



FEDERAL GOVERNMENT OPPORTUNITY TRIFECTA

COVID-19 ECONOMIC RECOVERY, SECURITY THREAT MITIGATION AND NDAA COMPLIANCE

Making funding available to replace systems and equipment from manufacturers identified in the NDAA would help 1.) mitigate national security threats consistent with the spirit of the law while, at the same time, 2.) helping with the COVID-19 economic recovery of U.S. large and small businesses through “shovel-ready” IT infrastructure projects and 3.) accelerating NDAA compliance.

PROBLEM

The economic impact to U.S. companies both large and small due to the COVID-19 virus is unprecedented. The Federal Government has an opportunity to stimulate the recovery from this crisis while at the same time help ensure agencies address threats to national security and mitigate these security vulnerabilities at Federal facilities across the world.

Today, there are a number of Federal facilities (e.g. DoD bases, VA hospitals, U.S. Mint, FBI headquarters, etc) that use Chinese-manufactured physical security equipment (i.e., video surveillance cameras). Physical Security technologies perform an important function for many U.S. Government agencies: providing situational awareness and protecting government sites from threats. Whether operating on a closed network or on a network with protected access to the internet, concerns have been raised by intelligence and security officials who warn that China could tap the technology provided by certain suppliers to spy on the United States.

Because of these security threats, Federal agencies are prohibited from procuring video surveillance equipment produced by certain Chinese companies, in addition to video surveillance services using such equipment, under the National Defense Authorization Act (NDAA) of 2019. According to a recent [Forbes](#) article “agencies are currently required to either have a plan for removing the relevant technologies or prove they’ve removed them already.” In response, the U.S. Government is taking steps at all levels of procurement intended to protect U.S. networks against cyber activities conducted through Chinese Government-supported video surveillance equipment and services.

The NDAA for Fiscal Year 2019 included Section 889 has the potential for having a significant impact on the United States Department of Defense and other United States Federal Government agencies in the procurement and deployment of telecommunications and video surveillance equipment and services.

Section 889 (a)(1) (A) provides a prohibition on the procurement of “covered telecommunications equipment or services” which is defined to include telecommunications equipment produced by Huawei Technologies Company and ZTE Corporation and video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities), as well as telecommunications or video surveillance services provided by such entities or using such equipment. This prohibition took effect August 13, 2019.

SOLUTION

Recently a bipartisan, bicameral letter was directed to the Comptroller General noting that section 889 was enacted to address threats to national security and observing that agencies may be slow to comply with section 889 due to the cost of replacing equipment and requesting annual reports on the steps taken to implement the statute including, among other things, the removal of equipment from program activities. Funding the replacement of equipment made by manufacturers identified in the NDAA would provide stimulus to the economy and aid the COVID-19 recovery with the opportunity to acquire physical security related equipment from U.S. based companies which would in turn generate business opportunities for small businesses to design, install and maintain the equipment. Many of these small businesses are in close proximity to these Federal facilities and would be able to provide timely installation and optimization services. In doing so, the Federal government would mitigate the threats to national security recognized by Congress when it passed the NDAA FY2019 and accelerate NDAA compliance.



Motorola Solutions proudly manufactures and deploys the sophisticated, cutting-edge communications, software, video security and analytics technologies that keep communities and nations safe. We have been on the frontlines with federal, state and local governments, including in times of crisis, for over 90 years. Today, our 17,000 innovators, engineers and manufacturing specialists are eager to help address critical gaps in the availability of medical and health management technology needed to fight the COVID-19 pandemic. We are pleased to offer hundreds of thousands of feet of secure, U.S.-based manufacturing, unrivaled operational agility and the capacity for rapid deployment.

MOTOROLA SOLUTIONS STANDS READY TO SERVE OUR COUNTRY IN THIS **MOMENT THAT MATTERS.**

HOW MOTOROLA SOLUTIONS CAN HELP

Motorola Solutions along with Avigilon offers US manufactured end to end video surveillance solutions, which are NDAA compliant. We have a state-of-art manufacturing facility in Plano, Texas. By manufacturing in the United States we provide a level of quality our customers can trust, while being able to accelerate the speed at which we can go from innovation to providing products for our US customers as well as around the globe.

Our technology is open allowing us to design a replacement plan for the specified banned cameras in the NDAA act referenced above. We can replace them with our quality US manufactured cameras which will meet or exceed what your current cameras capabilities. Our broad camera portfolio supports ONVIF that allows them to integrate into other vendors' head-end video management software. This allows us to be flexible when designing solutions for our customers and helping you remove the vulnerabilities that exist in your system today. Our engineering staff are experts in their field and work collaboratively with you to ensure the system we provide delivers the desired outcomes you need.

We are the only company that manufactures and develops the end to end video solution. We start at the edge with our self learning analytic cameras, network bandwidth sensitive with our patented technology HDSM (High Definition Stream Management), switches, appliances, NVRs (Network Video Recorders) and our own VMS (Video Management Software), designed and developed in Boston, MA. Our end to end solution is designed to let the technology do the work of detection and visualizing the data to your personnel so they can apply reasoning.

Our video management software ACC (Avigilon Control Center) is designed to be intuitive and user friendly with everything an end user needs is within

three clicks or less. Our flexible end user views allow you to configure the workstation whether a single monitor, multiple monitors or video wall easily and quickly. Our search capability is bar none the quickest and easiest in the industry today. The ease of use, coupled with our best in class analytics and bandwidth conservation technology HDSM, the system can significantly reduce the amount of time to locate items of interest and perform investigations. These actions can be reduced from hours to days depending down to minutes which saves time and provides a more effective response. The analytics reduce desensitization from false positives by using cutting edge techniques to narrow down and learn "real" events from noise.

Our solution when deployed end to end is a powerful ally, enabling safety and security to be more precise and persons focused on critical events reducing distraction allowing them to be far more effective. The time saved by letting our technology do the work is easily converted to wise and well chosen ROI.

Our solutions are available today.

CALL FOR ACTION

The Federal Government has an opportunity to address multiple critical needs by providing funding for replacement of telecom and video systems made by certain Chinese vendors. First, it will aid in the COVID-19 economic recovery for U.S. companies large and small. Second, it will mitigate security threats at thousands of Federal facilities across the globe. Finally, it will help agencies more rapidly comply with the 2019 NDAA.

We urge the Federal government to expeditiously provide the funding and initiate procurement actions to allow U.S. companies to deploy technology to secure our Federal facilities and mitigate the threats to national security recognized by Congress.

