The devil is in the details. The broader implications of the U.S. Government ban on Chinese video surveillance manufacturers are being clarified in the federal rule-making process, and a public hearing in July gave the industry a chance to speak up about the impact of the law.

**Ban on equipment**

The hearing centered on Section 889 of Title VII of the National Defense Authorisation Act (NDAA) for FY 2019, specifically paragraph (a)(1)(B). The paragraph "prohibits agencies from entering into a contract (or extending or renewing 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."
“Covered equipment” refers to products and services from Huawei, ZTE Corp., Hytera, Hikvision and Dahua

“Covered equipment” refers to products and services from Huawei Technologies Co., ZTE Corp., Hytera Communications Corp., Hangzhou Hikvision Digital Technology Co. and Dahua Technology Co. Hikvision and Dahua are two of the largest manufacturers of video surveillance equipment, and Huawei manufactures HiSilicon chips widely used in video cameras.

‘Chinese ban’ provision

The public hearing was part of the rule-making process for paragraph (a)(1)(B), which the industry has informally referred to as the “blacklist” provision of the NDAA. However, the “Chinese ban” provision [Paragraph (a)(1)(a)] is not at issue, was not covered by the public hearing, and is already scheduled to go into effect a year after the law was signed by President Trump (August 13, 2018).

There were seven presentations at the public hearing. Presenters included the Security Industry Association (SIA), two Hikvision integrators, a representative of communications manufacturer Hytera, an economist and an attorney on behalf of telecommunications company Huawei, and Honeycomb Secure Systems, a federal contractor. There was no livestream or transcription of the meeting, although PowerPoint summaries of the 10-minute presentations were published.

SIA emphasizes on clarity

In its presentation, the Security Industry Association (SIA) emphasized that contractors need clarity, i.e., that paragraph (a)(1)(B) applies to an entity’s use of covered equipment or services in the performance of federal contracts, but NOT to non-federal sales or use of covered equipment by a contractor that is unrelated to federal work.
SIA also focused on the distinction (and contrasting risk profiles) between video surveillance equipment, which are endpoint devices that may or may not be on the Internet, and telecommunications equipment. In contrast, telecommunications equipment is essential to Internet infrastructure and manages all data on a network, encrypted or not.

**Fully-compliant video surveillance products**

"Security equipment suppliers and integrators doing federal work can offer fully compliant video surveillance products"

SIA’s presentation included the following "outcome" statement: "Security equipment suppliers and integrators doing federal work can offer fully compliant video surveillance products in the federal market, while offering other products tailored to technical requirements, price points and specific customer needs that vary widely for non-government commercial sectors – e.g. malls, banks, convenience stores, etc."

In other words, involvement in government contracts should not restrict an integrator’s flexibility to offer any and all products and services (included those from the listed Chinese companies) to non-government customers. The two integrators made similar points, specifically about their business with Hikvision. One presenter was Rick Williams, General Manager of Selcom, a systems integrator in Selma, Ala., with 10 employees. They have been a Hikvision partner since 2012 with a year-to-date revenue from Hikvision products of approximately $400,000.

**Hikvision integrators speak out**

A second integrator at the hearing was Mark Zuckerman of Clear Connection Inc., a security company in Beltsville, Md., with 32 local employees, that focuses on electronic security, telecommunications and IT. Clear Connection designs, installs and services systems throughout Metro DC and Baltimore, including commercial entities, schools and non-profit organizations. They do about $120,000 a year in business as a Hikvision partner and have over $500,000 in business
awaiting federal NSGP [Nonprofit Security Grant Program] approval.

In two almost identical presentations, the integrators sought clear guidance on how to comply with the language of the law as written, specifically confirmation that Section 889 of the NDAA does not apply to non-federal sales or use of covered equipment. "This is critical to my company as I 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 customer needs that vary widely for each sector," said Williams.

Hytera speaks at hearing

"It is not clear what Section 889 means, who it applies to, or how far its prohibitions extend," commented Zuckerman. "If interpreted broadly, some of my customers would be barred from entering into a federal contract because they have covered products installed in their facility to protect their property and staff."

Also presenting at the hearing was Hytera, a manufacturer of open standard digital mobile radio technology. The presentation emphasized that Hytera does not sell to U.S. telecommunications carriers, and does not supply 5G components or video surveillance equipment. Hytera equipment is used by federal customers such as the National Gallery of Art, National Archives, National Zoo and the Holocaust Museum.

Impact on clients and commerce

"These federal entities do not play a role in national security, and the Hytera systems do not connect to any critical systems," says the company. "However, the lack of clarity in the implementation of the NDAA has a significant impact on Federal, state and commercial clients, impacting competition and choice."
Hytera's presentation continues: "Hytera has never been informed by any U.S. government entity that its equipment posed a national security risk and as such has not been given the opportunity to respond to any concerns. The result of Section 889 is the creation and circulation of misinformation in the marketplace." Hytera also said that the federal proposed rules and regulations should exempt federal agencies that do not include a national security component, and equipment not interconnected with the public network.

Impact on cybersecurity

Consolidating the number of equipment suppliers hinders rather than helps cybersecurity"

James E. Gauch, an attorney with James Day speaking on behalf of Huawei, offered a global argument that could be applied to any of the banned companies: “Virtually all equipment manufacturers rely on a global supply chain and face security risks from a wide range of sources, excluding may be one or two vendors based on their national origin will not address these risks.”

He adds, “However, consolidating the number of equipment suppliers hinders rather than helps cybersecurity. Creating a small number of dominant suppliers, regardless of national origin, reduces the incentives of those suppliers to embrace industry-leading standards and creates greater exposure to vulnerabilities of a single supplier.”

Author Profile
Larry Anderson

Editor, SecurityInformed.com & SourceSecurity.com

An experienced journalist and long-time presence in the US security industry, Larry is SecurityInformed.com's eyes and ears in the fast-changing security marketplace, attending industry and corporate events, interviewing security leaders and contributing original editorial content to the site. He leads SecurityInformed's team of dedicated editorial and content professionals, guiding the "editorial roadmap" to ensure the site provides the most relevant content for security professionals.
Amid Interesting Times, Hikvision’s Outlook Remains Upbeat In The USA

Despite any negativity you may hear, Hikvision is optimistic about their role in the U.S. market. “We demonstrate that we can be trust..." 

What Are The New Buzzwords In The Security Market?

Technology advancements often come with new terms and definitions. The language of our marketplace evolves to include new words that describ..." 

The Rise Of Access Control In The Cloud

Among the cloud’s many impacts on the physical security market is a democratization of access control. Less expensive cloud systems ar..." 

Chinese Ban Looms, But ‘Blacklist’ Provision Delayed For Feedback

As political winds present new challenges for Chinese companies doing business in the U.S. market, the countdown is under way to implementat..."
How Are Standards Changing Physical Security?

The definition of a standard is “an authoritative principle or rule that usually implies a model or pattern for guidance, by comparison..."