VICON

FILLING THE SUPPLY GAP:

How the NDAA is Driving Innovation Among U.S. Camera Manufacturers

FEBRUARY 2022 | WHITEPAPER

Introduction

In the United States, our national defense relies upon mitigating security threats each day. IP cameras and surveillance systems are critical tools for reducing the threats in private and public spaces, including office buildings, schools, hospitals, factories, and more. Yet, sometimes using that technology can open new cybersecurity vulnerabilities.

The John McCain National Defense Authorization Act (NDAA) is legislation that Congress passes each year to make changes to the policies and organization of United States defense agencies. In addition to the Department of Defense, the legislation covers military-related programs run by other agencies, such as the Department of Energy's nuclear weapons programs and the Federal Bureau of Investigation's counterintelligence activities. Congress uses the NDAA to establish defense priorities, make organizational changes to military agencies, and provide guidance on how funding should be allocated.[1]

Congress uses the NDAA to establish defense priorities, make organizational changes to military agencies, and provide guidance on how funding should be allocated.

In 2018, Congress used the NDAA to limit some Chinese camera manufacturers from conducting business with the U.S. federal government and its agencies, due to concerns regarding the vulnerability of U.S. telecommunication systems and data security. In 2021, Congress went further, passing legislation through the FCC that ensured untrustworthy communications equipment was no longer authorized for use domestically, effectively shutting down banned Chinese companies' abilities to import and market their products in the U.S. Both pieces of legislation impacted the U.S. security marketplace. The legislation removed lower-cost security cameras (with security vulnerabilities) from distribution and changed how end-users and integrators purchase, install, and service security equipment.

This white paper provides background on the NDAA and the FCC ban and addresses resulting issues related to funding, compliance, and industry impact. It also presents options for integrators and end-users to address the marketplace void with Vicon's high-quality, feature-rich, and affordable NDAA-compliant solutions.

[1]National Defense Authorization Act (NDAA) Definition (investopedia.com)

Background of the NDAA

In 2018, it was determined that certain Chinese video surveillance companies had insecure backdoors within their products that allowed outsiders to access and control the security cameras. As a result, Congress passed NDAA Section 889: Prohibition on Certain Telecommunications and Video Surveillance Services or Equipment, which prevented the use of these cameras by U.S. federal government agencies. It also called to end the use of chipsets that are powered by Huawei HiSilicon System on a Chip (SoCs).

U.S. Congresswoman Vicky Hartzler (R-MO) played an instrumental role in drafting the NDAA that went into effect in Fiscal Year 2019. In explaining her support for the amendment, she said: "We must face the reality that the Chinese-government is using every avenue at its disposal to target the United States, including expanding the role of Chinese companies in the U.S. domestic communications and public safety sectors. Video surveillance and security equipment sold by Chinese companies exposes the U.S. government to significant vulnerabilities, and my amendment will ensure that China cannot create a video surveillance network within federal agencies."[2]

Details of the NDAA

Section 889 has three parts that detail the prohibited uses of "covered" equipment. "Covered" is defined as equipment from banned Chinese manufacturers and the Huawei HiSilicon System on a Chip (SoCs).

1. A procurement ban, Section 889(a)(1)(A), which bans federal procurement of "covered" equipment and/or service.
2. A blacklist ban, Section 889(a)(1)(B), which prohibits federal agencies from entering into (or extending or renewing) a contract with a company that uses "covered" telecommunications equipment or services.
3. A funding ban, which prohibits federal dollars from being spent on "covered" goods/services.

[2]National Defense Authorization Act Passes the House | Congresswoman Vicky Hartzler

In short, systems integrators can no longer sell, install, support, or use cameras from banned Chinese manufacturers if they wish to be eligible to participate in any projects that receive federal funding. Blacklisted manufacturers are identified as Huawei, ZTE, Hytera, Hikvision, Dahua, and their subsidiaries.[3] The moratorium also covers private-labeled cameras sold under other brand names – including American brands – but that utilize essential components from the covered manufacturers, including Huawei HiSilicon SoCs.

Common Concerns

There are many common questions and concerns regarding the details of NDAA.

Some integrators and their customers are unsure whether the legislation pertains to them. Section 889 applies to security technology manufacturers and integrators who sell, install, and service affected equipment to U.S. federal agencies or to organizations dependent on federally funded money. It directly affects every executive agency of the U.S. federal government, including agencies such as Homeland Security, the Department of Treasury, the Department of Labor, the FCC, the FBI, the State Department, the National Park Service, and countless others. It indirectly affects schools, hospitals, and other entities that may receive federal funding. They must be careful not to use any federally obtained dollars to pay for security solutions that include non-compliant devices or risk monetary fines.

There are also questions surrounding replacement parts. For example, is an integrator permitted to fix a banned camera that is still in use? Non-compliant cameras should not be fixed – they should be replaced. Furthermore, Section 889 says that contractors are required to report (within one business day) to the project's contracting officer any covered equipment or services discovered while performing contract work.

From the customers' perspective, funding to replace cameras is an area of uncertainty. Who will pay for these updates? Section 889 instructs grant awarding agencies to encourage and facilitate transition away from covered telecommunications and services. Federal agencies must "prioritize available funding and technical support to assist affected businesses, institutions and organizations...to transition from covered communications equipment and services to procure replacement equipment and services."[4] However, many organizations are awaiting more detailed instructions on how to obtain such grants before replacing cameras, as existing budgets cannot afford the expense.

Contractors are required to report (within one business day) to the project's contracting officer any covered equipment or services discovered while performing contract work.

[3]ndaa section 889 prohibitions

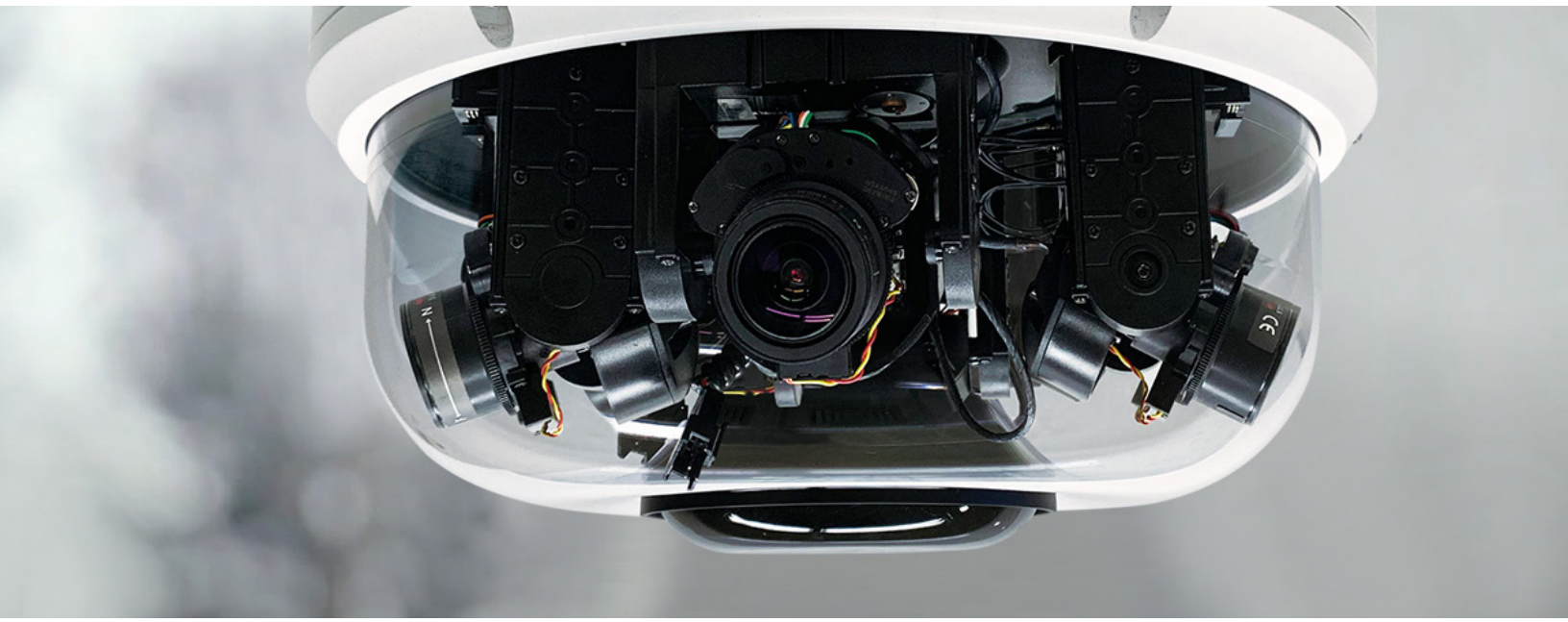
[4]https://www.jdsupra.com/legalnews/frequently-asked-contractor-questions-1773846/

Private Industry Impact - H.R. 3919

While the NDAA doesn't specifically apply to private U.S. businesses, there are real implications for the entire security industry since the October 2021 passage of H.R. 3919, the Secure Equipment Act, which requires the Federal Communications Commission (FCC) to adopt rules prohibiting "equipment authorization" for certain Chinese telecommunications and video surveillance equipment. Its companion bill in the U.S. Senate, S. 1790, was introduced by Senators Marco Rubio (R-Fla.) and Ed Markey (D-Mass.). H.R. 3919 passed unanimously in the Senate on Oct. 28 and was signed into law by President Biden on Nov. 11, 2021.

According to the Security Industry Association, "The marketing, importation, and sale of new video surveillance equipment from these Chinese manufacturers without current FCC authorization will be prohibited...When finalized, the FCC action will reduce supply and eventually eliminate future availability in the U.S. of products from these companies, which will require adjustments by all companies that may still be utilizing them, and impact product offerings, costs, and other business operations – even if they are not federal suppliers."[5]

[5]Congress Passes Bill Requiring FCC to Limit New Authorizations for Chinese Equipment, Prohibiting Revocation - Security Industry Association



Ensuring Compliance

Shortly after the passage of NDAA Section 889, the Department of Defense (DOD) issued a waiver, and a subsequent extension, setting the date by which implementation must occur. Contractors approved for a waiver currently have until September 30, 2022 for their projects to meet compliance.[6] That date is likely to hold firm, as there are now many NDAA-compliant camera options in the market available at various price points.

It is the integrator's job to present all documentation verifying that the equipment they install is compliant, and they must take compliance seriously. Failing to do so could lead to a False Claims Act violation by which the U.S. government can seek damages and up to $23,000 in penalties per violation.[7] The cost of merely defending against and resolving an allegation of a False Claims Act violation can be enormous. Integrators should be cautious; while most manufacturers are honest in posting their cameras' NDAA status, there have been incidents of misrepresentation. Federal forms are available that integrators should require manufacturers to complete, attesting to their certified status. Vicon has already responded to many such requests on behalf of its clients.

Failing to do so could lead to a False Claims Act violation by which the US government can seek damages and up to

$23,000

in penalties per violation.

[6]https://www.jdsupra.com/legalnews/dod-extends-section-889-waiver-to-73582/

[7]https://www.technologylawsource.com/2020/06/articles/section-889/what-you-need-to-know-about-section-889-compliance-as-we-move-closer-to-the-august-2020-implementation-deadline/

A surefire means to verify manufacturer compliance is by checking the GSA Advantage! website. Any manufacturer who is a GSA supplier has already been vetted and certified. Vicon's GSA schedule can be found online, under contract 47QSWA19D006F. Since passage of Section 889, Vicon has been focused on the reengineering of its product line to comply with new regulations. A full table of its certified products is listed on the company website under the "NDAA Compliance" tab.

Vicon's NDAA-Compliant Solutions

The sudden elimination of major Chinese manufacturers from the marketplace has created a vacuum for customers reliant on low-priced cameras. In the past decade, these companies transformed the video surveillance category through predatory pricing practices – gobbling up market share in a "race to the bottom." For installations requiring large quantities of devices, the pricing of these imports became the deciding factor. Lower-tier cameras made elsewhere, by manufacturers utilizing fair labor practices, experienced difficulty competing. By contrast, the high-end camera market remained dominated by highly-respected, non-Chinese manufacturers, including Vicon.

With the NDAA and FCC ban and the exit of Chinese camera manufacturers from the U.S. marketplace, end users will need to find alternatives. Will they turn to the premium lines from companies with established reputations? Perhaps, but sticker-shock is likely to make those cameras an unsuitable substitute.

Fortunately, Vicon's NDAA-compliant Roughneck line offers a range of value-priced models with features and performance typical of higher-end devices. They offer customers a cost-effective alternative to premium lines without compromising quality.

Roughneck cameras boast a range of distinctive features, including smart IR, durable IP67/IK10 construction, and smart H.265 encoding to reduce bandwidth and storage costs. For cutting-edge capabilities, the Pro series adds advanced AI-driven analytics as well as adaptive IR for clearer images in darkness, and Starlight low-light color imaging in the 2, 5 and 8MP domes and bullets.

The Roughneck Camera Series is also ONVIF certified, allowing devices to transition into any compatible video surveillance security operation seamlessly. Cameras are in stock, available now, approved through GSA, have no FCC issues, and provide the perfect solution for customers purging their facilities of blacklisted models.

Final Thoughts

The NDAA and the FCC ban have dramatically altered the security camera market. Their impact is not limited to government work. The FCC ban effectively ends the use of all Chinese camera imports within the United States. Vicon has filled the supply gap with a sophisticated portfolio of compliant solutions packed with high-quality features, unparalleled performance, and reliability, all at competitive price points.

Learn more about the Roughneck Camera Series at vicon-security.com

vicon-security.com