



Security Industry Association
8405 Colesville Road, Suite 500
Silver Spring, MD, 20190
301-804-4705
www.securityindustry.org

Submitted by email: osd.dfars@mail.mil

October 19, 2018

Re: Section 889 of the FY19 National Defense Authorization Act

The Security Industry Association (SIA) respectfully submits the following early input comments regarding the implementation of Section 889 of the FY19 National Defense Authorization Act (NDAA), P.L. 115-232.

SIA is a U.S. trade association representing over 900 security solutions providers, ranging from large global technology firms to locally owned and operated small businesses. Our membership includes most manufacturers of video surveillance equipment with business operations in the U.S. as well as a significant number of security systems integrators that install and maintain video surveillance systems for end users in both the government and commercial sectors. This includes nearly 300 providers of products and services related to video surveillance and more than 30 companies that provide video surveillance products to the federal government through GSA Federal Supply Schedule contracts.

Section 889 of the NDAA, entitled “Prohibition on Certain Telecommunications and Video Surveillance Services or Equipment,” restricts federal procurement of telecommunications and video surveillance equipment and services produced by certain China-based firms, beginning in August 2019.

SIA shares the government’s interest in protecting and ensuring the security of information and communications technology utilized by the federal government, which is especially critical for technology supporting national and homeland security missions. However, as other industry submissions have noted, the unusual and complex language found in the provision creates considerable ambiguity regarding specific aspects of its expected implementation, which subsequent rulemaking must resolve to allow agencies and suppliers to clearly understand the requirements, so they can ensure they are fully compliant with them.

Inapplicability to Non-Federal Sales and Use

The most critical need for clarity identified by our members is the scope of the prohibition relating to contracting in subsection (a)(1)(B). Here is the key language:

(a) PROHIBITION ON USE OR PROCUREMENT.— (1) The head of an executive agency may not—

(A) procure or obtain or extend or renew a contract to procure or obtain 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; or

(B) enter into a contract (or extend or renew a contract) with an entity that uses 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.

Given the foregoing language and the title of the bifurcated subsection, “Prohibition on Use or Procurement,” it is clear that subsection (a)(1)(A) restricts direct government procurement of covered equipment or services, while subsection (a)(1)(B) additionally restricts government use, specific to entering into contracts with entities that use covered equipment or services in a substantial way in contracts with the United States.

The tandem provisions ensure that the restriction encompasses equipment and services used by private entities in performing contracts with federal agencies, in addition to simply prohibiting direct procurement (and later, obligation or expenditure of federal loan and grant funds by federal agencies for the covered equipment and services).

Accordingly, any implementing regulation should clarify that the prohibition on contracting in subsection (a)(1)(B) applies to an entity’s use of covered equipment or services in the direct performance of federal contracts. In other words, the prohibition would not apply to non-federal sales or use of such equipment by a government contractor.

This clarification will enable straightforward compliance and limit the potential economic impact on small businesses.

For example, for products meeting the definition of covered video surveillance equipment in subsection (f)(3)(B), federal contractors could support agency compliance and objectives of the provision by:

1. Ensuring no such products are included in any offerings to the federal government or paid for with federal loan or grant funds, and
2. Ensuring no such products are used by the contractor in the performance of a contract with the federal government.

With clear guidance, contractors could reasonably certify the above after taking the appropriate steps. Specific to video surveillance products, while tangible economic impact will result, the impact will be limited because federal procurement of covered products is already limited in scale by restrictions pursuant to both the Buy American Act (BAA) and Trade Agreements Act (TAA), which limit the eligibility of Chinese products for federal purchase.

Clear guidance that Section 889 does not apply to non-federal sales or use of covered equipment is critical to U.S. security companies as they provide integrated security solutions across multiple government and commercial markets, using a mix of products from different manufacturers tailored to the technical requirements, price points and specific customer needs that vary widely for each sector—from universities to courthouses, convenience stores, hospitals, etc.

Products offered in the federal market are tailored specifically to government requirements. However, we estimate the federal government accounts for less than 5% of the U.S. video surveillance market. Thus, security companies must remain competitive in the commercial market to stay in business. While the eligibility of Chinese products for federal purchase is limited, products provided by the two China-

based video surveillance manufacturers referenced in section 889, among the 10 largest manufacturers of these products globally, are ubiquitous in commercial security use.

Without clarification that the restriction in subsection (a)(1)(B) applies only in the context of performance of federal contracts, an open-ended meaning could be inferred that prohibits the government from entering into contracts with entities that happen to use covered equipment in ways wholly unrelated to the performance of their federal contract. This far-reaching prohibition would amount to a government-wide boycott or “blacklisting” of businesses that utilize the covered equipment in a general sense, potentially encompassing the sale of such products to non-federal customers. Such an outcome would impose crippling financial burdens on many U.S. security companies that serve the commercial marketplace and other non-federal customers, and ultimately increase security costs to the U.S. business community at-large. There is little evidence Section 889 was intended broadly to disrupt commercial sector security products, business models and supply chains and we do not believe the language of the statute, read in its plain, ordinary meaning and in context, supports such an interpretation.

Importantly, under the requirements of the Regulatory Flexibility Act, the government must consider a regulatory approach to implementing Section 889 that minimizes negative economic impact to small businesses and other small entities. The blacklisting of contractors using this common security equipment, unrelated to federal procurement or funding, would have a significant negative economic impact on small businesses in the U.S. The following are just three examples of specific ways this may occur.

- Small security integrators that do some business with the federal government or work on federally-funded projects may have to choose between federal work and changing their commercial product line. Small businesses are less likely to be able to either absorb the loss in revenue or pass on to consumers the additional costs they may incur from using different products.
Example: A small U.S. security integrator who happens to use covered equipment on a security project for a local hospital system could not also enter into a GSA Federal Supply Schedules contract to provide security solutions in which it only used video surveillance products not considered covered equipment.
- Small security integrators that do not do business with the federal government or work on federally-funded projects, yet serve customers that work with the government, may have to choose between changing their commercial product line or serving only customers that do not work with the government. Again, small businesses are less likely to be able to either absorb the loss in revenue or pass additional costs on to consumers.
Example: A small U.S. security integrator is not able to make a competitive offer to provide a video surveillance system monitoring the offices and parking lot of a chemical company that is also under contract to supply chemicals to the federal government.
- Small companies, of all types, that do business with the federal government or work on federally funded projects may be limited in choice of equipment for their own security use, as a condition of doing business with the government, significantly increasing security costs. The China-based video surveillance manufacturers named in the prohibition offer some of the most commonly

utilized products in certain commercial sectors in the U.S. For example, products provided by these companies account for more than 20% of the small and medium sized business market in North America. Artificially increased security costs are more burdensome to small businesses than others, making such businesses more likely to face a difficult choice between higher cost solutions or lower levels of security for their facilities, patrons and employees.

Example: A local produce grower and distributor under contract (small business set-aside) with the Defense Logistics Agency (DLA) to provide fruits and vegetables for commissaries and dining halls on military bases in the region, cannot renew the contract unless covered video surveillance equipment part of the security system for its processing and storage facility, distribution centers and offices are replaced.

Clarifying the Scope of Covered Equipment

Additional clarity is also needed regarding what video surveillance equipment is covered by the prohibition and when it applies.

Under the definition in subsection (f)(3)(B) the prohibition covers video surveillance and telecommunications equipment *“produced by”* the Hytera Communications Corporation, Hangzhou Technology Company (Hikvision) and Dahua Technology Company (or their affiliates or subsidiaries), when use is *“for the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes,”* and the covered equipment or services are used a *“substantial or essential component”* or *“as critical technology as part of any system.”*

None of these key terms are defined in Section 889. Some may have analogues in other federal laws or regulations (such as import/export regulations in 22 C.F.R. § 120.45 (ITAR), etc.), which might be applicable to terms in the provision itself or helpful for those needed in the implementing regulations. Providing such definitions and/or additional guidance regarding these terms will allow stakeholders to clearly identify the apparent use threshold triggering the prohibition, helping to ensure successful implementation.

Related to establishing this threshold, the government should consider developing a risk-based protocol for determining whether a video surveillance product is prohibited in cases where firms covered by the prohibition are not the manufacturers of the end-item but rather suppliers to another manufacturer. U.S. security manufacturers utilize a globally integrated supply chain for electronics, contracting with suppliers for various components and subcomponents incorporated into their products. Supplier relationships can range from private label or white label products sold by a reseller to original equipment manufacturing (OEM) and original design manufacturing (ODM), as well as complex supplier relationships where brand-specific hardware, firmware and/or software is highly customized by the recipient. Manufacturers working with contract suppliers may also incorporate their own unique cybersecurity features and/or testing programs.

Since these relationships are so varied and complex, a mechanism should be provided to allow industry participants to validate their supply chain security practices and cyber-risk mitigation strategies. Such an approach would align with federal supply chain risk management legislation currently under consideration in Congress, which would establish a government-wide supply chain security strategy and standards for all agencies and industry stakeholders to measure supply chain risk.

Additionally, consistent with the exclusion provided in subsection (a)(2)(B) for “*equipment that cannot route or redirect user data traffic,*” it is important to ensure that applicability of the prohibition to equipment within a system considers the presence of various mitigating cyber-security controls utilized by the system to block routing or redirection of user traffic.

Finally, in light of the significant differences between video surveillance products and the other types of equipment and services covered by the prohibition, the definition provided subsection (f)(3)(B) specific to these products and the need for additional clarity specific to them outlined above, SIA recommends that a separate implementing regulation(s) with respect to video surveillance be considered.

Federal law specifically defines “Telecommunications Equipment” and “Telecommunications Service” in 47 U.S.C. § 153(52-53) in such a way that excludes video surveillance equipment and services. “Video surveillance” technology is in fact quite different from “telecommunications” technology. Much of the ambiguity in section 889 stems from addressing these two different categories of technology interchangeably. Therefore, at the very least, they should be addressed separately in the implementing regulation(s).

Thank you for consideration of SIA’s comments. We stand ready to assist in providing further input or any additional information from the industry that may be necessary.

Respectfully Submitted,

A handwritten signature in black ink, appearing to read "Jake Parker". The signature is fluid and cursive, with a long horizontal stroke extending to the right.

Jake Parker
Director of Government Relations
Security Industry Association
jparker@securityindustry.org