wiley

ALERT

What Government Contractors Need to Know About the Fiscal Year 2022 NDAA

December 21, 2021

On December 15, 2021, Congress passed the National Defense Authorization Act (NDAA or Act) for Fiscal Year (FY) 2022, which President Biden is expected to sign into law soon. As usual, the NDAA contains numerous provisions that impact government contractors. Below are some of the key highlights of what made it into the final version of the NDAA, as well as important provisions that ultimately did not make the cut.

Supply chain readiness remains a focus (Sections 802, 841-848, 851). The systemic shock of COVID-19 on international supply chains is reflected in the NDAA, with several provisions that are designed to strengthen the supply chain for critical defense items. The U.S. Department of Defense (DOD) will be required to collect supply chain risk information, perform risk assessments, and develop mitigation strategies. The NDAA also emphasizes developing regional supply chains, including increasing domestic content in major defense acquisition programs, and requires better forecasting to reduce supply chain fluctuations for dual-use items that have both military and non-military applications. The Act prohibits procurement of products mined, produced, or manufactured by forced labor from the People's Republic of China's Xinjiang Uyghur Autonomous Region or any entities that used forced labor from that region. And as specifically related to COVID-19, the bill also prohibits procurement of personal protective equipment (PPE) from China, Russia, Iran, and North Korea. The Act also delays until January 1, 2027 implementation of the sourcing restrictions on printed circuit boards from those same countries, which were included in the FY2021 NDAA.

Authors

Tracye Winfrey Howard
Partner
202.719.7452
twhoward@wiley.law

Kara M. Sacilotto
Partner
202.719.7107
ksacilotto@wiley.law

J. Ryan Frazee
Partner
202.719.3751
jfrazee@wiley.law

Practice Areas

Buy American and Trade Agreements Acts
Cybersecurity
Government Contracts
National Security
Privacy, Cyber & Data Governance
Telecom, Media & Technology

Continued emphasis on "Made in America" laws (Section 809, 842). Enhancing the domestic supply chain is also apparent in the NDAA's focus on domestic preference laws. The Act requires DOD to submit a report to Congress on violations of domestic preference laws, including the identity of the contractor and the action taken by DOD in response to the violation—a clear incentive for DOD to refer the matter to suspension and debarment officials. The Act also adds additional products—beef products; molybdenum and molybdenum alloys; optical transmission equipment, including optical fiber and cable equipment; armor on tactical ground vehicles; graphite processing; and advanced AC-DC power converters—to the list of high priority goods to be analyzed by DOD for procurement from U.S. or allied suppliers.

Streamlining procurement for innovative technologies (Sections 803, 806, 807, 834). The NDAA introduces a few provisions that will change how the government conducts business, although the ultimate impact may not be felt immediately. Multiple provisions in the NDAA are aimed at promoting acquisition of innovative products, as well as making it easier for DOD to procure the items it needs. One provision allows a more streamlined evaluation of proposals for commercial products or services that are "new" as of the date of the proposal, with a ceiling of $100 million. Pilot programs will also be established to develop acquisition practice for emerging technologies and to accelerate procurement and fielding of innovative technologies. DOD will also have to conduct reviews and provide annual reports on the highest and lowest performing acquisition programs, and conduct an assessment of the impediments and incentives for improving acquisition of commercial products and services. And the Act repeals the preference for fixed-price contracts introduced in the FY2017 NDAA.

Increased focus on small businesses (Sections 861-867). The NDAA authorizes more funding for the use of Small Business Innovation Research programs. The Act also requires additional analysis and reports on the effect of DOD's proposed Cybersecurity Maturity Model Certification (CMMC) on small businesses. Final determinations of HUBZone status are also transferred from the Small Business Administration to the Office of Hearing and Appeals, bringing additional transparency to the process. But there are also additional obligations placed on small businesses, which now must affirmatively notify the contracting officer if there is a change in their size status following a size protest that affects their eligibility for a solicitation with a pending bid and update their registration in the System for Award Management (SAM.gov) within two days of an adverse size determination.

Revisions to other transaction authority (Sections 821-836). The NDAA introduces several modifications to DOD's authority to enter into Other Transaction Agreements (OTAs). DOD can now award prizes for advanced technology achievements in excess of the prior $10 million ceiling, provided that the Under Secretary of Defense for Research and Engineering approves and notification is provided to Congress. The Act also instructs DOD to ensure that the Defense Innovation Unit, the Strategic Capabilities Office, and the Defense Advanced Research Projects Agency all enter into at least two OTAs for specified projects by September 2023. DOD is also required to review and make recommendations as to whether the use of OTAs should be modified or expanded for certain types of acquisitions, as well as collect and publicize data concerning the Department's use of OTAs.

Bringing structure to termination decisions (Section 811). The Government's right to terminate contracts for its convenience is one of the defining characteristics of government contracts, but exercising that right obligates the Government to pay the reasonable costs associated with the termination. Occasionally, contracts are terminated without an appreciation of the associated costs. The NDAA requires DOD during the annual budgeting process to perform a more structured review of certain multiyear contracts likely to be terminated, identifying the expected costs associated with the termination as well as what the Government expects to save.

Cybersecurity emphasized but mandatory reporting left out (Sections 866, 1501-1552). Cybersecurity remains a priority for Congress, as evidenced by the NDAA's significant investment in cybersecurity, including an assessment of the Cyber Maturity Model Certification program and its impacts on small businesses. The NDAA also requires Cyber Command to establish a voluntary process to engage with industry to develop defensive cyber capabilities, which the NDAA highlights as a continued area of activity in federal procurement. Most notably, the NDAA establishes a pilot program for a public-private partnership to detect and disrupt malicious cyber operations. The final version of the NDAA did not include some cybersecurity provisions that were included in the House version of the NDAA. For example, as we discussed in our recent newsletter article, the House version of the NDAA included a provision to establish a Cyber Incident Review Office within the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA). Under the House bill, CISA would have set a mandatory reporting requirement of security breaches for companies across 16 sectors deemed to be "critical infrastructure." Although that provision was not included in the final version of the Act, we expect Congress to continue consideration of a mandatory reporting requirement for cybersecurity breaches.

Additional National Security Matters (Sections 855, 1243, 1251, 1509). The NDAA imposes a variety of additional measures directed at national security concerns relating to China and other U.S. adversaries. For example, the statute requires contractors doing business in China to disclose whether they employ one or more individuals who will perform work on non-commercial contracts in excess of $5 million. Section 1243 revises a requirement from the FY2000 NDAA that requires DOD to provide a comprehensive annual report to Congress on military and security developments within China, including among other things, cyberwarfare capabilities directed at DOD infrastructure and space and counter-space programs and capabilities. Another provision requires the Undersecretary of Defense for Research and Engineering to work with the Director of the Office of Net Assessment to prepare a comparative assessment of the efforts of the US. and Chinese governments to develop and deploy critical modernization technology with respect to military applications in the areas of (i) directed energy systems; (ii) hypersonics; (iii) emerging biotechnologies; (iv) quantum science; and (v) cyberspace capabilities. The Act also requires the Commander of United States Cyber Command and the DOD Under Secretaries of Defense for Policy and Intelligence and Security to jointly sponsor or conduct an assessment of the current and emerging offensive and defensive cyber posture of adversaries of the United States (e.g., Russia, China, North Korea, and Iran) as well as plans for Armed Forces offensive cyber operations during potential crises or conflict.

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