wiley

ALERT

Important NDAA Provisions for Contractors and Their Supply Chains

December 18, 2023

On December 14, 2023, the House of Representatives passed the National Defense Authorization Act for Fiscal Year 2024 (NDAA), following the Senate's passage a few days earlier. The President is expected to sign the NDAA into law soon. Below are some provisions of the NDAA that will impact government contractors, as well as some notable provisions that were introduced but not included in the final version of the NDAA. Although much of the NDAA will take effect immediately, some provisions, including those that will result in changes to government contracts regulations or modifications to existing contracts, will go into effect at a later date. In the interim, contractors should consider how these provisions, and the compliance obligations that may result, may affect their business.

Restrictions on certain foreign purchases (Sections 804, 805, 812, 825, 835, and 1821-1833). Similar to last year's act, the NDAA emphasizes Congress's focus on domestic preference and avoidance of acquiring goods or services from companies with ties to our adversaries. The NDAA will increase the domestic content requirements for major defense acquisition programs to help develop a secure domestic supply chain.

The NDAA also prohibits the U.S. Department of Defense (DOD) from obtaining logistics software from the People's Republic of China, the Republic of Cuba, the Islamic Republic of Iran, the Democratic People's Republic of Korea, the Russian Federation, and the Bolivarian Republic of Venezuela under the regime of Nicolas Maduro Moros. The NDAA also prohibits DOD from procuring certain goods, services, and technologies from Chinese military companies, in addition to prohibiting DOD from contracting with any natural gas, oil, or coal company operating in Russia or doing business with the Putin

Authors

Tracye Winfrey Howard
Partner
202.719.7452
twhoward@wiley.law

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

J. Ryan Frazee
Partner
202.719.3751
jfrazee@wiley.law

Joshua K. Waldman
Associate
202.719.3223
jwaldman@wiley.law

Scott Bouboulis
Associate
202.719.4434
sbouboulis@wiley.law

Practice Areas

Buy American and Trade Agreements Acts
Cost Accounting and Cost Allowability
Cybersecurity
Government Contracts
National Security
Small Business Programs and Nontraditional Defense Contractors
Strategic Competition & Supply Chain
Telecom, Media & Technology
Uncrewed Aircraft Systems (UAS)

regime. The NDAA includes a provision aimed at perceived conflicts of interest for entities that provide consulting services to DOD and also do business with the Chinese or Russian governments. Companies that provide consulting services to DOD will have to certify that neither they nor their subsidiaries or affiliates currently holds a contract with the Russian or Chinese governments or the government of any country on the State Department's list of terrorist sponsors.

The NDAA also includes the American Security Drone Act of 2023, which prohibits the U.S. Government from procuring or operating Unmanned Aircraft Systems (UAS) manufactured or assembled by covered entities. The prohibitions extend to UAS services provided to the Government by contractors. A list of covered entities will be published by the Federal Acquisition Security Council and listed on SAM.gov, and will include the Consolidated Screening List and entities identified as subject to foreign control by the U.S. Department of Homeland Security.

Facilitating acquisitions of emerging technologies (Sections 229, 809, 1543, and 1544). The NDAA includes several provisions aimed at facilitating DOD's access to and procurement of new technologies. To that end, the NDAA provides the Secretaries of the military departments the authority to initiate development activities for up to one year to leverage emergent technological advancements to address immediate military threats. The NDAA also directs DOD to establish a pilot program to explore the use of consumption-based solutions to quickly address defense needs. This "anything-as-a-service" pilot program will focus on technology-supported capabilities that utilize any combination of software, hardware, equipment, data, and labor to provide capabilities that are billed based on actual usage at fixed price unites.

Consistent with the Artificial Intelligence (AI) Executive Order released earlier this year, the NDAA directs DOD to develop processes for determining whether AI technologies are developed and functioning responsibly. The NDAA also directs DOD to carry out a prize competition to identify technologies capable of detecting and watermarking generative AI.

Commerciality of defense systems (Sections 230 and 801). Building on last year's requirement for offerors to establish the commercial nature of any subsystems, components, and spare parts, the NDAA requires DOD to share the contracting officer's ultimate commerciality determination upon the contractor's request. Contractors could then rely on those decisions in their commerciality assertions to other contracting officers or prime contractors. The NDAA also directs the Air Force to establish a pilot program to award grants for contractors to commercialize Air Force prototypes.

Greenhouse gas (GHG) emission disclosures (Section 318). Last year, the Federal Acquisition Regulatory (FAR) Council issued a proposed rule that would require certain contractors to make representations regarding GHG emissions and climate-related financial risk. The NDAA prohibits DOD from using federal funds to make such representations a condition of an acquisition.

Updates to contractors' cost or pricing data obligations (Sections 802 and 826). Consistent with Congress's ongoing interest in perceived inflated prices for parts procured on a sole-source basis from commercial suppliers, the NDAA includes two provisions related to contractors' submission of cost or pricing data. The

NDAA directs the Under Secretary of Defense for Acquisition and Sustainment to define actions of a contractor that constitute a denial of "uncertified cost or pricing data," and to make a public notation of offerors that have failed to provide certain cost or pricing data within 200 days of request. This information will also to be included in the Under Secretary's annual report to the leadership of the offerors named in the report. The NDAA also extends for Fiscal Year 2024 the authority granted to DOD in the FY 2023 NDAA to modify contracts to provide for appropriate economic price adjustments to address inflation. Such modifications are discretionary and depend in part on the availability of funds.

Continued focus on small business contractors (Sections 862, 863, and 865). In an effort to help small business contractors in particular, the NDAA emphasizes the need for prime contractors to make full and timely payments to their subcontractors. Should the contracting officer determine that those payments have not been made, the NDAA requires prime contractors to cooperate with contracting officers in their efforts to ensure full payment to the subcontractor. The NDAA also increases the government-wide participation goal for procurements from service-disabled veteran owned small businesses. The NDAA also directs DOD to amend its supplement to the FAR to require contracting officers to consider the past performance of affiliates when evaluating small businesses' offers.

Expanded cybersecurity programs and operations (Sections 1502, 1506, 1507, 1512, 1519, 1535, 1536, 1545, and 3113). The NDAA creates programs to dedicate focused cybersecurity capabilities and resources to protect designated weapons systems such as nuclear weapons and homeland missile defense, as well as DOD laboratories. It promotes and expands DOD's use of red teaming, including foreign adversary emulation and vulnerability assessments for major weapons systems and DOD critical infrastructure. A provision directs DOD to pilot civilian and contractor participation in its operational cyber forces, and another creates dedicated cyber support for geographic combatant commands.

Focus on critical infrastructure supporting DOD operations (Sections 1514, 1517, 1526, 2809, and 2853). The NDAA contains several provisions focusing on DOD critical infrastructure and critical infrastructure systems that support DOD operations, consistent with an increased focus on adversaries such as China and Russia's capabilities and intent to disrupt DOD deployments by hacking supporting infrastructure. One provision establishes a series of exercises that will test restoration of power, water, and telecommunications infrastructure that support DOD facilities in the event of a significant cybersecurity incident that disrupts state and local infrastructure, while others direct an assessment of risks to federally-owned critical infrastructure on military installations and authorize DOD to transfer to eligible private sector entities data and technology that protect electricity distribution industrial control systems. Another provision directs DOD to develop a strategy for deploying private networks based on 5G and open radio access network (Open RAN) architecture to DOD bases and facilities.

Continued enhancements for supply chain security (Sections 1513 and 6306). The NDAA creates a pilot program for the National Security Agency's Cybersecurity Collaboration Center to improve the cybersecurity of the supply chain for the design, manufacturing, assembly, packaging, and testing of semiconductors, including protecting against intellectual property theft of those capabilities. Another provision establishes a fund for the State Department to advance the adoption and deployment of secure and trustworthy information and

communications technology (ICT) infrastructure and services.

Protections for federal employee mobile devices (Sections 1552 and 6308). The NDAA directs DOD to create a department-wide mobile device and application acceptable use policy to address cybersecurity and operational security risks. It also authorizes the State Department to provide cybersecurity protection for the department-provided mobile devices and IT equipment of department personnel who are "highly vulnerable" to cybersecurity incidents.

Short-term extension of Foreign Intelligence Surveillance Act (FISA) 702 authority (Section 7902). The NDAA includes a "clean," short-term extension of FISA 702 authority until April 19, 2024. As Wiley has noted, there is a spirited debate underway in Congress about potential changes to the program. The NDAA extends the deadline for the program's expiration without making changes. We expect debate to continue around the competing reauthorization proposals until the new program expiration date in April.

Key provisions left out. An earlier version of the NDAA included a provision prohibiting DOD from providing funding to education institutes for research with government agencies or defense laboratory systems in the People's Republic of China. The NDAA also omitted a provision included in an earlier version which would have prohibited DOD from acquiring computers or printers from companies owned or otherwise controlled by the Chinese government.

An earlier version of the NDAA would have established a pilot program in which contractors that filed, and ultimately lost, contract award bid protests at the Government Accountability Office would be required to reimburse DOD for the expenses it incurred as a result of the protest. The final version of the NDAA also omitted a provision that would have provided DOD the authority to withhold contractual payments to a contractor for the pendency of any investigation into whether the contractor offered or made payments to federal officers, officials, or employees in an attempt to influence a contract.

Earlier versions of the NDAA also included a requirement for regulations that would require U.S. persons to notify the Secretary of the Treasury of transactions in "critical capabilities sectors" involving adversary countries, limitations on DOD obtaining certain types of data from data brokers, and reforms to the Federal Information Security Management Act. These proposals did not make into the final bill.

***

Wiley's Government Contracts, Telecom, Media & Technology, and National Security practices closely track implementation of the NDAA and are prepared to update and help clients navigate any of the issues addressed by the law.