



Key Provisions You Should Know From FY 2021 NDAA

By: Townsend Bourne, Daniel Alvarado, and Nikole Snyder

On January 1, 2021, Congress overrode President Trump's veto of the Fiscal Year ("FY") 2021 National Defense Authorization Act ("NDAA") (the "Act"). The \$740 billion defense bill establishes funding levels for United States Department of Defense ("DOD") activities for the fiscal year. While the bill includes nearly 1500 pages, here we provide summaries of select provisions of the Act in three categories: (1) generally noteworthy for government contractors, (2) supply chain security, and (3) semiconductor incentives.

Generally Noteworthy for Government Contractors

Section 806. Definition of material weakness for contractor business systems.

This provision amends Section 893 of the FY2011 NDAA which required the Secretary of Defense to develop and initiate a program for the improvement of contractor business systems. Previously, Section 893 focused on the identification of "significant deficiencies." Section 806 replaces "significant deficiency" and "significant deficiencies" from Section 893 with "material weakness" and "material weaknesses." The Act provides a definition of "material weakness", which means –

deficiency or combination of deficiencies in the internal control over information in contractor business systems, such that there is a reasonable possibility that a material misstatement of such information will not be prevented, or detected and corrected, on a timely basis. For purposes of this paragraph, a reasonable possibility exists when the likelihood of an event occurring—

"(A) is probable; or

"(B) is more than remote but less than likely."

Previously, the definition of "significant deficiency" focused on "a shortcoming" in a contractor's business system that "materially affects" DOD officials and the contractor's ability to rely on the information produced by the system. The revised language provides a much clearer definition of requirements and provides two definitions of "reasonable possibility" for use by DOD officials and contractors in evaluating whether

a “material weakness” exists in the contractor’s business system. Additionally, the shift likely provides contractors with additional flexibility due to the higher standard established by the revised language – (1) increased from shortcoming to deficiency/combination of deficiencies and (2) the addition of the reasonable possibility requirement.

Section 833. Listing of other transaction authority consortia.

It’s no secret that the use of other transaction authority has significantly increased over the past five years, as shown by the recent Center for Strategic & International Studies report which found that the DOD’s use of Other Transaction Authority increased 75 percent in FY2019 and 712 percent since FY2015 (\$0.7 billion to \$7.4 billion).¹ The DOD has authority to enter into other transaction agreements (“OTAs”) through 10 U.S.C. 2371b to carry out certain prototype, research and production projects. Under Section 845 of the FY2016 NDAA, DOD was given permanent other transaction authority to award OTAs under 10 U.S.C. 2371 for (1) research, (2) prototype, and (3) production purposes.

A main point of discussion regarding other transaction authority and the award of OTAs is the lack of transparency. This is largely due to the inapplicability of FAR and DFARS provisions to these types of agreements. While OTAs primarily are meant to be used to entice non-traditional contractors who would not otherwise enter into a government contract due to the maze of regulations and compliance obligations, the majority of OTAs recently awarded by the DOD have been to “consortia.” These consortia are made up of both large traditional defense contractors and large technology companies.

Section 833 of the FY2021 NDAA requires the Secretary of Defense to create and maintain a list of consortia awarded OTAs on a government-wide point of entry within 90 days. Additionally, this government-wide point of entry will be used to announce or otherwise make available OTA opportunities. This requirement will provide significant transparency regarding these OTAs given the large amount of funds provided under these agreements and increase the ability of non-traditional contractors to find and compete for these opportunities.

Section 837. Safeguarding defense-sensitive United States intellectual property, technology, and other data and information.

This section of the Act requires the Secretary of Defense to coordinate with relevant DOD departments and agencies regarding policies and procedures for safeguarding of defense-sensitive United States intellectual property, technology, and other data and information, such as hardware and software, from acquisition by the government of China. The goal is to identify these policies and procedures and determine the extent to which they are sufficient to protect such information. If the Secretary of Defense determines these policies and procedures are insufficient, new policies and procedures must be developed to ensure this information is protected.

There are two matters for consideration provided under this section which require action by the Secretary of Defense. First, the Secretary of Defense must establish and maintain a list of critical national security technology that may require certain restrictions on current or former employees, contractors, or subcontractors of the DOD that have contributed to such defense-sensitive technology. Second, the Secretary of Defense

¹ Rhys McCormick, Department of Defense Other Transaction Authority Trends: A New R&D Funding Paradigm?, Center for Strategic & International Studies, <https://www.csis.org/analysis/department-defense-other-transaction-authority-trends-new-rd-funding-paradigm>.

must review the policies and procedures currently in place subjecting DOD employees to post-employment restrictions related to foreign governments or entities subject to foreign ownership, control, or influence. Further, additional policies and procedures should be identified should the Secretary of Defense determine additional measures to be necessary to enhance these authorities.

Lastly, in addition to the general policies and procedures related to post-employment with foreign entities for all DOD employees, the Secretary of Defense is tasked with examining the restrictions placed on current or former employees of DOD contractors and subcontractors who have contributed “significantly or materially to” defense-sensitive intellectual property, technology, or other data and information. The Secretary of Defense is charged with examining mechanisms restricting direct employment with companies wholly owned by the government of China or entities determined by the United States to be under the ownership, control, or influence of the government of China for these DOD contractor or subcontractor individuals.

Overall, this examination of post-employment restrictions by the Secretary of Defense will affect both government employees and contractors and subcontractors at all tiers.

Section 839. Comptroller General Report on Intellectual Property Acquisition and Licensing.

The Act requires the Comptroller General to provide a report regarding the implementation of Department of Defense Instruction 5010.44. This instruction applies to the acquisition and licensing of intellectual property acquired for the DOD and enables coordination across DOD components to develop and implement strategies for intellectual property acquisition and licensing through communication with industry. The goal of this instruction is to have a consistent strategy across DOD components and ensure program managers are aware of the DOD’s and contractor’s rights and obligations in intellectual property.

The Act provides several elements that must be included in the report, beginning with the extent to which (1) the DOD has fulfilled the core principles of DOD Instruction 5010.44, and (2) the Defense Acquisition University has carried out the requirements of the instruction. Additionally, the report must evaluate the DOD’s progress in establishing a group of intellectual property experts and the extent to which they are executing their roles and responsibilities to provide, among other things, functional input and assist with the coordination of critical planning and life-cycle management.

Further, the Comptroller General should evaluate the DOD’s performance in assessing and demonstrating the effectiveness of the experts in their roles and responsibilities, their provision of resources relating to intellectual property acquisition and licensing, and the effect the implementation of the instruction has had on particular acquisitions. Lastly, the report should review the extent to which the DOD incorporated industry feedback from large and small businesses and traditional and non-traditional defense contractors. This report must be submitted no later than October 1, 2021.

Section 869. Extension of participation in 8(a) program.

The Act extends the participation of small businesses in the Small Business Administration (“SBA”) 8(a) program from 9 years to 10 years if the small business was an 8(a) program participant on or before September 9, 2020. Small businesses may elect to exercise this additional year of participation regardless of whether the small business previously elected to suspend participation in the program pursuant to guidance from the SBA Administrator.

Participation in the SBA 8(a) program is extremely beneficial to small businesses due to agencies designating solicitations as small business set-asides and the award of sole-source contracts to 8(a) program participants. The additional year of participation in the 8(a) program has likely been provided due to the struggles businesses have had as a result of the COVID-19 pandemic and will provide some additional relief to participating small businesses so they may continue benefitting from this program. The SBA Administrator must issue regulations implementing this section within 15 days of enactment under emergency rulemaking authority.

Section 883. Prohibition on Awarding of Contracts to Contractors that Require Nondisclosure Agreements Relating to Waste, Fraud, or Abuse

The Act amends the Defense Contractor Whistleblower Protection Act to prohibit DOD from entering into contracts with contractors who silence whistleblowers through the use of nondisclosure agreements (“NDAs”) relating to waste, fraud, or abuse. The prohibition requires contractors to make two representations. First, a contractor must represent that it does not require its employees to enter into NDAs that prohibit lawful whistleblowing relating to waste, fraud, or abuse during the performance of a DOD contract. Second, a contractor must represent that it informs its employees of the limitations regarding these types of NDAs. DOD contracting officers may rely on these representations as long as they have no reason to question their accuracy. This prohibition and the representations are similar to those in FAR 52.203-19, Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements, and FAR 52.203-18, Prohibition on Contracting with Entities that Require Certain Internal Confidentiality Agreements or Statements – Representation, and will ensure defense contractors do not prohibit disclosure of important information regarding waste, fraud, or abuse especially given that the DOD spends billions of dollars each year on defense contracts. We expect this to be incorporated in an update to the FAR/DFARS in the near future.

Supply Chain Security

Section 801. Report on Acquisition Risk Assessment and Mitigation as Part of Adaptive Acquisition Framework Implementation.

This provision requires each service acquisition executive to submit a report to the Secretary of Defense, the Under Secretary of Defense for Acquisition and Sustainment, the Under Secretary of Defense for Research and Engineering, and the Chief Information Officer of the Department of Defense, detailing how each service acquisition executive is assessing, mitigating, and reporting acquisition program risks. This includes technical risks, integration and interoperability risks, operations and sustainment risks, workforce and training risks, and supply chain risks (including, among other things, cybersecurity and foreign control and ownership of key elements of supply chains).

Section 848. Supply of Strategic and Critical Materials for the Department of Defense.

This provision sets out an order of preference for the acquisition of strategic and critical materials required to meet the defense, industrial, and essential civilian needs of the United States. The order of preference is from (1) sources located within the United States, (2) sources within the national technology and industrial base, and (3) other sources as appropriate. This is intended to facilitate the goals of eliminating dependence on vulnerable or unreliable supply sources, developing robust processing and manufacturing in the United States, and ultimately ensuring minimal disruption to DOD’s access to critical materials in its supply chain.

Section 850. Implementation of Recommendations for Assessing and Strengthening the Manufacturing Defense Industrial Base and Supply Chain Resiliency.

This provision requires the Under Secretary of Defense for Acquisition and Sustainment to develop recommendations for further strengthening the manufacturing and defense industrial base and resilience of the United States supply chains. It requires DOD to recommend specific executive actions, programmatic changes, regulatory changes, and legislative proposals and changes, as appropriate.

The Under Secretary is required to submit the recommendations to the Secretary of Defense, who then submits the recommendations to the President, the Director of OMB, the Assistant to the President for National Security Affairs, and the Director of the National Economic Council. The Secretary of Defense also is required to brief the recommendations to the congressional defense committees.

Section 1738. Assistance For Small Manufacturers in the Defense Industrial Supply Chain on Matters Relating to Cybersecurity.

This provision allows DOD (in consultation with NIST) to award financial assistance to a “Center” (as defined by the National Institute of Standards and Technology Act) for the purpose of providing cybersecurity services to small manufacturers. These services include compliance with the DFARS cybersecurity requirements (including awareness, assessment, evaluation, preparation, and implementation of cybersecurity services); and achieving compliance with the Cybersecurity Maturity Model Certification (“CMMC”). DOD will establish and publish the criteria for such funding on grants.gov.

Section 9413. National Institute of Standards and Technology Manufacturing Extension Partnership Program Supply Chain Database.

This provision requires the Director of NIST to conduct a study to evaluate the feasibility, advisability, and costs of establishing a national supply chain database within the Manufacturing Extension Partnership program of NIST. The purpose of the database would be to understand the manufacturing capabilities of United States manufacturers, and to minimize disruptions in the supply chain.

Semiconductor Incentives

Sections 9901-9908. These eight sections are grouped together, and make up “Title XCIX – Creating Helpful Incentives to Produce Semiconductors for America.”

Section 9901 provides the relevant definitions for the subtitle. Most notably, it includes the definition of a “foreign entity of concern,” which means any foreign entity that is –

- (A) designated as a foreign terrorist organization by the Secretary of State under section 219 of the Immigration and Nationality Act (8 U.S.C. 1189);
- (B) included on the list of specially designated nationals and blocked persons maintained by the Office of Foreign Assets Control of the Department of the Treasury;
- (C) owned by, controlled by, or subject to the jurisdiction or direction of a government of a foreign country that is listed in section 2533c of title 10, United States Code; or
- (D) alleged by the Attorney General to have been involved in activities for which a conviction was obtained under—

- i. chapter 37 of title 18, United States Code (commonly known as the “Espionage Act”) (18 U.S.C. 792 et seq.);
 - ii. section 951 or 1030 of title 18, United States Code;
 - iii. chapter 90 of title 18, United States Code (commonly known as the “Economic Espionage Act of 1996”);
 - iv. the Arms Export Control Act (22 U.S.C. 2751 et seq.);
 - v. sections 224, 225, 226, 227, or 236 of the Atomic Energy Act of 1954 (42 U.S.C. 2274–2278; 2284);
 - vi. the Export Control Reform Act of 2018 (50 U.S.C. 4801 et seq.); or
 - vii. the International Economic Emergency Powers Act (50 U.S.C. 1701 et seq.);
- or
- (E) determined by the Secretary, in consultation with the Secretary of Defense and the Director of National Intelligence, to be engaged in unauthorized conduct that is detrimental to the national security or foreign policy of the United States under this Act.²

Section 9902 directs the Department of Commerce (in coordination with State, DOD, DHS, Energy, and ODNI) to develop a financial assistance program, intended to incentivize investment in facilities and equipment in the United States for semiconductor fabrication, assembly, testing, advanced packaging, or research and development. It provides eligibility criteria, and specifically prohibits Commerce from approving applications from an entity that is a “foreign entity of concern.” It also outlines proper uses of the funds, and clawback provisions for both funding and technology in certain circumstances.

Section 9903 directs DOD (in consultation with Commerce, Energy, DHS, and ODNI) to establish a public-private partnership to incentivize one or more consortia of companies to ensure the development, production, packaging, and testing of measurably secure microelectronics. Such incentives may include the grants outlined under sec. 9902. Section 9903 also outlines risk mitigation requirements and national security considerations, and allows for the use of contracts, grants, cooperative agreements, commercial agreements, other transactions authority, or other arrangements to attract nontraditional defense contractors and commercial entities.

Section 9904 requires the Department of Commerce (in consultation with DOD, DHS, and Energy) to conduct a survey to assess the capabilities of the United States industrial base to support the national defense, taking into consideration the global nature of the supply chain. The survey will request information related to the manufacture, design, or end use of microelectronics by various entities with physical operations in the United States.

Section 9905 authorizes the Secretary of Commerce to establish a trust fund (the “Multilateral Semiconductors Security Fund” or the “Fund”). It outlines investment of Fund amounts and appropriate use of the Fund, including to support the development and adoption of measurably secure semiconductors and measurably secure semiconductor supply chains. It also allows for coordination with foreign partners via a common funding mechanism.

² Under this definition, thousands of entities qualify as a “foreign entity of concern.” The definition includes entities on the State Department’s [Foreign Terrorist Organizations list](#); entities on OFAC’s [SDN list](#); any entity that is owned, controlled by, or subject to the jurisdiction of the governments of North Korea, China, Russia, or Iran; any entity that has been convicted under the seven statutes outlined in the definition; and any other entity that the Secretary of Commerce, Secretary of Defense, and Director of National Intelligence determine should be designated as a foreign entity of concern.

Section 9906 requires the President to establish a National Science and Technology Council subcommittee related to the United States' leadership and competitiveness in microelectronics technology and innovation. The subcommittee is required to develop a national strategy on microelectronics research, development, manufacturing, and supply chain security. The primary goals are to accelerate and strengthen the domestic microelectronics development, production, and workforce, and to ensure the United States is a global leader in microelectronics research and development.

This section also requires establishment of an industrial advisory committee related to the microelectronics industry; a national semiconductor technology center to conduct research and prototyping of advanced semiconductor technology; a national advanced packaging manufacturing program; a microelectronics research program at the NIST; and a manufacturing USA institute focused on semiconductor manufacturing.

Section 9907 prohibits any of the funding authorized to carry out this subtitle from being provided to a "foreign entity of concern."

Section 9908 requires the President to submit a report to Congress outlining a plan of action for any use of authorities available in Title III of the Defense Production Act to establish or enhance domestic production capabilities for microelectronics and related technologies.

Questions? Contact:



Townsend Bourne

Partner
202.747.2184
tbourne@sheppardmullin.com



Daniel Alvarado

Associate
202.747.2325
dalvarado@sheppardmullin.com



Nikole Snyder

Associate
202.747.3218
nsnyder@sheppardmullin.com

This alert is provided for information purposes only and does not constitute legal advice and is not intended to form an attorney client relationship. Please contact your Sheppard Mullin attorney contact for additional information.