Updates
December 29, 2022

The FY 2023 National Defense Authorization Act: Key Provisions Relevant to Defense Contractors

Inflation relief for defense contractors, a ban on procurement of products and services containing certain Chinese semiconductors, and codification of the Federal Risk and Authorization Management Program (FedRAMP) governing cloud security are among the key provisions relevant to defense contractors in the Fiscal Year (FY) 2023 National Defense Authorization Act (NDAA), which President Biden signed into law on December 23, 2022.

The 2023 NDAA provides $857.9 billion in FY 2023—an $80 billion increase over FY 2022. As in prior years, the NDAA is a vehicle for enacting legislation related to U.S. Department of Defense (DOD) acquisition. Among other things, it provides funding for the DOD's use of artificial intelligence (AI) and emerging technology as well as new restrictions on the procurement of goods and services using Chinese semiconductor technologies.

In this Update, we provide a summary of key provisions from the 2023 NDAA affecting government contractors and their implications.

Inflation Relief

Recognizing the impact of high inflation on contractors, the NDAA authorizes prime contractors to seek an adjustment to their contract price if the cost of performing the contract exceeds the contract price due "solely" to inflation. (Section 822). Such relief is also available to subcontractors, who may submit requests for contract adjustments through the prime or directly to a contracting officer. The price adjustments are contingent upon continued performance and are limited to a contractor's "actual cost of performing" the contract or subcontract.

The impact of the provision on industry is far from clear. Although the NDAA authorizes adjustments due to inflation, it does not obligate contracting officers to grant them, and the provision will require appropriated funds. The bill directs the DOD to issue guidance implementing the provision within 90 days of passage of appropriations. The DOD's guidance should shed additional light on what qualifies as an eligible contract (i.e., whether relief is limited to firm fixed-price contracts) and what support the contractor must provide to secure relief. However, it remains to be seen how meaningful this relief will be for contractors hit hard by inflation.

Restrictions on Chinese Semiconductors in Federal Government Supply Chains

The NDAA contains a significant new provision prohibiting executive agencies from contracting with entities that obtain certain semiconductor products or services from certain Chinese entities. By December 2027, executive branch agencies may no longer acquire electronics containing semiconductor products or services covered by U.S. export controls and restrictions without a waiver. (Section 5949). The new law defines "covered semiconductor parts or services" subject to the ban as semiconductor products—or services that utilize such products—that are designed, produced, or provided by: (1) Semiconductor Manufacturing International Corporation (SMIC); (2) ChangXin Memory Technologies (CXMT) or Yangtze Memory Technologies Corp

(YMTC); or (3) an entity that the secretaries of defense or commerce, in consultation with the director of national intelligence or the director of the Federal Bureau of Investigations (FBI), determines to be an entity owned or controlled by, or otherwise connected to, the government of a foreign country of concern. Section 5949 will require a rulemaking process before it becomes binding on contractors. By December 2025, the Federal Acquisition Regulatory Council (FAR Council) is required to prescribe implementing regulations, including a requirement that prime contractors flow down the substance of these prohibitions to suppliers via subcontracts and purchase orders.

FedRAMP Codification

Of relevance to companies seeking to sell cloud-based services to the government, the NDAA codifies into law FedRAMP, a government-wide certification and risk management program for cloud services overseen by the General Services Administration (GSA). (Section 5921). Although FedRAMP has existed since 2011, it has not been the subject of specific statutory authority until now. The FedRAMP Authorization Act (the Act) included in the NDAA sets forth specific statutory mandates and standards to guide FedRAMP in providing a government-wide, standardized certification and assessment process for acquiring secure cloud services. The Act establishes a FedRAMP board, a public-private cloud advisory committee, and other measures aimed at streamlining and accelerating government-wide implementation. The GSA is tasked with providing a public online repository with timely guidance and resources for FedRAMP customers. The provisions of the Act will be codified at 44 U.S.C. §§ 3607-3616.

The authorization of FedRAMP is significant given the government's increasing demand for cloud-based computing and industry's desire to market cloud services across agencies. Indeed, according to GSA's most recent data, 290 cloud services have been FedRAMP-authorized.

Focus on AI and Emerging Technologies

As with prior NDAAs in recent years, the 2023 NDAA promotes the DOD's use of AI and acquisition of emerging technologies, including directing the DOD to do the following:

- Establish priority enterprise projects for data management and AI to increase efficiency and enhance warfighting capabilities (Section 1513).
- Develop a five-year roadmap and implementation plan for adopting AI systems and data management processes for the DOD's cyber operations forces. (Section 1554). The roadmap will include identifying how the DOD's AI systems can reduce threats from AI; how the DOD plans to acquire relevant AI systems; roles and responsibilities of DoD entities; long-term technology gaps to be addressed by AI-related research; and assessing threats from foreign adversaries' use of AI.

Cybersecurity Testing of Commercial Products and Cloud Services

The NDAA directs the DOD to implement a policy for testing and evaluating the cybersecurity of the commercial cloud service providers that contract with the DOD for storage or computing of classified DOD data. (Section 1553). The NDAA also directs the DOD to develop plans to test and evaluate commercial products that the DOD uses to meet its own cybersecurity requirements to ensure the products are effective and survivable prior to operation on a DOD network. (Section 1514). The DOD has until February 1, 2024, to issue implementing regulations.

The final NDAA omitted a closely watched proposal to require that contractors provide a software bill of materials (SBOM) on covered existing contracts and requests for proposals. Like a list of ingredients on food packaging, an SBOM provides a formal record of the details and supply chain relationships of various components used in building software.

The House-passed version of the NDAA would have gone further by requiring contractors furnishing software not only to provide the SBOM, but also to certify that the items are free from all known vulnerabilities or defects affecting the security of the end product or service. This provision was dropped from the final bill after facing criticism from information technology (IT) trade associations as vague, premature, and inconsistent with other industry and government initiatives.

Still, scrutiny of software supply chains and development practices is increasing. Agency initiatives to implement Section 4 of President Biden's May 12, 2021, Executive Order on Improving the Nation's Cybersecurity (the Executive Order)—which is focused on software supply chain security—are underway, including a FAR Case (2023-002) addressing software development requirements. In a September 14, 2022, memorandum to executive departments and agencies regarding the implementation of the Executive Order, the White House Office of Management Budget (OMB) instructed agencies to only use software provided by software producers who can attest to complying with certain software development practices as described in National Institute of Standards and Technology (NIST) guidance. The OMB also stated that agencies may require SBOMs in their solicitation requirements.

Rapid Acquisition Procedures

The bill authorizes and directs the DOD to prescribe new procedures for the urgent acquisition and deployment of capabilities to respond to operational needs. (Section 804). The DOD may determine a need for urgent acquisition and deployment where there is a "deficiency" resulting from combat casualties or certain contingency operations or cyberattacks that could result in loss of life or critical mission failure.

Capabilities that may be subject to the rapid acquisition procedures include those that can be fielded within two to 24 months, do not require substantial development effort, are based on proven and available technologies, and can be acquired under fixed-price contracts.

Greater Oversight for Commercial Products Used in Major Weapon Systems

The NDAA amends existing law allowing contracting officers to acquire subsystems and spare parts for major weapon systems as commercial products to specify certain data that must be obtained from contractors. (Section 803). Contractors offering subsystems or spare parts for major weapons systems as commercial products for which there is no existing determination of commerciality must submit all three of the following:

- A description of the comparable commercial product sold to the public or nongovernmental entities demonstrating that the product is "of a type" customarily used by the general public or by nongovernmental entities for nongovernmental purposes;
- A comparison of the physical characteristics and functionality between the subsystem and the commercial product; and
- The National Stock Number (NSN) for the comparable commercial product and the subsystem, if assigned.

The NDAA also provides new requirements for establishing price reasonableness for these subsystems and spare parts offered as commercial products, requiring offerors to submit either (1) a representative sample of the prices paid for the same or similar commercial products under comparable terms and conditions by both government and commercial customers, and the terms and conditions of such sales; or (2) a representative sample of the prices paid for the same or similar commercial products sold under different terms and conditions, and the terms and conditions of such sales. If the contracting officer determines the foregoing is insufficient to determine price reasonableness, then other relevant information may be used.

Other Transaction Authority Clarification

As in past years, the DOD's use of its "other transaction" (OT) authority to fund prototype projects with the possibility for follow-on procurement contracts is once again the subject of attention in this year's NDAA.

The bill clarifies the meaning of "prototype projects," which may be performed under agreements using the DOD's OT authority, 10 U.S.C. § 4022. (Section 843). The bill specifies that the term "prototype project" includes a project that addresses: (1) a proof of concept, model, or process, including a business process; (2) reverse engineering to address obsolescence; (3) a pilot or novel application of commercial technologies for defense purposes; (4) agile development activity; (5) the creation, design, development, or demonstration of operational utility; or (6) any combination of the foregoing. The bill provides that the DOD may establish a pilot program to run through September 2025 for prototype projects that enhance the DOD's ability to prototype the design, development, or demonstration of new construction techniques or technologies to improve military installations.

Whistleblower Protections for Grantees, Sub-Grantees, and Personal Service Contractors

The bill clarifies the whistleblower protections found at 10 U.S.C. § 4701 (applicable to defense contracts) and 41 U.S.C. § 4712 (applicable to civilian contracts) as extending to grantees, sub-grantees, and personal services contractors. (Section 807). While existing law prohibits reprisals against employees of grantees, sub-grantees, and personal services contractors who report gross mismanagement; abuse of authority; violations of law, rule, or regulation; or public health or safety danger, certain provisions of the whistleblower statutes, including those relating to investigations and remedies, did not expressly include the terms "grantee" or "sub-grantee," causing confusion with regard to the scope of the statute. These revisions are intended to provide clarity both to agencies and to the recipients of federal funds.

Extension of Pilot Program To Accelerate Contracting and Pricing Processes

The bill also extends a pilot program instituted by the 2019 NDAA allowing contracting officers to deviate from the requirements of the Defense Federal Acquisition Regulation Supplement (DFARS) 215.403-1(c)(4)(A), which establish a procedure for obtaining a waiver of cost or pricing data under exceptional circumstances. (Section 818). The class deviation, which permits contracting officers to determine price reasonableness on contracts in excess of $50 million based on actual cost and pricing data for similar DOD products—rather than based on certified cost and pricing data—will be extended by another 12 months such that contracting officers need not first determine that the property or services cannot reasonably be obtained without granting of the waiver, or that there are demonstrated benefits to granting the waiver, before waiving requirements to submit cost or pricing data. The extension of the pilot program does not change the requirement that the contracting officer must still determine that the price is fair and reasonable without the submission of certified cost or pricing

data before granting the waiver.

*This update was also published on January 13, 2023, here on *Westlaw Today*.

Authors

Alexander O. Canizares

Partner
ACanizares@perkinscoie.com 202.654.1769

Explore more in

Government Contracts

Related insights

Update

Ninth Circuit Rejects Mass-Arbitration Rules, Backs California Class Actions

Update

CFPB Finalizes Proposed Open Banking Rule on Personal Financial Data Rights