White Paper

NDAA, BAA and TAA Compliance for DMP Products

2019 NDAA background

The National Defense Authorization Act 2019 (NDAA) is a U.S. federal law that funds the continued operation of the Department of Defense (DOD). The NDAA 2019 Section 889 Part A prohibits the U.S. government from procuring video and telecommunication equipment from certain Chinese companies and their subsidiaries.

Part A of Section 889 became law on Aug. 13, 2018 and went into effect one year later. (Congress.Gov)

Section 889 of the 2019 NDAA imposed restrictions on government procurement related to "covered telecommunications equipment or services." The NDAA defines "covered telecommunications equipment or services" to include telecommunications equipment or services provided by Huawei Technologies Company, ZTE Corporation, Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company and Dahua Technology Company, as well as their subsidiaries and affiliates. The NDAA also authorizes the Secretary of Defense to designate additional Chinese companies as providing covered telecommunications equipment or services.

Section 889 includes three primary procurement restrictions:

- Effective as of Aug. 13, 2019, subsection (a)(1)(A), referred to as Part A, prohibits direct government procurement of "any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system."

Section 889 primary procurement restrictions, continued:

- Effective beginning Aug 13, 2020, subsection (a)(1)(B), referred to as Part B, bars the U.S. government from contracting with any entity that "uses any equipment, system or service that uses covered telecommunication equipment or services as a substantial or essential component of any system, or as critical technology as part of any system."
- Also, effective beginning Aug. 13, 2020, subsection (B) bars recipients of government grants and loans from using federal funds to purchase goods or services that use covered telecommunications equipment or services.

Federal Acquisition Regulation Subsection (a)(1)(A) published

On Aug. 13, 2019, the U.S. government published an interim final rule that generally prohibits government agencies from acquiring goods or services that use certain covered telecommunications equipment or services.

"Federal Acquisition Regulation: Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment," Federal Register.

The broad scope of the definition of "Uses"

In February 2020, representatives from the Department of Defense, which is the government agency charged with drafting the rule implementing Part B, indicated that the working draft of the rule at that time encompassed companies that merely have a commercial relationship with Huawei or ZTE or that use goods and services of a company that relies upon Huawei or ZTE.

They offered the practical example that the rule would potentially bar procurement from a company with an office in Germany that uses a local internet service provider deploying Huawei routers.

Federal Acquisition Regulation Subsection (a)(1)(B) published

On July 14, 2020, the U.S. government published the interim final rule that generally extends the contracting prohibition to any entity that merely "uses" covered telecommunications equipment or services, even if the targeted technology is not part of the goods or services that the U.S. government is purchasing. The prohibition is limited to use that is "a substantial or essential component, of any system, or as critical technology as part of any system."

"Federal Acquisition Regulation: Prohibition on Contracting With Entities Using Certain Telecommunications and Video Surveillance Services or Equipment," Federal Register.

Other resources include:

Security Industry Association (SIA) Analysis of FAR Rule for Section 889(a)(1)(B) of the NDAA

"SIA Analysis of New Government Rules on Select Chinese Video Surveillance and Telecom Firms," SIA.

Security Industry Association (SIA) Position on Implementation for Section 889(a)(1)(B) of the NDAA

"SIA Position: Government Should Delay Implementation of NDAA Section 889 Part B," SIA.

Secretary of Defense for Acquisition and Sustainment Ellen Lord testified before the House Armed Services Committee, seeking Congress to delay Section 889(a)(1)(B)'s effective date

Secretary Lord expressed concerns with the DOD's ability to implement the restrictions by the rapidly approaching deadline and to ensure complete compliance within two years. Given the complexity of the defense supply chain, she suggested that an additional year is needed to prevent the statutory prohibition from creating any potential unintended consequences to the defense industrial base. Industry would also like to see a delay in implementation, as well as a scaling back of the prohibition's reach.

"Full Committee Hearing: 'Department of Defense COVID-19 Response to Defense Industrial Base Challenges,'" House Armed Services Committee.

Additional Analysis of the FAR Rule for Section 889(a)(1)(B)

"Interim Rule Confirms Section 889 Part B Restriction on Contractor Use of Chinese Telecom Will Go Into Effect August 2020," Government Contracts & Investigations Blog.

"What is Section 889?" National Defense Industrial Association.

"Second Supply Chain Risk Management Rule Drops Putting Agencies, Vendors on Notice," Federal News Network.

"Interim Rule Issued by DoD, GSA, and NASA," Acquisition.Gov.

"Section 889 Part B Expands Ban on Federal Contracting with Companies Using Chinese Company Equipment and Services," Lexology.

"Long Awaited, Controversial NDAA Section 889 Rule on Huawei, ZTE, and Video Companies Emerges from FAR Council," Wiley.

"U.S. Government Releases Awaited "Section 889" Rule on Prohibition on "Use" of Covered Teleco Communications Equipment by Federal Contractors," Covington & Burling, LLP.

"What You Need to Know About Section 889 Compliance as We Move Closer to the August 2020 Implementation Deadline," Porter Wright Morris & Arthur LLP.

"U.S. Government Issues Section 889 Part B Interim Rule," The National Law Review.

Manufactured in the U.S.A. with U.S. and Global Components

Made in the USA" is something you rarely see today — more and more products are made elsewhere. But DMP is honored to be a U.S. manufacturer!

DMP is a privately held, independent manufacturer of innovative intrusion, fire, access control, network and cellular communication products. Through quality engineering and in-house design, software development and tight control of every step, DMP is able to produce high-quality security products at competitive prices. That's been DMP's commitment since 1975.

Still to this day, all DMP products are designed, engineered and manufactured in Springfield, Missouri. To assure customers that DMP systems will reliably perform as expected, DMP's "quality first" philosophy is backed by functional testing of 100% of its finished products.

We have partnered with a limited number of sensor manufacturers that provide OEM products for us from around the world. Additionally, some of the components we use aren't indigenous to the U.S.; therefore, you'll see "Manufactured in U.S.A. with U.S. and Global Components" printed on the products that you receive from us. By resourcing the best components we can find from all over the world and continuing to manufacture in our country's heartland, we're able to guarantee cutting-edge technology and a short supply chain.

From the initial concept of the product, the schematic of the circuitry, the printed circuit board and software design, it's all completed inside DMP's facility. Because of our USA manufacturing and focus on USA content, we are honored to certify that our security products meet the requirements of the Buy American Act (BAA).

DMP Products are NDAA Section 889 Part A Compliant

DMP is one of the few security manufacturers that still designs, engineers and manufactures all of its control panels in the United States. Since 1975, DMP has maintained a strong commitment to the highest level of quality and attention to detail. Our encrypted intrusion products have allowed us to meet the security needs of numerous U.S. government agencies for decades.

The DMP GSA lists, both present and historical, indicate that no "covered equipment" from any of the Chinese companies have ever been offered for sale to any U.S. government agency by DMP.

While DMP manufactures products that meet the needs of U.S. government agencies, we do not offer a video solution that is designed or intended for U.S. government use.

You can rest assured that DMP is in full compliance with NDAA Section 889 Part A. While we do sell a limited number of video surveillance products into residential and small business markets, DMP takes extra measures to protect customers' data. In fact, DMP takes privacy and cybersecurity extremely seriously and is one of the only security companies that leverage a Virtual Private Network (VPN) in any of its video product offerings. Using a VPN ensures that video transmitted over the internet or a network remains private — that's because it encapsulates and encrypts the traffic before it's sent over the internet to another network, thus keeping the user data secure and private. DMP's EASYconnect-VPN™ firmware is standard protocol on all cameras that DMP OEMs from its various camera partners. To learn about other cybersecurity solutions that DMP employs, click here for a related White Paper, "Network Security is Serious Business."

DMP Products are TAA Compliant

TAA refers to the Trade Agreements Act (19 U.S.C. § 2501—2581), which is intended to foster fair and open international trade. TAA requires that products must be produced or undergo "substantial transformation" within the United States or a designated country, including countries that have reciprocal trade agreements with the United States.

If you are supplying products for GSA Schedules and other government contracts, those products must comply with TAA. Failure to comply with TAA can lead to award cancellation, multimillion-dollar fines and suspension due to increased governmental oversight, whistleblower lawsuits and TAA related bid protests.

TAA compliance requirements are built into federal procurement contracts such as GSA Schedule contracts, IDIQ contracts and most Department of Defense contracts. The General Services Administration states:

- Since the estimated dollar value of each Schedule exceeds the established TAA threshold, TAA is applicable to all Schedules. In accordance with TAA, only U.S.-made or designated country products shall be offered and sold under Schedule contracts.

That means all products offered under GSA Schedule contracts must be TAA compliant, regardless of cost.

Determining TAA compliance isn't as simple as looking at a "made in" stamp. Complex issues of "substantial transformation" during the manufacturing process can affect whether a product is compliant or not, requiring determination according to the particular facts of each case. It may not be practical or even possible for contractors to go through every product they sell to determine compliance. It is more cost effective and reliable to source products from manufacturers that clearly manufacture their products within the United States rather than pouring over convoluted supply chain agreements and complicated joint partnerships and foreign factories under complex corporate ownership scenarios.

The government has made TAA compliance enforcement a priority, and TAA audits have led to suspension or debarment for contractors found to be in violation. Some vendors have also begun to police their competitors for TAA compliance, using violations to lodge bid protests and invalidate competitors' awards. GSA Schedule contracts provide a gateway to millions of dollars in, but they also carry a significant responsibility of regulatory compliance.

You can simplify your GSA and U.S. government contracting by simply offering products that are TAA compliant. Products that DMP manufactures are TAA compliant.

The biggest part of understanding what is TAA compliant is knowing what countries to watch for — to ensure you're not doing business with a partner that's going to violate your GSA Schedule terms and conditions. The main countries to watch for are China, Russia, India and Malaysia. These countries are all on the non-compliant list and can cause a lot of problems for your business if you try to sell products or services from these countries through a GSA Schedule.

If your control panel supplier has not certified their products that you resell to the U.S. government as being TAA compliant, you should immediately request they do so.

DMP Products are NDAA Section 1655 Compliant

The 2019 NDAA includes a number of provisions focused on enhancing supply chain security. We have discussed Section 889 Part A above. 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.

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 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 with a foreign government or with a foreign person on behalf of such a government." This latter requirement applies to both noncommercial and commercial products, systems and services.

DMP has chosen not to enter the Chinese market due to the requirement that products must have the CCC mark, which is administered by the Certification and Accreditation Administration (CNCA). This is an approval agency within the Chinese government that requires the source code be provided as part of the review process. In our effort to protect the security of our many high-level financial and U.S. government users, we have chosen not to enter the Chinese market and allow the PRC to gain access to this very vital information, our products source code.

DMP products are NDAA Section 1655 compliant. For ICD-705 and other high-security U.S. government applications, make sure the intrusion products you consider are Section 1655 compliant.

DMP XR & XT Series Control Panels are NDAA Section 889 Part B Compliant

The NDAA Section 889 Part B includes "essential component of any system" and "critical technology as part of the system" from the named manufacturers. This includes systems on a chip or an embedded processor circuitry capable of executing software commands.

DMP has made inquiry and received certification from its component vendors that supply "critical technology" for our XR Series™ and XT Series™ Intrusion Control Panels (including Verizon and AT&T cellular modems).

No technology, embedded processor circuitry or anything capable of executing software commands of any kind from any of the covered Chinese companies are used, included or embedded in any of the XR Series or XT Series Intrusion Control Panels that DMP manufactures.

The Section 889 Part B interim final rule extends the contracting prohibition to any entity that merely "uses" covered telecommunications equipment or services, even if the targeted technology is not part of the goods or services that the U.S. government is purchasing. The prohibition is limited to use that is "a substantial or essential component, of any system, or as critical technology as part of any system."

DMP has made inquiry and is certifying that it does not use any technology or services from any of the covered Chinese companies in its IT infrastructure, data networks or telecommunications systems.

Conclusion

The interim rule will require entities contracting with the federal government to certify that they do not use equipment or services produced or provided by the Chinese telecommunications companies or their subsidiaries or affiliates, regardless of whether such equipment or services are used in, or in connection with, the products to be procured by the government. It contains no "nexus" requirement which would limit its application to uses "in connection with" a contract or subcontract. In other words, the prohibition is very far reaching and applies even if the use of covered equipment or services is completely unrelated to federal business.

What is even more difficult for companies to comply with is that the prohibition is not limited to end products; it covers most any product that incorporates technology provided by the Chinese entities. It could even apply to the foreign office of a U.S. entity with a government contract.

The interim rule provides a number of welcome clarifications that limit Part B's potential scope and makes the review and certification process more practical. First, the interim rule clarifies that the Part B certification only pertains to the entity contracting with the government, not its parent, affiliates or subsidiaries. Second, a contractor may certify that it does not use covered equipment or services, based on a "reasonable inquiry" designed to uncover information in the contractor's possession regarding the identity of the producer or provider of its covered telecommunications equipment or services; it does not need to conduct an internal or external audit. Third, a contractor is not required to flow its Part B obligations to its subcontractors; the obligation pertains to the prime contractor alone.

However, legal authorities and advisors do not think that Part B makes it impossible for a company to distribute or sell said "covered" products to other segments of their business. (1) As discussed, Section 889 Part A prohibits the purchase of covered technology by the U.S. government and Part B prohibits the government from contracting with a company that uses covered technology. But the rules do not cover the sale of covered technology in the commercial marketplace. So, it is our opinion that you can still have covered products on your shelves to sell commercially so long as you don't sell it to the government or use it.

Furthermore, because of the far-reaching scope implications of the "uses" products or services by any entity that "uses" products or services, many advisors agree it is nearly impossible for anyone to truly certify to NDAA Section 889 Part B in its current form. We are aware that industry is making a major push for a legislative remedy to the vagaries of implementation and a delay to the implementations deadline.

Notwithstanding, we have attempted to clarify our position and provide transparency and full confirmation that the covered technologies are NOT included in the products that DMP manufacturers.

NDAA Section 889 Compliant Products	Yes	No
• All XTL Series Control Panels & Peripherals	Yes	
• All XT Series Control Panels & Peripherals	Yes	
• All XR Series Control Panels & Peripherals	Yes	
• All DMP Keypads	Yes	
• All DMP 1100 Series Wireless	Yes	
• All DMP Central Station Receiver Products	Yes	
• All DMP Zone Expanders, Access Control Modules & Devices	Yes	
• All SecureCom Video 5000 Series Cameras	Yes	
• All SecureCom Video 4000 Series Cameras, Including V-4061DB Video Doorbell		No
• SecureCom Video NVR		No

(1) Footnote Sources:

"Integrators Prepare for Full NDAA Implementation As interim FAR Takes Effect Next Week, Many Questions Remain," Security InfoWatch.

"What You Need to Know About the New NDAA Section 889 Implementation Rules," SIA.

"The Long Reach Of Section 889 (aka the Anti-Huawei Rule)," The Coalition for Government Procurement.

"GSA Provides Additional Guidance on Section 889 Part B Implementation and "Waivers," JD Supra.

"2019 NATIONAL DEFENSE AUTHORIZATION ACT, SECTION 889 Q&A," SheppardMullin.com.

"DoD Weighs In As Federal Contractors Search for Guidance on Implementation of Section 889 Part B," Alston & Bird Government Contract Blogs.

"US GSA Explains NDAA 889 Part B Blacklisting," IPVM.

866-266-2826
DMP.com
INTRUSION • FIRE • ACCESS • NETWORKS
2500 North Partnership Boulevard
Springfield, Missouri 65803-8877