australia, the United Kingdom, and Canada defense articles and defense services that are not covered by an exemption under the ITAR.

Section 1345 amends Arms Export Control Act Section 38(f)(3) to waive the congressional notice requirements for establishing a country exemption for Australia or the United Kingdom, and it mandates that the Department of State carry out reviews of the United States Munitions List not less frequently than every 3 years.

**Exportability**

Section 810 directs the Under Secretary of Defense for Acquisition and Sustainment to update guidance on planning for exportability for certain defense programs. Specifically, within one year of the NDAA's enactment, guidance should require (1) major defense acquisition programs, and (2) programs carried out using the rapid fielding or rapid prototyping acquisition pathway that transition to a major capability acquisition program to review their exportability.

Additionally, within 3 years of enactment, the Under Secretary is to update guidance for program protection plans to determine exportability needs for such programs.

Section 873 requires the Under Secretary to annually compile a list of systems that would benefit from investment in exportability features to support the security cooperation objectives of the regional theaters.

**Combating Global Corruption Act**

Section 5405 specifies that the executive branch should evaluate, for the purposes of potential imposition of sanctions, whether there are foreign persons engaged in significant corruption in: (1) specific countries that do not meet minimum standards for the elimination of corruption, and (2) relation to the planning, construction, or operation of the Nord Stream 2 pipeline.

**Foreign Military Sales Updates**

Section 873 introduces new requirements related to visibility of foreign acquisition programs. Among other requirements, it instructs the Under Secretary for Defense Acquisition and Sustainment and each military department to appoint an individual to serve as a single point of contact for foreign military sales (FMS) inquiries from the defense industrial base and partner countries.

Additionally, it requires the Secretary of Defense to host an annual industry day to raise awareness about FMS—enabling U.S. companies to learn about foreign demand for U.S. weapons systems and foreign governments to learn about U.S. solutions. The section also requires the Secretary of Defense to create an advisory group made up of senior defense industrial base employees to advise on DoD's role in the FMS process.

**Human Rights and Sourcing Critical Minerals**

Section 5411 directs the Secretary of State to convene a meeting of foreign leaders to establish a multilateral framework to end human rights abuses, including forced labor and child labor that is related to mining and sourcing critical minerals. The Secretary is also required to lead the development of an annual global report on the implementation of this multilateral framework, which should discuss progress and recommendations to end such human rights abuses.

**Other Department of Defense Organization and Management Matters**

Section 918 requires the Secretary of Defense to improve the policies, processes, and procedures applicable to technology release and foreign disclosure decisions by DoD.

**AMERICAN SECURITY DRONE ACT**

The "American Security Drone Act of 2023" prohibits executive agencies from procuring unmanned aircraft systems that are manufactured or assembled by a "covered foreign entity," with limited exceptions. Covered foreign entities are those:

(1) Included on the Consolidated Screening List;

(2) Subject to a foreign government's extrajudicial direction;

(3) Domiciled in or subject to control by the People's Republic of China; or

(4) Deemed to pose a national security risk. The Act also requires agencies to account for any existing inventory of unmanned aircraft manufactured or assembled by covered foreign entities.

The Act further requires the Office of Management and Budget—in connection with the Department of Homeland Security, DOJ, and National Institute of Standards and Technology—to establish a government-wide policy for any unmanned aircraft system procurements that meet the narrow set of exceptions to the Act's general rule, given that they serve non-DoD or intelligence community operations through non-federal grants or cooperative agreements.

Finally, the Act obligates the Under Secretary of Defense for Acquisition and Sustainment to provide to Congress a report on the supply chain for covered unmanned aircraft systems, including a discussion of current and projected future demand for covered unmanned aircraft systems.

**FEDERAL DATA CENTER ENHANCEMENT ACT**

Sections 5301 and 5302, titled the Federal Data Center Enhancement Act of 2023, revise the recently expired Federal Data Center Optimization Initiative to address the government's evolving need for secure, reliable, and protected data centers, while continuing to consolidate data centers and prioritize cost savings. The Act establishes three requirements to address these objectives.

First, the Act amends 44 U.S.C. § 3601 to include minimum operating requirements that relate to availability, use, overhead costs, uptime percentages, and various safety and security protections for new data centers. The General Services Administration (GSA) must establish these requirements within 180 days of the NDAA's enactment and incorporate the same requirements for existing data centers within 90 days of establishment.

Second, the Act requires guidelines for covered agencies to operate their existing data centers. These guidelines must require the head of a covered agency to (1) regularly assess and update its application portfolio to properly utilize modern technologies, and (2) leverage commercial data center solutions, like hybrid cloud, multi-cloud, co-location, interconnection, or cloud computing.

Third, the Act requires the GSA administrator to maintain a public facing website with information, data, and explanatory statements regarding agencies' compliance with the above requirements. Website content must be updated biannually and be maintained as open government data assets.