To Whom It May Concern:

Homeland Safety Systems feels it is our duty to educate our clients to ensure they are legally protected. Section 889 of the 2019 National Defense Authorization Act (NDAA), prohibits the federal government, government contractors, as well as grant and loan recipients from procuring or using certain “covered telecommunication equipment or services”. The NDAA prohibits the use of certain companies and brand names, such as Dahua and Hikvision, that are commonly used by security surveillance equipment installers. Telecommunications equipment from Huawei, Hytera, and ZTE also fall under this list. By using these products, you could be vulnerable to cyber-attacks or compromise the security of your institution and lose federal funding.

Before the NDAA passed the law in August of 2018, there were several cyber-security attacks, in which entire networks were shut down and sensitive information was held for ransom. By banning the equipment mentioned above, we can prevent this from happening in the future. For your convenience, we have attached brief explanations of the NDAA, Federal Acquisition Regulation (FAR) Rule, and the Secure Equipment Act of 2021.

Our company proudly holds a GSA Schedule 84 Contract (Contract # GS-07F-063BA). All GSA Schedule 84 vendors’ products are TAA (Trade Agreements Act of 1979) compliant and compliant with the NDAA; meaning all products listed on the GSA Schedule Contract must be manufactured or “substantially transformed” in the United States or a TAA “designated country”. In addition, we manufacture and install all our own products, and place our equipment on an isolated network.

At Homeland Safety Systems, we pride ourselves on being able to provide the most reliable, durable equipment and efficient service both onsite and remotely. If you have any hesitation or uncertainty regarding the compliance of your current equipment, please let us know. We are happy to perform a FREE risk assessment, to help and assist!

Thank you for your time,

Anthony P. Marquis
President/CEO
Homeland Safety Systems

HOMELAND SAFETY SYSTEMS

NDAA BANNED EQUIPMENT BRANDS

HOMELAND SAFETY SYSTEMS

CORPORATE OFFICE: 724 W. 61ST STREET, SHREVEPORT, LA 71106 • 888.909.2261 • 318.221.8062
WWW.HOMELANDSAFETYSYSTEMS.COM • INFO@HSSEMS.COM • FACEBOOK.COM/HOMELANDSAFETYSYSTEMSLA

Security Camera Compliance with the 2019 National Defense Authorization Act (NDAA)

Who is Affected by the Ban?

On August 13, 2018, the United States government passed Section 889 of the H.R.5515 - John S. McCain National Defense Authorization Act for Fiscal Year 2019 into law preventing any organization that receives federal funding, or institution that is planning a major project receiving federal grant money (ex. universities, schools, and law enforcement agencies), from purchasing or using telecommunications and surveillance camera equipment originally manufactured by certain companies in China.

On November 11, 2021, the Secure Equipment Act of 2021 was signed into law, requiring the FCC to adopt rules clarifying that it will no longer review or approve ANY authorization application for equipment that poses an unacceptable risk to national security.

What is Banned?

The NDAA specifically prohibits the following:

- Video surveillance and telecommunications equipment produced by Hangzhou Hikvision Digital Technology Company (Hikvision), Dahua Technology Company (Dahua), Hytera Communications Corporation (Hytera), or any subsidiary or affiliate of such entities.
    - Familiar Hikvision and Dahua OEM's you may recognize:

• Honeywell	• Bosch	• LTS	• Panasonic
• Alarm.com	• ADI	• IC Realtime	• ToughDog Security
• Lorex	• Interlogix	• Alibi	• Elite Security Supply

- Telecommunications equipment produced by Huawei Technologies Company (Huawei) or ZTE Corporation
- Telecommunications or video surveillance services provided by such entities or using such equipment.
- Telecommunications or video surveillance equipment or services produced or provided by an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.

What Does the Law State?

NDAA – Section 889

1.) The head of an executive agency may not procure or obtain banned equipment, which includes extending or renewing a contract to procure or obtain any banned equipment, system, or service. However, the head of an executive agency is not prohibited from procuring with an entity to provide a service that connects to the facilities of a third party, such as backhaul, roaming, or interconnection arrangements. Furthermore, telecommunications equipment that cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits, or otherwise handles is not covered.

2.) The head of an executive agency may not use loan or grant money to procure, or obtain, the banned equipment, services, and systems mentioned above. This includes extending or renewing any contract to obtain or procure banned equipment, services, or systems. In implementing the prohibition, the heads of executive agencies administering loan, grant, or subsidy programs shall prioritize available funding and technical support to assist affected organizations and institutions, as is reasonably necessary, transition from covered communications equipment or services, to procure replacement equipment and services.

3) The ban covers telecommunications equipment or services produced by Huawei technologies company or ZTE Corporation (or any subsidiary or affiliate of such entities).

4) The ban covers video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or DahuaTechnology Company (or any subsidiary or affiliate of such entities).

FAR Rule – Part A and B

A) Effective as of August 13, 2019, Part A prohibits the government from obtaining (through a contract or other instrument) certain telecommunications equipment (including video surveillance equipment) or services produced by Huawei, ZTE Corp, Hytera, Hikvision, Dahua, and their subsidiaries/affiliates.

B) Effective as of August 13, 2020, Part B prohibits the government from contracting with any entity that uses certain telecommunications equipment or services produced by the entities listed in the statute.
   - The Government cannot contract with an entity 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.
   - Prohibition applies regardless of whether or not that usage is in performance of work under a Federal contract.
   - The prohibition applies to every sector and every dollar amount. Your ability to enter into contracts with the Government will be impacted by Part B.
   - After conducting a reasonable inquiry, entities will represent whether they do or do not use prohibited telecommunications equipment or services.

Secure Equipment Act of 2021

1) This bill requires the Federal Communications Commission (FCC) to establish rules stating that it will no longer review or approve any authorization application for equipment that is on the list of covered communications equipment or services. (Listed communications equipment or services are those that the FCC determines pose an unacceptable risk to national security or the security and safety of U.S persons.)

How will the Ban be Implemented?

As of August 8, 2019, the United States government released rules that are currently in effect on how the NDAA ban will be implemented.

Why the Ban?

Hikvision is one of the world's largest electronic security manufacturers. According to the New York Times, "Their products allow clients to track people based on facial features, body characteristics, and speech monitoring on a highly intrusive level. In 2017, one company removed hundreds of Hikvision and Dahua cameras and found a secret "back door" in the devices." This "back door" enables an outside party to exploit their way into the system, as well as download personal information. Upon further investigation, it was found that company information had been trafficked off-site via the cameras to an unknown Chinese IP address. Members of Congress also believe that by banning these products it will bring manufacturing back to the United States and shield us from dangerous cyber-security attacks.

Recent Cyber Security Threats

Nvidia

California-based graphics processor manufacturer, Nvidia, has confirmed that its networks were hacked late February 2022. The company witnessed this cyberattack, where a group of hackers stole data from company servers, including sensitive information and employee credentials. 1 TB (1,000 GB) worth of information was said to have been stolen, and it was confirmed that the hackers had begun leaking the company's data online.

Brownsville, TX Public Utility Board (BPUB)

In early March 2022, one of the largest cities in South Texas (pop.200,000) became a random target for a Ransomware Attack. Brownsville, TX and Cyber Security Firm Emsisoft, are investigating the matter further. Confirmation has been provided that a Russian Ransomware gang, listed BPUB on their website, stating that sensitive information will be leaked if a ransom is not paid.

Cost of a Ransomware Attack in 2022

As of 2019, the average cost of a Ransomware Attack was $141,000. There has been an unnerving increase with each passing year, moving up to $283,000 in 2020 and a staggering $1.85 million in 2021. It will be important for everyone to maintain a laser-focus on strengthening their security measures.