STINSON

News & Insights

National Defense Authorization Act for Fiscal Year 2021 Passes Out of Committee for Consideration by Full Senate

Alert
07.07.2020

By Susan Warshaw Ebner

House Version Still in Committee

Preparing the defense budget is not an easy thing. Typically, the goal is to have the bills passed by the House and Senate, and then to go into conference to resolve differences and develop a single bill that can pass through both houses of Congress before the end of the current fiscal year and the start of the new one.

It appears, at least for now, that efforts to accomplish this budgetary requirement are in process. Both the House and Senate are working on their versions of the National Defense Authorization Act for Fiscal Year 2021 (NDAA). The House version is in committee markup. The Senate version has been rolled out of committee and is being considered by the full Senate.

Below are some key points regarding the government contracting aspects of the current Senate bill:

- Assessments of Programs and Capabilities

The proposed NDAA would require the Department of Defense (DoD) to conduct a number of assessments of DoD programs. These include Sec. 111, Integrated Air and Missile Defense Assessment, requiring a targeted assessment and analysis to counter identified current and emerging threats to "cruise, hypersonic, and ballistic missiles," unmanned aerial systems, rockets, and indirect fire. In addition, Sec. 802 seeks an assessment of the National Security Innovation base.

Perhaps in response to the current COVID-19 environment, Sec. 231 provides for "an assessment and direct comparison of capabilities in emerging biotechnologies for national security purposes, including material, manufacturing, and health, between the capabilities of the United States and the capabilities of adversaries of the United States" and recommendations to improve and accelerate the U.S. capabilities. Other assessments covered by the bill relate to military personnel, management, end strength, and military justice and related matters.

The bill also seeks analysis of DoD infrastructure, facilities and assets that could be affected by "permafrost thaw" (Sec. 351) and extreme weather (Sec. 354).

- Research and Development

The bill contains numerous research and development programs. In connection with applying artificial intelligence (AI) to the National Defense Strategy, Sec. 213 asks DoD to identify five test cases for prototyping the use of AI enabled systems to improve management of enterprise acquisition, personnel, audit, financial management or other management functions. Sec. 214 and following seek to enhance innovation by: extending DoD laboratories' pilot program authority; establishing programs and agreements on quantum computing; establishing R&D programs for DoD science and technology reinvention laboratories and institutions of higher education; establishing water sustainment technology; and expediting the maturation and fielding of hypersonic technologies.

- Supply Chain Risk Assessment and Management

Supply chain risk lies at the heart of a number of initiatives proposed in the Senate version of the NDAA FY '21. Sec. 801 includes policy recommendations for implementing the Executive Order 13806, Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency. Sec. 803 also seeks to improve the national technology and industrial base by identifying specific technologies, companies, laboratories, and factories, and factories of or located in the U.S. or non-U.S. members. Notably the section provides for the National Technology and Industrial Base Regulatory Council to address issues with supply chain security and integrity throughout the development, marketing, sale and use processes:

> "(A) address and review issues related to industrial security, supply chain security, cybersecurity, regulating foreign direct investment and foreign ownership, control and influence mitigation, market research, technology assessment, and research cooperation within public and private research and development organizations and universities, technology and export control measures, acquisition processes and oversight, and management best practices; and (B) establish a mechanism for national technology and industrial base members to raise disputes that arise within the national technology and industrial base at a government-to-government level."

Sec. 804 also addresses supply chain risk assessment and management. It would modify the framework for modernizing acquisition processes to ensure the integrity of the defense industrial base (DIB) by managing supply chain risk. The proposed provision would seek an assessment of DIB policies, programs, procedures, limitations and acquisition guidance to manage supply chain risks. Programs and policies identified in this section for assessment include Small Business Innovative Research (SBIR), Title III Defense Production Act (DPA), the Trusted Capital Marketplace Program, the Berry Amendment and others.

Sec. 805 calls for the development of a methodology for actual and continuing assessment of industrial base capabilities and capacity of the U.S. versus foreign adversaries technological and industrial bases – (1) determining the competitive advantages sought by foreign adversaries with regard to regulation, raw materials, educational capacity, labor and capital accessibility; as well as (2) evaluating the competitive strengths and weaknesses of U.S. industry versus foreign adversaries.

Sec. 806 would have DoD review and analyze the materials, processes and technology sectors of the DIB to address sourcing and industrial capacity, examining (1) restrictive procurement processes, such as buying from the U.S. "national technology and industrial base," which as defined in 10 U.S.C. § 2500(1) includes "the persons and organizations that are engaged in research, development, production, integration, services, or information technology activities conducted within the United States, the United Kingdom of Great Britain and Northern Ireland, Australia and Canada;" (2) buying from suppliers in other allied nations, (3) buying from other suppliers; (4) actions to increase investment to expand capacity, diversify supply sources, develop alternative approaches through R&D or procurement; versus (5) taking no actions, implementing no restrictions, or refraining from additional investment.

Not surprisingly, the foregoing analysis would be prioritized by looking at (a) goods and services covered under existing restrictions where Domestic Nonavailability Determinations (DNADs) have been issued finding that there was a lack of the particular good in sufficient quantities and of the quality required from a U.S. source; (b) critical technologies identified in the National Defense Strategy; (c) DIB technologies and sectors; (d) microelectronics, printed circuit boards and other electronics components; (e) pharmaceuticals, medical devices, and Personal Protective Equipment (PPE); (f) rare earth materials, (g) synthetic graphite, and (h) coal-based rayon carbon fibers.

On the manufacturing side of supply chain risk, Sec. 807 Microelectronics Manufacturing Strategy would bring back to the U.S. the foundry and other industrial capabilities needed for the domestic manufacture of state-of-the-art integrated circuits.

Printed Circuit Boards (PCBs), which are used for a multitude of purposes from telecommunications to data communications and storage, medical applications, networking, 5G cellular communications, computing, radar, munitions, and other systems and processes, have been the target of counterfeit and malware activities in recent years. PCBs are traditionally considered commercial items and in some cases may be Commercial Off-The-Shelf (COTS) items that are exempt from certain "buy American" requirements currently. Section 808 would address the security of PCBs by imposing a different kind of "buy American" restriction – one that would require that the supplier include an increasing percentage of the value of PCBs from the U.S. or other "covered nations." The proposed section would initially mandate a 25% U.S. or other covered nation requirement by October 2023. The percentage would rise each year until the ultimate requirement of 100% of manufacture and assembly of PCBs value was in "covered nations" at the end of ten years. Under the bill, any exception to the percentage requirement would require notification to congressional defense committees. A contractor or subcontractor that could not complete the required certification might be permitted to remediate compliance for an appropriate period, but such remediation would require reporting to the congressional defense committees and require that the particular contractor or subcontractor audit its supply chain "to identify any areas of security vulnerability and compliance with Section 224 of the NDAA FY '20, which requires defense microelectronics products and services to meet trusted supply chain and operational security standards. Under the proposed Sec. 808, China, Russia, North Korea and Iran, and possibly others in future, would be expressly excluded from "covered nation" status and therefore would not be eligible for an exception or waiver.

Similarly, Sec. 809 seeks to eliminate, by 2030, U.S. dependence on "unsecure sources of supply" for the processing or manufacturing of any strategic mineral or metal deemed essential to national security, through incentives and stockpile programs.

Given the focus on ensuring security and integrity of the supply chain through mandated covered nation content, it is unclear why Sec. 814 would increase the Berry Amendment's small purchase threshold to except permitted purchases at or below $150,000 from the requirements of that Amendment.

- Procurement Policy

Sec. 831 and following seek to address Procurement Policy and Management. In particular, Sec. 831 would require a report on acquisition risk assessment and mitigation as part of the DoD implementation of its adaptive acquisition framework. Under the framework, DoD seeks to address technical, integration, interoperability, operations and sustainment, workforce, as well as cyber and supply chain risks, in its acquisition programs. Sec. 831 also would require an assessment of DoD software acquisition and pilot programs from the Comptroller General by March 2021.

National Defense Authorization Act for Fiscal Year 2021 Passes Out of Committee for Consideration by Full Senate

Sec. 841 Innovative Commercial Products and Services Acquisition would establish new authority to acquire "innovative commercial products and services" using "general solicitation competitive procedures" to allow DoD to enter into fixed price contracts or agreements. Under this section, innovative products or services would be deemed to include a new technology, process, or method, or any new application of an existing technology, process or method.

In contrast to opening up acquisition for innovative products and services, Sec. 845 Revised Definition of Business System Deficiencies for Contractor Business Systems would appear to raise the bar for determining a contractor has acceptable business systems for contract operation and payment. Specifically, under the business systems rules, contractors must have suitable business systems to perform government contracts. Contractors that are audited and determined to have significant deficiencies in one or more elements of their business systems may face withholdings or even an inability to obtain advance payments for work under their contracts. Contractors found significantly deficient may also face adverse consideration in future option exercises or contract awards. The proposed bill would amend the requirements for approval of government contractor business systems to provide that the contractor's business system cannot have "material weaknesses." The section would define a "material weakness" as "a deficiency, or combination of deficiencies, in internal control over risks related to Government contract compliance or other shortcomings in the system, such that there is a reasonable possibility that a material noncompliance will not be prevented, or detected and corrected, on a timely basis. A reasonable possibility exists when the likelihood of an event occurring is either reasonably possible, meaning the chance of the future event occurring is more than remote but less than likely, or is probable."

Sec. 861 Implementation of Modular Open Systems Architecture Requirements would provide the government the right to at least a government purpose rights license to software-defined interfaces for systems, major systems, or major components, as well as cyber-physical weapon systems, developed in whole or in part with government funding. The section directs the government also to negotiate with a contractor or subcontractor to obtain a government purpose rights license for a system or component software interface developed solely at private expense. The section provides that such government rights would not impair the contractor's patent or copy rights, nor its rights to fees or royalties for software or processes developed exclusively at private expense. This clause would also establish an interface repository to permit the military services, defense agencies, field activities, combatant commands, and contractors access to such interfaces "to facilitate system, major system, and major component segregation and reintegration." Separately, but within this same section, the bill would task DARPA with demonstrating technologies developed under its System of Systems Integration Technology and Experimentation program, including STITCHES technology. The DoD Chief Information Officer (CIO) then would be tasked with assessing the technology demonstrated.

In addition to research and development, future acquisitions are the subject of increased supply chain scrutiny and management. Under Sec. 882 Balancing Security and Innovation in Software Development and Acquisition, the bill calls for the development of requirements for future solicitations of both commercial and developmental solutions to ensure software security, including management of the supply chain and third party software sources and component risks. This security effort will include reviews of code for security and procedures for operation of the software acquisition pathway.

Intellectual property theft and mergers and acquisitions are also targeted by the bill. Under Sec. 891 Safeguarding Defense-sensitive U.S. Intellectual Property, Technology, and Other Data and Information, the Senate bill would require DoD to undertake efforts to protect defense-sensitive intellectual property, data and information from acquisition by China. Potentially, this could cover the handling and sale of intellectual property and information generated in whole or in part with government funding or in performance of government contracts and subcontracts.

- 5G and 6G Telecommunications, Irregular Warfare and Foreign Threats

Those who analyzed the Trump National Security Strategy and Cyber Strategy published shortly after President Trump took office will view those documents as foreshadowing things to come. These strategy documents identified foreign economic and political threats, and the risks of asymmetric warfare. Since then we have seen risks identified with regard to Chinese equipment and components in telecommunications infrastructure and other systems and threats from Kaspersky secure software and services, among others. The Senate's proposed bill addresses these types of threats directly.

In Sec. 1046 Consideration of Security Risks in Certain Telecommunications Architecture for Future Overseas Basing Decisions, Congress would require that DoD take into account the security risks of 5G and 6G telecommunications network architecture, including telecommunications equipment provided by "at-risk vendors" such as Huawei, ZTE, etc. when deciding where to base personnel and what can be used at those venues.

Sec. 212 would establish a "public-private partnership between Defense and industry" regarding wireless 5G networking, presumably to ensure the safety and security of those networks.

Similarly, Sec. 1082 Personal Protective Equipment (PPE) Matters addresses the fielding of new generations of PPE to members of the armed forces, including barriers and challenges to obtaining such equipment and issues and injuries arising from "ill-fitting or malfunctioning PPE."

To better prepare against irregular threats, Sec. 1209 Functional Center for Security Studies in Irregular Warfare would establish a center for the study of cybersecurity, nonstate actors, information operations, counterterrorism, stability operations and the hybridization of such matters.

Similarly, Sec. 1285 Modification of Initiative to Support Protection of National Security Academic Researchers form Undue Influence and Other Security Threats would ensure that officials at institutions of higher education are briefed on espionage risks, as forewarned is forearmed.

Sec. 1286 recognizes that the U.S. and its allies face similar threats and may be able to leverage their developments. Sec. 1286 would establish a U.S.-Israel Operations Technology Working Group for cooperative technology programs to develop and field capabilities in missile defense, countertunneling, and counterunmanned aerial systems to deter and defect respective adversaries.

Sec. 1601 and following cover other strategic programs, cyber, and intelligence matters. These sections would address the potential risks of a war in space -- including resilient and survivable positioning, navigation, and timing capabilities, as well as the space launch program.

Cybersecurity also is deemed a critical concern. Sec. 1611 and following would address DoD cyber matters by establishing a Principal Cyber Advisor and a cross-functional team of subject matter experts and developing a framework for cyber hunt forward operations, including pre-deployment planning and metrics to evaluate discovered malware and infrastructure concerns. Sec. 1615 would aid in DoD's assessment and identification of redundancies and gaps in its cyber operations, sensor deployment, data collection and analysis. Sec. 1617 and Sec. 1625 would address cyber operational planning and deconfliction policies and processes for operation of the Cyber Command and other DoD activities, as well as the cybersecurity duties of the National Guard.

Notably, Sec. 1623 includes a plan for the deployment of commercial off-the-shelf (COTS) solutions to monitor DIB (contractor and supply chain) public-facing Internet attack surfaces. Sec. 1624 also would extend the Cyberspace Solarium Commission which issued a report in June 2020 on a new strategic approach to cybersecurity and layered cyber deterrence by (1) shaping U.S. and its allies' and partners' behavior in cyberspace, (2) denying benefits to adversaries that have exploited cyberspace to their advantage and to U.S. disadvantage, and (3) ensuring the U.S. will be able to maintain capability, capacity, and credibility to retaliate on actors that would target the U.S. in and through cyberspace. This extension would allow the Commission to track and analyze feedback regarding its report.

Sec. 1629 and Sec. 1630 address cyber vulnerabilities in DoD command and control systems through a Strategic Cybersecurity Program and evaluation of major weapon system vulnerabilities.

The DoD Cybersecurity Maturity Model Certification (CMMC) program also is mentioned in the Senate bill. In particular, Sec. 1631 addresses the DIB participation in a cybersecurity threat intelligence sharing program to be established and would base information sharing on the level of the contractor's CMMC certification. The section indicates interest in not only DoD sharing of information, but obtaining contractor consent to the sharing of information in contractor systems through "queries of foreign

intelligence collection databases related to the contractor," providing that sources and methods of such data collection are protected. Sec. 1632 also provides for DoD to assess the threat hunting elements of each of the CMMC levels and the need for continuous threat hunting operations on DIB networks by DoD, the prime contractor, and third-party cybersecurity vendors.

Sec. 1635 would expand the authority under which DoD may access and obtain information relating to cyber attacks on operationally critical contractors, including forensic analyses to determine whether and, if so, what data was exfiltrated or compromised. DoD would be provided mechanisms to assist the contractor (when requested) in detecting and mitigating penetrations.

Under Sec. 1642, the NDAA bill proposes to provide financial assistance to small manufacturers to obtain cybersecurity services for compliance with cybersecurity requirements and CMMC certification.

Sec. 3131 of the bill addresses required reporting of penetrations of contractor or subcontractor networks covered by the Atomic Energy Act, as well as access to such networks to conduct forensic analysis. The requirements of this section would apply to the subcontractor as well as the prime contractor. Of significance, "subcontractor" here is broadly defined as "a private entity that has entered into a contract or contractual action with a contractor or another subcontractor to furnish supplies, equipment, materials or services of any kind in connection with another contract in support of any program of the administration."

Under Sec. 3151 and following, the Senate bill would enhance procurement authority to manage supply chain risk. The proposed legislation would establish a "special exclusion action" that would prohibit the award of contracts or subcontracts by DoD or the Department of Energy components to a source the Secretary has determined represents a supply chain risk. This section would go beyond the current Supply Chain Risk rule, DFARS 252.239-7018, and provide a specific period of time during which no contract or subcontract can be awarded to a person or entity identified by the Secretary as a supply chain risk. The bill also continues the limitation and exclusions relating to acquisition of uranium from Russia.

- Other Matters

The Senate version of the bill contains a number of other provisions, these include increasing shipbuilding projects designed to promote and protect the security of that portion of the industrial base, e.g., Sec. 1025 Sense of Congress on Actions Necessary to Achieve a 355-Ship Navy; Sec. 124, Procurement Authorities for Certain Amphibious Shipbuilding Programs; Sec. 811, Stabilization of Shipbuilding Industrial Base Workforce; Sec. 864 Disclosures for Certain Shipbuilding Major Defense Acquisition Program Offers (including whether an offeror's planned contract performance includes "any foreign government subsidized performance, financing, financial guarantees, or tax concessions"); as well as Sec. 172, which would provide authority to use the F-35 aircraft accepted by the Government of Turkey but never delivered; actions to align and implement the new Space Force; and military personnel and base matters.

National Defense Authorization Act for Fiscal Year 2021 Passes Out of Committee for Consideration by Full Senate

The Senate version also includes provisions on a host of issues, including Sec. 377, which deals with renaming of DoD items that "honor or commemorate the Confederate States of American [the Confederacy] or any person who served voluntarily with the [Confederacy]."

- Next Steps

The aforementioned and other matters may impact the debate and timing of the NDAA's passage. While the full Senate continues its consideration of the current bill; the House is working on its own version. That version is still in committee as of the time of this alert.

We are following these matters and will report on future developments. In the interim, please contact Susan Warshaw Ebner or the Stinson LLP contact with whom you regularly work if you have questions about Federal contracting matters.

RELATED CAPABILITIES

Business Litigation

Energy

Environmental & Natural Resources

Government Contracts & Investigations