COVINGTON

Who's in Your Supply Chain? Contractors Face Increasing Compliance Obligations and Restrictions

August 30, 2018

Government Contracts

How well do you actually know your supply chain—from the materials you acquire to the software you include in your products or services? If you have not answered this question recently, you should consider adding it to your "to do" list. Not only does the U. S. Government want to know, it is increasingly imposing new compliance obligations on its contractors. The Department of Defense (DoD), Department of Homeland Security (DHS), Federal Bureau of Investigation (FBI), and the Intelligence Community (IC) in particular are seeking to integrate national security considerations into the acquisition process and expect contractors to be the first line of defense.

U.S. economic and military superiority have relied on a dominant U.S. global economic position and technological advantage. The United States has increasingly relied on a global industrial supply chain and a relatively open environment for foreign investment in early stage technology development to sustain this dominant position. The U.S. Government has growing concerns that these past practices meant to extend U.S. military advantage are contributing to its erosion. As a result, DoD, other Executive agencies, and Congress are taking steps to mitigate risks across the defense industrial and innovation supply chains that provide hardware, software, and services to the U.S. Government.

DoD recently launched an initiative called "Deliver Uncompromised," which originated with Section 1696 of the Fiscal Year 2018 National Defense Authorization Act (NDAA). On June 21, 2018, three senior DoD officials responsible for acquisition, research and engineering, and intelligence testified about this initiative during a House Armed Services Committee hearing, emphasizing that security must become "a fourth pillar in defense acquisition" alongside cost, schedule, and performance. In particular, one DoD official emphasized the need to make security a business differentiator for those seeking to compete for U.S. Government contracts. Contractors need to understand these security obligations and implement compliance processes, or they may find themselves at competitive disadvantage or even precluded from competition.

The FY 2019 NDAA, signed into law in August, includes a number of provisions focused on enhancing supply chain security. Section 889 imposes restrictions on the procurement and use of certain telecommunications equipment, software, and services from manufacturers owned, controlled, or connected to the Government of the People's Republic of China (PRC). Sections 1654 and 1655 create disclosure obligations related to technology when the supplier has an obligation to allow a foreign person or government to review the underlying code.

These restrictions are the most recent examples of the many steps that the U.S. Government has taken in this area. Part I of this alert provides background on key U.S. Government initiatives to protect its supply chain; Part II explains the requirements of Section 889; Part III explains the requirements of Sections 1654 and 1655; and Part IV focuses on how Deliver Uncompromised is likely to influence DoD going forward. We conclude by examining the impacts on defense contractors.

How Did We Get Here?

The U.S. Government has been focused on supply chain issues for more than a decade. As the threats have increased, so has the Government's scrutiny of its contractors and their suppliers. Underlying these efforts is the concern that a foreign government will be able to expropriate valuable technologies, engage in espionage with regard to sensitive U.S. Government information, and/or exploit vulnerabilities in products or services. A review of some of the actions taken by the U.S. Government to evaluate and protect against harm from its supply chain over the past decade provides useful context for understanding the current restrictions in Section 889.

Country- and Product-Specific Bans

Much like the Section 889 prohibitions, U.S. Government agencies are already authorized to exclude certain contractors and products from certain countries. As far back as 2006, the NDAA included a provision prohibiting DoD from procuring goods or services on the munitions list of the International Traffic in Arms Regulation (ITAR) through a contract or subcontract from any Communist Chinese military company.

Eight years later, Section 515 of the Consolidated Appropriations Act of 2014 required certain non-DoD agencies to conduct a supply chain risk assessment before acquiring high- or moderate-impact information systems. See our analysis of Section 515 here. The relevant agencies are required to conduct the supply chain risk assessments in conjunction with the FBI to determine whether any cyber-espionage or sabotage risk associated with the acquisition of these information systems exist, with a focus on cyber threats from companies "owned, directed, or subsidized by the People's Republic of China."

Most recently, U.S. intelligence agencies raised concerns that Kaspersky Lab executives were closely tied to the Russian government, and that a Russian cybersecurity law would compel Kaspersky to help Russian intelligence agencies conduct espionage. As a result, DHS issued a Binding Operational Directive effectively barring civilian Government agencies from using the software. In the FY 2018 NDAA, Congress prohibited the entire U.S. Government from using products and services from Kaspersky or related entities. In June 2018, this prohibition was implemented as an interim rule across the U.S. Government by FAR 52.204-23.

Broader Supply Chain Assessments

In addition to the product- and country-specific prohibitions noted above, both DoD and the IC have broad authorities to exclude contractors and products from procurements for sensitive Government information systems. For example, in Section 806 of the FY 2011 NDAA (as amended by the FY 2013 NDAA), Congress authorized the heads of DoD agencies to exclude information technology contractors from procurements and permit DoD to withhold consent to subcontract if DoD determines that a contractor or subcontractor presents a supply chain risk for

national security systems (NSS). This section is not limited to particular countries, but instead is focused on protecting information systems that carry some of DoD's most sensitive information. See our prior discussion of DoD's implementation of Section 806 here.

As recently as March 2018, the Deputy Secretary of Defense issued a memorandum requiring DoD to enhance Section 806 procedures "to proactively address supply chain threats that present [national security] risk" when purchasing information and communications technology ("ICT") (whether as a product or service) that are included in NSS. From a practical standpoint, these enhanced procedures likely mean that DoD anticipates exercising its Section 806 authority more often going forward.

The IC has similar authorities and has established a procedure for the identification, assessment, and mitigation of supply chain threats through the use of comprehensive risk assessments for all mission-critical products and services. These procedures are reflected in Intelligence Directive 731, which we discussed previously here.

Future Actions

Multiple agencies and the Administration are looking for additional areas where supply chain regulation may be appropriate. Some examples are discussed below.

In April 2018, the Federal Communications Commission (FCC) issued a proposed rule seeking to bar the use of funds from its Universal Service Fund to purchase equipment or services from companies posing a national security threat to U.S. communications networks or the communications supply chain.

The Defense Security Service (DSS) is transitioning to a risk-based National Industrial Security Program informed by foreign intelligence threats—including supply chain threats—and is increasing its field and analytical counterintelligence resources focused on critical technology protection in the cleared sector. As part of its traditional security vulnerability assessment, DSS is implementing in phases a new threat assessment methodology and matrix, which evaluates foreign exploitation of the supply chain and business processes and security controls related to supply chain protection. In connection with this enhanced security vulnerability assessment, DSS will expect each cleared company to develop a tailored security plan, with recurring DSS review.

In July 2018, DHS announced the establishment of the National Risk Management Center and the Center's Information Communions Technology Supply Chain Task Force. That Task Force is asking industry to identify hardware, software, and information technology devices that may pose a risk to the U.S. supply chain.

Finally, there are reports that the Trump Administration is considering issuing new Executive Orders addressing supply chain risks that may expand some of these authorities.

Given the Deliver Uncompromised initiative and the significant risks to national security, contractors should expect these types of changes to continue.

Section 889: Prohibition of Covered Telecommunications Equipment and Services

Prohibitions

Section 889 of the FY 2019 NDAA provides that no Executive agency may procure or obtain (either by contract, grant, or loan) any telecommunications and video surveillance equipment and services provided by Huawei Technologies Company and ZTE Corporation (or any subsidiary or affiliate of such entities). This prohibition also covers telecommunications and video surveillance equipment and services provided by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities) if the equipment or service is for the purposes of public safety, U.S. Government facility security, physical security surveillance of critical infrastructure, or other national security purposes. Finally, a catch-all provision bars telecommunications and video surveillance equipment or services from any entity that the Secretary of Defense, in consultation with the Director of National Intelligence or the FBI, reasonably believes is owned, controlled by, or connected to the government of the PRC.

Under Section 889, Executive agencies also may not contract (or extend or renew a contract) with entities that use covered telecommunications equipment or services as a substantial or essential component or as critical technology as part of "any system." These prohibitions apply to procurement contracts, loans, and grant funds. Although "system" is not defined, it appears that this limitation extends to an entity's internal systems because contractors could store, process, or transmit sensitive U.S. Government information on their internal information systems.

Exceptions

There are two exceptions to Section 889's prohibitions. Under the first exception, Executive agencies may procure services "that connect[] to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements." Thus, Section 889 likely will not penalize a telecommunications provider merely for exchanging traffic and otherwise having common network arrangements with covered entities. The second exception excludes any covered telecommunications equipment that "cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles." In other words, it appears that Section 889 allows for Executive agencies to contract with entities that use covered telecommunications equipment as a substantial or essential component of a system, so long as that system cannot access or interact with the content of the data it handles.

Implementation Questions Remain

Section 889 does not define many key terms, including "an entity owned or controlled by, or otherwise connected to, the government of [the PRC]." As drafted, the statutory prohibitions are quite broad. How these terms ultimately will be defined will be at the discretion of each implementing agency. Nonetheless, some guidance can be gleaned from how similar prohibitions have been implemented by the U.S. Government in the past. For example, in the sanctions area, an entity is "owned or controlled" by the government of Iran, if it is a "corporation, partnership, association, or other entity in which the Government of Iran owns a 50 percent or greater interest or a controlling interest, and any entity which is otherwise controlled by that government."

Agencies that have promulgated regulations implementing similar supply chain prohibitions have exempted certain systems and products from those prohibitions. Key to the exclusions are whether the systems and products access or manage sensitive U.S. Government information. For example, excluded from these prohibitions are systems that do not process Government information and physical parts such as cabling, cable adaptors, power cables, network server racks, wired keyboards and mice, and items with no integrated circuitry. This suggests that these types of items may not be considered sensitive enough to require a ban and may provide some guidance as to what may be considered "substantial", "essential", or "critical technology." But until regulations are promulgated, these key issues will remain unresolved.

Effective Dates

The prohibition on Executive agencies procuring, obtaining, extending or renewing a contract for covered telecommunication equipment or services is effective one year after the enactment of the FY 2019 NDAA, which was signed on August 13, 2018. For the prohibitions on the U.S. Government entering into a contract (or extending or renewing a contract) with an entity that *uses* any equipment, system or service as a substantial or essential component or critical technology of any system, Section 889 requires compliance two years after enactment of the NDAA. The same two year effective date applies to the prohibition on Executive agencies obligating loan or grant funds to procure covered telecommunication equipment or services.

Sections 1654 and 1655: Foreign Review Disclosure Obligations

The Senate's version of the NDAA included expansive—but unclear—disclosure provisions regarding foreign access to and review of information technology code. The provisions were animated in part by concerns about Kaspersky Lab and its links to the Russian government, although the proposed remedy swept much broader. Our firm analyzed those provisions in a June 15 article, and we expected the conference committee to address some of the questions left open by the Senate language.

Modestly revised versions of these provisions became Sections 1654 and 1655 of the NDAA. The two sections work in tandem. Section 1654 requires DoD to develop "a prioritized list of countries of concern related to cybersecurity based on their governments' hostility, intelligence activity, criminal activity, and willingness and ability to disrupt the U.S. government's supply chain." Section 1655 establishes new disclosure rules and use prohibitions "to mitigate the risks derivative of foreign governments' code review of information technology products used by the Department of Defense."

With respect to the Section 1654 "countries of concern," contractors must disclose whether they have allowed a listed government to review the source code of *any* product, system, or service used by DoD. For all other countries, Section 1655 requires both the disclosure of whether a contractor has allowed a foreign government to review the code of "noncommercial" products, systems, and services developed for the DoD, and more broadly, "any obligation to allow a foreign person or government to review the source code of a product, system, or service . . . as a condition of entering into an agreement for sale or other transaction with a foreign government or with a foreign person on behalf of such a government." As written, this latter requirement applies to both noncommercial and commercial products, systems, and services. As in the Senate bill, Section 1655 also imposes new disclosure requirements on the efforts of a prospective vendor to obtain a license under the Export Administration Regulations (EAR) or the ITAR.

The NDAA provided some helpful clarifications, including that the disclosure obligations and use rules apply prospectively to DoD procurements and a five-year limitation on the lookback period for code-sharing obligations. However, key questions remain unresolved. Certain undefined terms could widen or narrow the application of these provisions. For instance, the concepts of "obligation," "review," and "foreign person" are open to varying interpretations, as we highlighted in our previous article.

Operational questions abound, as well. The NDAA does not address the nuances of the mitigation that the Secretary of Defense may impose, including the scope of mitigation (i.e., whether the company could be excluded from unrelated procurements); whether mitigation options include outright exclusion; whether the details of mitigation must be publicly reported; and what due process rights contractors have to challenge mitigation determinations.

The legislation specifically requires DoD to publish implementing regulations for the disclosure obligations, so we expect to see some additional clarity through the regulatory process. The mitigation process, on the other hand, may evolve in a much less transparent manner.

DoD's Deliver Uncompromised Initiative

Meanwhile, DoD is pursuing its focus on the security of the defense industrial supply chain under the aegis of "Deliver Uncompromised." The term originated with a former director of counterintelligence for DSS. It describes the objective of ensuring that capabilities—both hardware and software—arrive to end users with protections against vulnerabilities that an adversary can exploit. We have seen significant action in DoD, across the Administration, and in Congress to carry out these goals, and we expect that momentum to continue.

The Government Accountability Office includes DoD supply chain management on its "high risk list" published biennially, at the start of each new Congress. Although GAO has acknowledged the progress that DoD leaders have made in scoping and addressing the risks associated with supply chain vulnerability, the pace at which those risks continue to proliferate threatens to outstrip the government's ability to address them.

As these legislative and regulatory actions proceed, government contractors should plan to deploy an agile, iterative, and flexible infrastructure to respond to the twin roles of the government as *customer* and *regulator*. In other words, contractors must meet the government's business expectations and minimize the risks associated with governmental compliance obligations. In doing so, contractors and subcontractors at all stages of the supply chain must align efforts across business functions within the company—from operations and R&D to legal, human resources, and government relations—and among the multiple companies that comprise complex DoD supply chains.

This summer, the federally funded research and development center MITRE published a strategy document with policy options to implement "Deliver Uncompromised" throughout the government. It begins by grounding the need for action in the "changing character of war." The recommendations range from short-term actions to long-term goals, all designed to "make better use of [DoD's] existing resources to identify, protect, detect, respond to, and recover from network and supply chain threats."

The report aims to re-orient the approach to industrial security as one in which the U.S. Government rewards contractors for uncompromised products, and incentivizes businesses to consider supply chain security as a potential "profit center" rather than an overhead compliance obligation.

These goals are ambitious. Even many of the "short-term" recommendations, if implemented, would be highly disruptive. Consistent with the DoD congressional testimony we highlighted at the outset of this alert, the MITRE report recommends changes to DoD's acquisition policies and instructions that would make security a "primary metric," or "fourth pillar" of acquisition like cost, schedule, and performance. Over the longer term, the report includes recommendations to enhance the tax advantages of investments in cybersecurity and supply chain resilience.

Congress and DoD are likely to stay closely aligned on the objectives. We expect to see continued progress, particularly as the NDAA remains one of the relatively few pieces of legislation that reliably passes the Congress each year. Both branches of government will, of course, bring unique perspectives and refine the approach through the give-and-take of the regulatory and legislative process. DoD has already issued a notice seeking comments on the regulations that will be promulgated to implement the FY 2019 NDAA and, as in past years, DoD will send legislative proposals to the Hill during the fall as the FY 2020 NDAA begins to take shape. Those proposals will undoubtedly include recommendations related to "Deliver Uncompromised" initiatives.

These recommendations can be instructive for contractors, because they represent signals about the priorities of both legislators and end users. For instance, an FY 2019 proposal would have expanded the coverage of legislation governing forward-deployed acquisition by various Combatant Commands, the so-called "Never Contract with the Enemy" law. Congress declined to adopt DoD's full, expansive set of recommendations, but the Armed Services Committees did agree with part of DoD's request to update the sunset provisions in current law, and effectively extend the effectiveness of the provisions. Thus, even if the legislative proposals are not codified, they signal to contractors where key points of discussion and negotiation within the U.S. Government could affect business operations and compliance obligations.

Consequences for Contractors

The provisions in the FY 2019 NDAA are notable examples of the sourcing limitations that the U.S. Government is imposing on its contractors to protect its systems from malicious foreign infiltration. Although there are no specific penalties imposed by Sections 889, 1644, and 1645, a failure by contractors to monitor their supply chain, secure it from threats, and comply with the myriad prohibitions now in place could result in variety of adverse actions. These consequences range from negative past performance ratings, loss of award fees, exclusion from a competition or the National Industrial Security Program, or even suspension or debarment if the Government has significant concerns about a contractor's controls for its supply chain. To the extent that contractors execute contracts or submit disclosures without vetting their supply chain for compliance with these sourcing requirements, contractors also could face civil or criminal allegations of false statements and false claims.

Moreover, the consequences are not merely contractual. A failure to comply could result in serious national security issues, if foreign adversaries steal valuable research and development, national security systems are infiltrated, or sources and methods of information collection are

compromised. Contractors that cause or enable these effects could have their security programs heavily scrutinized and curtailed and a responsibility determination initiated.

In the final analysis, contractors and the U.S. Government share the strategic objectives of protecting the United States' competitive edge and sustaining overmatch on the battlefield. This article highlights some of the friction points in pursuing those goals. With planning, forethought, and experienced counsel, contractors can minimize disruption and continue to accomplish their business goals while providing outstanding support to the men and women of the U.S. national security enterprise.

If you have any questions concerning the material discussed in this client alert, please contact the following members of our Government Contracts practice:

Susan Cassidy	+1 202 662 5348	scassidy@cov.com
Zachary Mears	+1 202 662 5414	zmears@cov.com
Heather Finstuen	+1 202 662 5823	hfinstuen@cov.com
Ashden Fein	+1 202 662 5116	afein@cov.com
Catlin Meade	+1 202 662 5889	cmeade@cov.com
Jeffrey Bozman	+1 202 662 5829	jbozman@cov.com