crowell moring

CLIENT ALERT

National Defense Authorization Act for Fiscal Year 2021: Need-to-Know Provisions for Government Contractors

Jan.12.2021

On December 11, 2020, Congress presented to President Trump H.R. 6395, National Defense Authorization Act for Fiscal Year 2021. On December 23, 2020, President Trump vetoed the bill. Subsequently, the House voted on December 28, 2020 and the Senate voted on January 1, 2021 to override the veto.

This Act contains numerous provisions that will impose new requirements, expectations, or opportunities for government contractors. Crowell & Moring's Government Contracts Group discusses the most consequential changes in the FY2021 NDAA for government contractors below.

Cybersecurity

The FY2021 NDAA is notably replete with cybersecurity measures, particularly those intended to shore up the cybersecurity posture of the Defense Industrial Base (DIB). The cybersecurity measures include:

Section 1260F establishes an assessment of the effectiveness of the current National Cyber Strategy, which is aimed at deterring industrial espionage and cyber theft of intellectual property and personal information by the People's Republic of China.

Section 1712 establishes requirements for each major weapon system to be assessed for cyber vulnerabilities and to identify priority critical infrastructures by broad weapon system mission areas. This section also creates a Strategic Cybersecurity Program to improve systems, critical infrastructure, kill chains, and processes related to nuclear deterrence and strike, certain long-range conventional strike missions, offensive cyber operations, and homeland missile defense.

Section 1714 renews the Cyberspace Solarium Commission, which has become influential in developing cybersecurity approaches to defend the United States against cyberattacks.

Section 1716 authorizes the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) with the power to issue administrative subpoenas to internet service providers when it detects critical infrastructure security vulnerabilities but cannot detect the owner.

Section 1735 enables the Department of Defense (DoD) to integrate capabilities and systems for user activity monitoring, as well as for endpoint cybersecurity and the collection of metadata on network activity. The purpose is to enable mutual support and information sharing. The section also encourages the DoD to consider using Big Data Platform instances that host cybersecurity metadata for storage and analysis of all activity monitoring data collected across the DoD.

Section 1736 enables the DoD to complete an assessment of the feasibility and resourcing required to establish a DIB Cybersecurity Sensor Architecture Program responsible for deploying commercial-off-the-shelf solutions to monitor the public-

facing internet attack surface of the DIB. The DoD will devise a governance structure that will allow for collection of cybersecurity data on the public-facing internet attack surfaces of DIB contractors in a manner that is compatible with the Department's (1) existing or future capabilities for analysis, and (2) instrumentation and collection, as appropriate, of cybersecurity data within the Department's Information Network. This section also encourages the Principal Cyber Advisor to consult with and "solicit recommendations" from industry stakeholders across the DIB regarding implementation of the sensors and potential costs to the DIB.

Section 1737 requires the DoD to complete an assessment of the feasibility and resourcing required to establish a DIB threat information sharing program. As part of the program, this section tasks DoD to:

- Set specific, consistent timeframes for all categories of cybersecurity incident reporting; and
- Establish a single clearinghouse for all mandatory cybersecurity incident reporting to the Department, including incidents involving Controlled Unclassified Information (CUI) and classified information.

Section 1739 requires the DoD to complete an assessment of the feasibility and resourcing required to establish a DIB Cybersecurity Threat Hunting Program to actively identify cybersecurity vulnerabilities within the DIB. This section specifies that the assessment will evaluate, among others:

- The threat hunting elements required for contractors under the Cybersecurity Maturity Model Certification (CMMC), including practices pertaining to continuous monitoring, discovery, and investigation of anomalous activity indicative of a cybersecurity incident.
- The suitability of a continuous cybersecurity threat hunting program, as a supplement to the CMMC requirements, that will consider: (i) Collection and analysis of metadata on network activity to detect possible intrusions; (ii) Rapid investigation and remediation of possible intrusions; (iii) Requirements for mitigating any vulnerabilities identified pursuant to the cybersecurity threat hunting program; and (iv) Mechanisms for the DoD to share within the DIB malicious code, indicators of compromise (IOCs), and insights on the evolving threat landscape.
- Participation of prime contractors and subcontractors in the cybersecurity threat hunting program. The DoD is considering procurement prohibitions for a contractor that is noncompliant with the future threat hunter program.

The extent to which a contractor may be required to participate in the threat hunting program may depend upon the nature and volume of CUI handled under a DoD contract.

Section 1742 requires the DoD to assess each Department component against the CMMC framework and submit a congressional defense report regarding findings. Components will be assessed against CMMC Level 3 or higher.

Section 3131 encourages the Administrator for Nuclear Security to establish procedures requiring contractors and subcontractors to report within 60 days of discovery to the Chief Information Officer when a covered network of a Department of Energy contractor or subcontractor is successfully penetrated.

Government Contracts Intellectual Property

Section 804 requires the DoD to issue regulations and guidance to facilitate DoD's access to and use of modular system interfaces. The regulations and guidance, in relevant part, must include requirements that:

- The program officer for each weapon system characterize the desired modularity of the weapon system for which the program officer is responsible; and
- Each contract following the implementation of the regulations and guidance includes requirements for the delivery of interfaces for modular systems deemed relevant in the acquisition strategy or documentation.

The regulations and guidance apply to any program office responsible for the prototyping, acquisition, or sustainment of a new or existing weapon system and may be extended to software-based non-weapon systems, including business systems and cybersecurity systems, one year after the regulations are implemented but not after two years from implementation.

Section 804 also amends 10 U.S.C. § 2446a to expand the requirement to use a modular open systems approach to the maximum extent practicable to programs beyond major defense acquisition programs. Section 804 also amends 10 U.S.C. § 2320 to grant government purpose rights to modular system interfaces developed exclusively at private expense or in part with federal funds. Section 804 further requires DoD to establish a central repository for interfaces and relevant documentation and to provide access to such repository to government and non-government entities, consistent with the rights schemes established by 10 U.S.C. § 2320.

Section 839 requires the Government Accountability Office (GAO) to submit a report to Congress by October 1, 2021 evaluating DoD's implementation of Instruction 5010.44 Intellectual Property Acquisition and Licensing, including, in relevant part:

- The extent to which the DoD is fulfilling the core principles established in the Instruction;
- The effect the implementation of the Instruction has had on particular acquisitions; and
- DoD's progress in establishing a cadre of intellectual property experts as required by 10 U.S.C. § 2322.

Other Transactions (OTs)

Section 833 requires the DoD to publish a list of OT authority consortia used to disseminate OT contracting opportunities. This listing will make it easier for companies to identify relevant consortia and, in turn, potential projects.

Section 1752 delegates the newly established National Cyber Director authority to enter into contracts and OTs as necessary to conduct the Office of the National Cyber Director's responsibilities. This section, along with Section 5301 below, reflects Congress' continuing efforts to expand the use of OTs.

Section 2866(c)(1) requires the Secretary of the Army to establish a pilot program for the development and use of an online real estate inventory tool to identify existing space available at Army installations. The provision expressly requires the Army to consider innovative approaches, including the use of OTs and commercial off-the-shelf technologies, for this program.

Section 5301 authorizes the National Institute of Standards and Technology (NIST) to use OTs, among other vehicles, to support measurement research and development of best practices and standards for artificial intelligence (AI), produce data sets for AI research, development, and use; and develop voluntary consensus standards and guidelines for trustworthy AI systems.

Section 9903 directs the DoD to establish a public-private partnership to incentivize the creation of one or more consortia with the purpose of ensuring the development and production of secure microelectronics (including integrated circuits, logic devices, memory, and packaging and testing for the same). This provision authorizes the DoD to use OTs as well as other vehicles to encourage the domestic development of microelectronics manufacturing and research and development facilities. Section 9903 places certain conditions on the types of businesses that may participate, such as requiring that participants possess management processes to identify and mitigate supply chain security risks. The Secretary of Defense and the Director of National Intelligence shall select the participants for each consortium and may consider national security concerns when doing so (*e.g.*, history of government contracting; supply chain vulnerabilities; foreign ownership, control, or influence).

National Security

Given the current political focus on securing U.S. critical supply chains, cybersecurity, and potential vulnerabilities related to foreign ownership, control or influence (FOCI), there are numerous clauses related to national security risk assessments and mitigation measures, or reporting and sourcing preferences or restrictions.

Section 819 amends Section 847 of the FY2020 NDAA, which requires covered contractors and subcontractors (companies with a non-commercial item contract or subcontract with a value in excess of $5,000,000) to make disclosures about beneficial ownership and control and for DoD to perform a FOCI risk assessment as part of the responsibility determination. New Section 819 amends the prior section by requiring that DoD periodically assess contractor compliance with the FOCI disclosure requirements, create procedures for addressing relevant changes in ownership, and implement Section 847 through revised policies and training by July 1, 2021.

Section 835 requires the DoD to develop requirements for software security criteria to be included in solicitations for commercial and developmental software solutions and the evaluation of bids, and to develop procedures for security review of code, in coordination with cybersecurity efforts.

Section 837 requires the DoD to identify policies and procedures for protecting defense-sensitive U.S. intellectual property, technology, and other data and information (including hardware and software) from acquisition by the government of China and, to the extent existing policies and procedures are insufficient, develop additional policies and procedures. The section also requires DoD to consider mechanisms to restrict current or former employees of contractors or subcontractors (at any tier) that contribute significantly and materially to any critical national security technology from working directly for companies under ownership, control, or influence of the government of China.

Section 841 amends 10 U.S.C. § 2533c (prohibition on acquisition of sensitive materials from non-allied foreign nations) to add a restriction, effective January 1, 2023, from DoD acquiring covered printed circuit boards (any partially manufactured or complete bare printed circuit board or fully or partially assembled printed circuit board that performs a mission critical function in any product or service that is not a commercial product or commercial service) from a covered nation (North Korea, China, Russia, Iran). In addition, DoD must assess the benefits and risks of extending the prohibition to include printed circuit boards in commercial products or services or in COTS products or services.

Section 848 requires DoD, to the maximum extent practicable, to acquire strategic and critical materials required to meet defense, industrial, and essential civilian needs of the United States in order of preference: (1) from sources located within the US; (2) from sources located within the national technology and industrial base (NTIB, defined in 10 U.S.C. § 2500); or (3) from other sources as appropriate.

Section 885 amends 41 U.S.C. § 2313(d) to require disclosure of beneficial ownership in a database maintained by GSA with information on contractors and grant recipients with a federal agency contract or grant in excess of $500,000. This section closely relates to Section 6403 which updates the Anti-Money Laundering reporting requirements to include the reporting of beneficial ownership information for certain companies as part of any bid or proposal for a contract above the simplified acquisition threshold.

Section 9202 creates a "Public Wireless Supply Chain Innovation Fund" to provide grants on a competitive basis to support promoting and deploying 5G and successor communications networks and integration and security of multi-vendor networks, among other things. The section also creates the "Multilateral Telecommunications Security Fund" to support the development and adoption of secure telecommunications technologies.

Section 9905 establishes the "Multilateral Semiconductors Security Fund" to be created in coordination with foreign partners to support the development and adoption of measurably secure semiconductors and measurably secure semiconductor supply chains.

TINA & Business Systems

Section 806 replaces the term "significant deficiency" and its definition in Section 893 of the FY 2011 NDAA. Previously, the term was defined as "a shortcoming in the system that materially affects the ability of officials of the Department of Defense and the contractor to rely on information produced by the system that is needed for management purposes." The Section 809 panel, in its January 2019 report, raised concern that the term "significant deficiency" and its definition was inconsistent with the two-tiered characterization of internal control deficiencies used in generally accepted auditing standards, which created confusion about the seriousness of deficiencies identified in contractor business systems. As such, the panel recommended that the term "significant deficiency" be replaced with a private-sector definition of "material weakness." The FY2021 NDAA acknowledges and follows the panel's recommendation, changing "significant deficienc(ies)" to "material weakness(es)," and substantively adopting the private sector definition of "material weakness" as proposed by the panel—"a deficiency or a combination of deficiencies in the internal control over information in contractor business systems, such that there is a reasonable possibility [probable or more than remote but less than likely] that a material misstatement of such information will not be prevented, or detected and corrected, on a timely basis."

Section 814 amends 10 U.S.C. § 2306a by establishing a standard $2 million threshold for application of the requirements for certified cost or pricing data under Truth in Negotiations/Truthful Cost or Pricing Data statutes. Specifically, the amendment removes various specific and conjunctive requirements involving date limitations and different dollar thresholds that resulted from the threshold increase in 2018, and instead establishes a consistent $2 million trigger for the requirement for certified cost or pricing data for all prime contracts entered into on or after July 1, 2018, and for all subcontracts entered into and modifications made (to prime or subcontract) on or after July 1, 2018, regardless of the date of the prime contract award. In addition, consistent with the conference report's emphasis on the importance of rigorous oversight by acquisition executives to

mitigate risks of paying higher prices that are neither fair nor reasonable, Section 814 also requires the Secretary of Defense to submit a report analyzing the impact, including any benefits to the Federal Government, of the aforementioned amendment, by July 1, 2022.

Commercial Products & Services

Section 816 modifies the statutory procedures for commercial-product and commercial-service determinations by contracting officers at the DoD. These changes are designed to foster greater consistency for determinations of commerciality across the Department. The House bill had included more robust changes, which would have increased the burden upon contracting officers seeking to deviate from prior determinations of commerciality, and would have extended a presumption of commerciality to components of commercial products. In the end, however, Congress chose to make more modest changes. Section 816 amends 10 U.S.C. § 2380 to clarify that, when making a determination, the contracting officer may both (1) request support from the Defense Contract Management Agency, Defense Contract Audit Agency, and other experts in the Department; and (2) consider the views of public- and private-sector entities. Section 816 further establishes that a contracting officer must document the determination in a written memorandum, including a detailed justification, within 30 days of contract award.

Non-Disclosure Agreements

Section 883 prohibits the DoD from awarding a contract unless the contractor represents that (i) it does not require its employees to sign internal confidentiality agreements or statements that would prohibit or otherwise restrict such employees from lawfully reporting waste, fraud, or abuse related to the performance of a DoD contract, and (ii) it will inform its employees of the limitations on such confidentiality agreements. Currently, FAR 52.203-19, Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements prohibits inclusion of similar restrictions in internal confidentiality agreements and requires contractors to notify employees of the impact that the clause has on any pre-existing agreements to the extent that such prohibitions and restrictions are inconsistent with the prohibitions of this clause but there is no requirement for a broadscale notification about such prohibition or affirmative representation on the part of DoD contractors.

Small Business Matters

Section 815 amends the prompt payment provision of 10 U.S.C. § 2307 to require accelerated payments within 15 days after receipt of a proper invoice for the amount due, thereby removing the ability of the parties to agree in the contract to a later payment date.

Section 862 transfers and consolidates the certification of Service Disabled Veteran Owned Small Businesses (SDVOSBs) and Veteran Owned Small Businesses (VOSBs) from the Department of Veterans Affairs (VA) to the Small Business Administration (SBA). Section 862 also phases out self-certification of SDVOSBs for the purposes of federal-wide SDVOSB contracting and replaces it with a requirement for affirmative certification by the SBA. The VA will continue to verify an individual's status as a veteran or service-disabled veteran. Section 862 requires that the SBA's SDVOSB and VOSB certification program begin within 2 years after enactment of the Act. When the new consolidated program is in place, VOSBs and SDVOSBs will have one year to file a certification application with SBA.

Section 863 lengthens the lookback for employee-based size standards from 12 to 24 months. This follows the Small Business Runway Act's lengthening of the lookback period for receipts-based size standards from three to five years. In order to avoid the confusion that followed the enactment of the Small Business Runway Act of 2018 as to when concerns can begin certifying against the lengthened lookback period, the Act specifies that this section will take effect one-year after the date of enactment.

Section 864 amends various portions of the Small Business Act to increase the maximum award price for sole source manufacturing contracts to small disadvantaged businesses, WOSBs, and HUBZones from $5 million and $6.5 million to $7 million.

Section 866 amends the Small Business Act to provide assistance with accessing federal government contract opportunities to small business concerns with principal offices in the U.S. territories of the U.S. Virgin Islands, American Samoa, Guam, and the Northern Mariana Islands. For four years following enactment, SBA will provide two incentives to mentors who work with small business concerns in such territories, including positive past performance consideration for mentors that award subcontracts to protégés in these covered territories and the ability to count the costs incurred for providing training to these protégés towards the mentor's small business subcontracting plans.

Section 868 requires contracting officers to consider two types of past performance submitted by small business concerns: past performance as a first-tier subcontractor and work performed as part of a joint venture. Section 868 amends 15 U.S.C. § 644 to allow a small business concern, if it has no relevant past performance of its own, to rely on the performance of a joint venture in which it took part. The small business is required to describe its duties and responsibilities as part of the joint venture within its proposal. Section 868 also amends 15 U.S.C. § 637 to require prime contractors to provide small business concerns with a record of the entity's past performance as a subcontractor so that the small businesses may use that record in future proposals. Contracting officers will be required to consider this experience. SBA must issue rules implementing these changes within 120 days.

In light of the economic hardship suffered by many small business contractors during the COVID-19 pandemic, Section 869 provides that active participants in the SBA's 8(a) business development program as of September 9, 2020 (even if they had suspended their status at that time) may elect to extend their participation for an additional year. SBA has 15 days after enactment to issue regulations implementing this change on an emergency basis.

Bid Protests

Section 886 repeals Section 827 of the FY2018 NDAA, which called for the DoD to roll out a pilot program to determine the effectiveness of requiring contractors with revenues in excess of $250 million to reimburse the DoD for costs incurred in defending against protests filed between October 1, 2019 and September 30, 2022 that were denied by the GAO.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Charles Baek
Counsel – Washington, D.C.
Phone: +1 202.624.2894
Email: cbaek@crowell.com

Jonathan M. Baker
Partner – Washington, D.C.
Phone: +1 202.624.2641
Email: jbaker@crowell.com

Adelicia R. Cliffe
Partner – Washington, D.C.
Phone: +1 202.624.2816
Email: acliffe@crowell.com

Stephanie L. Crawford
Associate – Washington, D.C.
Phone: +1 202.624.2811
Email: scrawford@crowell.com

Peter Eyre
Partner – Washington, D.C.
Phone: +1 202.624.2807
Email: peyre@crowell.com

Christopher D. Garcia
Associate – Washington, D.C.
Phone: +1 202.688.3450
Email: cgarcia@crowell.com

Kate M. Growley, CIPP/G, CIPP/US
Partner – Washington, D.C.
Phone: +1 202.624.2698
Email: kgrowley@crowell.com

Michael G. Gruden, CIPP/G
Associate – Washington, D.C.
Phone: +1 202.624.2545
Email: mgruden@crowell.com

J. Chris Haile
Partner – Washington, D.C.
Phone: +1 202.624.2898
Email: chaile@crowell.com

Olivia Lynch
Partner – Washington, D.C.
Phone: +1 202.624.2654
Email: olynch@crowell.com

Nicole Owren-Wiest
Partner – Washington, D.C.

Phone: +1 202.624.2863
Email: nowrenwiest@crowell.com

Michael E. Samuels
Counsel – Washington, D.C.
Phone: +1 202.624.2711
Email: msamuels@crowell.com