Life after the NDAA

Security industry seeks clarity as federal ban on Hikvision, Dahua products takes effect

The ban that prohibits the purchase and installation of video surveillance equipment from Hikvision, Dahua and Hytera Communications in federal installations – passed as part of last year's National Defense Authorization Act (NDAA) – formally went into effect on Tuesday. In conjunction with the ban's implementation, the government has also published a Federal Acquisition Regulation (FAR) that outlines interim rules for how it will be applied moving forward.

Rules outlined in this FAR include:

- A "solicitation provision" that requires government contractors to declare whether a bid includes covered equipment under the act;
- Defines covered equipment to include commercial items, including commercially available off-the-shelf (COTS) items, which the rule says, "may have a significant economic impact on a substantial number of small entities;"
- Requires government procurement officers to modify indefinite delivery contracts to include the FAR clause for future orders;
- Extends the ban to contracts at or below both the Micro-Purchase Threshold ($10,000) and Simplified Acquisition Threshold ($250,000), which typically gives agencies the ability to make purchases without federal acquisition rules applying.
- Prohibits the purchase and installation of equipment from Chinese telecom giants Huawei and ZTE Corporation. This would also presumably extend to Huawei subsidiary Hisilicon, whose chips are found in many network cameras;
- And, gives executive agency heads the ability grant a one-time waiver on a case-by-case basis for up to a two-year period.

The rule is not yet finalized, however, and interested parties can submit feedback on the FAR until Oct. 15. Rules for a so-called "blacklist" provision that would prohibit government agencies from accepting bids from contractors that leverage equipment and services from the aforementioned providers are expected to be addressed separately and will go into effect a year from now barring changes to the law.

According to Jake Parker, Senior Director of Government Relations for the Security Industry Association (SIA), the most immediate impact of the interim rules released by the government for the industry will be the need for contractors to certify whether or not they are providing the covered products or services to the government. "There's standing contracts with GSA, for example, that people in the industry have and they will need to make their certifications there

and, in many cases, make certification at each order level when they receive a contact from an agency," he says.

In a statement provided to SecurityInfoWatch, a corporate spokesperson for Hikvision said the company was "disappointed" that the provision has taken effect without any review or investigation to warrant the aforementioned restrictions.

"We believe this provision is unjust and targeted Hikvision without reason or evidence of wrongdoing," the statement reads. "Meanwhile, we are evaluating every option available to contest this groundless inclusion and protect the rights and interests of the company and our partners. Since 2001, Hikvision's products have safeguarded people, communities, property and assets around the world. In doing so, Hikvision strictly complies with the laws and regulations in all countries and regions where we operate. We have made great efforts to ensure the security of our products adhere to all that is mandated by the U.S. Government, including the Federal Information Processing Standard (FIPS) 140-2 certification from the National Institute of Standards and Technology."

In a statement posted on its website, Dahua also criticized the government's decision to enact the ban.

"The prohibition was hastily enacted without any supporting evidentiary basis or due process," the statement said. "To be clear, the prohibition only relates to federal agencies. Commercial entities may continue to purchase Dahua products, as may state and local governments generally. Dahua is dedicated to legal compliance, both in the U.S. and around the globe."

Identifying the Problem

Given the vast OEM portfolios of the likes of Hikvision and Dahua, systems integrators, government contractors and procurement officers could face significant challenges in attempting to identify covered products they have already deployed or plan to install.

"We were hoping more clarity would be provided on the rule as far as what is considered covered," Parker says. "Unfortunately, the definition provided simply repeated what was in the underlying statute, which is one of the most poorly written and confusing statutes that we have reviewed. Given the fact the rule (does not contain) further definitions, agencies are clearly going to have a lot of discretion to implement this at their own guidance."

According to Michael Rogers, CEO, Securityhunter, a prime GSA Schedule Contractor, most end-users are also in the dark about the cameras hanging on their networks. "These clients really don't know…take for example Hikvision and Dahua cameras. How does an end-user actually know if it is a Hikvision or Dahua camera? It could be written on the enclosure, but

they OEM and private label so often – how is a federal agency really going to know?" Rogers asks. "Federal managers haven't used a company like Securityhunter to do a real assessment of what they really have and what is the multi-year phase plan to actually remove it. One of our clients, went to their IT department and the IT guys say, 'no you really don't have a problem.' We have to tell them that's completely bogus – they do have a problem. They can't just say,' we don't have any Hikvision' just because they don't see it."

Rip and Replace?

While some integrators have expressed concerns about the potential to have to rip and replace existing surveillance systems, Parker says there is nothing outlined in the FAR thus far that indicates that will be the case. "There's no rip-and-replace in the statute outside of if an agency is seeking a waiver," he says. "If an agency is seeking a waiver, they will need a phase-out plan to (eventually) replace existing equipment. I think the intention there is that that replacement will happen naturally though the procurement cycles and the cycle for tech refreshes."

Rogers agrees and says that the idea behind the ban is more or less to minimize the perceived risk moving forward than to cause undue hardships on budget-strapped agencies to overhaul their security systems.

"They aren't going to get punished (for having these products deployed) because it is an unfunded initiative – they just have to stop buying it today," Rogers explains. "(The NDAA ban) is really saying – 'hey there's a risk here,' and (Congress) doesn't want (the risk) to spread. It is a wake-up call – they need to identify this type of equipment, stop buying it, and then eventually it will be replaced under technology refresh contracts. The reality is, the NDAA has put us on a path where in 10 years, there will be no more (of the banned technologies) deployed by the government at all. The government loves to plan, and this is a very slow and inexpensive way to make this transition."

Rogers adds that his firm has offered to analyze the systems of some of their government clients, but that they do not seem to be in much of a rush. "We have talked to a few of these organizations and have offered to go ahead and evaluate it, but there doesn't seem to be much interest in that," he admits. "There is nobody up above really pushing for that yet, but I don't know if that will change (with the ban formally going into effect). It is really a challenge for civil servants who only have so many resources.

"We went out to try and educate some of our (government) customers about the NDAA, and how it basically says you need to know what's on your network and how these things create vulnerabilities, but the problem is it is another one of those 'unfunded initiatives' – and the federal government has a lot of them – where they say, 'hey you guys should be doing this or

looking for that but by the way, we aren't giving you any extra money,'" Rogers adds. "That's just more stress for the federal security guy who is trying to do something but doesn't have the financial resources or the manpower to execute it."

How Many Cameras Are Out There?

Despite concerns that equipment covered under the provision has an extensive footprint within the government, Rogers says that affected cameras and other products are mostly found on the edge in small and mid-size deployments.

"You will find them mostly 'on the edge' – for example, at dorms for the military, or parking garages, or at small hospitals for the VA and small office locations – because they are priced aggressively," he says. "You will see them under all these different (OEM) names because the government was maximizing value and never considered it a risk. On state and local levels, you would see a major percentage of those types of cameras, but that's not the federal government."

The Blacklist Provision

With regards to the blacklist provision, Parker says that based on the conversations that SIA has had with government officials thus far, they believe the prohibition will not be as broad as some people have speculated, and that it will more narrowly apply to the use of services and products by companies in the performance of federal contracts. SIA has also asked for more clarity on this point moving forward. "We've shared our thoughts with the government on that provision and I think that is a more significant part of the rule than this initial one and that's where we have the most concerns about it being sufficiently clear what it means," he says.

Bottom Line for Security Integrators

In the end, the NDAA could be a boon for integrators, according to Rogers, as it will enable them to upsell their government clients. "The NDAA is good for security integrators because when (your clients) are moving away from lower-priced options, that's obviously a good thing for us," he says.