CYBERSECURITY CONCERNS IMPACT U.S. GOVERNMENT AGENCIES AND U.S. MILITARY VIDEO SURVEILLANCE DEPLOYMENTS

(NATIONAL DEFENSE AUTHORIZATION ACT (PREVIOUSLY HR5515))

Pelco's Position

Cybersecurity is a top concern for many involved in the Physical Safety and Security industry, this includes Pelco, its customers, distributors, and system integrator partners. The US Government is one of the most demanding customers when it comes to the cybersecurity of its own deployments, as well as video surveillance systems used for critical infrastructure and public safety.

The US Congress took action on this subject through the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (NDAA) by banning the procurement or use of specifically named video surveillance camera and systems vendors as well as specifically named component suppliers that are used in some video surveillance products that could or are deployed in US Government-related video surveillance system deployments.

Some in the industry have expressed confusion as to the scope of the NDAA ban; the ban is related to named companies

(NDAA Section 889,3, B), not the country of origin (manufacturing location) of video surveillance products or components.

All Pelco products listed on the US government GSA contract are compliant with the NDAA and can be used in US Government-related deployments. These include all cameras and related accessories in the Sarix, Spectra, Optera, Exsite, Esprit, Evolution product lines. All Pelco VMS software and hardware is NDAA-compliant, including VideoXpert.

- For the convenience of all Pelco customers, a Pelco product compliance and non-compliance list will be regularly updated and posted on the Pelco.com website this will include products that may be introduced in the future.

Background / Details of the NDAA

On Aug 13, 2018, the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (US Government appropriations and procurement) was signed into U.S. Law. https://www.congress.gov/bill/115th-congress/housebill/5515/text

Amongst the many provisions in this law, there are several provisions which have very significant impact on new/future and existing US government agencies including the US Military video surveillance system procurement and deployment. Section 889 contains many of the relevant provisions.

https://www.congress.gov/bill/115th-congress/house-bill/5515/text#toc-4350A53097BD46409287451A50C4F397

The Act includes video surveillance equipment under the "covered telecommunications equipment" definition and calls out specific vendors, cameras, and components which are expressly forbidden for use in US Government-related video surveillance deployments.

(3) COVERED TELECOMMUNICATIONS EQUIPMENT OR SERVICES.—The term "covered telecommunications equipment or services" means any of the following:

(A) Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities).

(B) For the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes, 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).

(C) Telecommunications or video surveillance services provided by such entities or using such equipment.

(D) Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of the National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.

It should also be understood the NDAA ban extends to other manufacturers or vendors if the video surveillance cameras and systems are offered under another manufacturer's brand name typical of OEM, ODM and JDM relationships (Section 889, a1, A and B).

- Pelco does not have manufacturing relationships (OEM, ODM or JDM) with the named vendors in the NDAA.

- If at some point, Pelco does enter a relationship with a named manufacturer and offers a non-compliant camera for sale, we will post the name of the camera and its corresponding part number to the aforementioned "noncompliant" list. We will also ensure the product (camera) is not listed for sale on Pelco's GSA schedule.

SEC. 889. PROHIBITION ON CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT.

(a) PROHIBITION ON USE OR PROCUREMENT. — (1) The head of an executive agency may not—

(A) procure or obtain or extend or renew a contract to procure or obtain 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; or

(B) enter into a contract (or extend or renew 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.

The NDAA ban also includes "essential component of any system" and "critical technology as part of the system" from the named manufacturers. Pelco and others in the industry believe that the ban extends to the System on a Chip (SoC), which includes embedded processor circuitry capable of executing software commands, frequently used in various video surveillance cameras. Thus, these SoCs from specifically named vendors (previously addressed) are subject to Cybersecurity concern and are banned as well.

- The following Pelco camera product lines do not use or incorporate essential components or critical technology including SoCs produced by NDAA banned component vendors: Sarix, Spectra, Optera, Exsite, Esprit, and Evolution.

- The following Pelco VMS product lines do not use or incorporate essential components or critical technology, including SoCs produced by NDAA banned component vendors: VideoXpert, Digital Sentry and Endura.

- In addition to Pelco's GSA contract which does not include non-compliant product, Pelco has posted a NDAA-compliance list which identifies any camera (name and part number) that is not NDAA-compliant.

The NDAA (Section 889, 3c) effective date also calls for the removal of any banned but pre-existing cameras or systems that may already be deployed in US Government entities/infrastructure effective one year from the signing of the Act (this would be effective August 13, 2019). An optional waiver would extend the phase-out deadline by an additional year to provide US government agencies some time in identifying and removing banned cameras and systems. The waiver must be applied for and include a compelling reason as to why the agency will not be able to eliminate "covered telecommunications equipment" within the standard deadline. Parties seeking waiver must also submit a phase-out plan to eliminate the covered equipment from the entity's systems.

(c) EFFECTIVE DATES.—The prohibition under subsection (a)(1)(A) shall take effect one year after the date of the enactment of this Act, and the prohibitions under subsections (a)(1)(B) and (b)(1) shall take effect two years after the date of the enactment of this Act.

(d) WAIVER AUTHORITY.—

(1) EXECUTIVE AGENCIES.—The head of an executive agency may, on a one-time basis, waive the requirements under subsection (a) with respect to an entity that requests such a waiver. The waiver may be provided, for a period of not more than two years after the effective dates described in subsection (c), if the entity seeking the waiver—

(A) provides a compelling justification for the additional time to implement the requirements under such subsection, as determined by the head of the executive agency; and

(B) submits to the head of the executive agency, who shall not later than 30 days thereafter submit to the appropriate congressional committees, a full and complete laydown of the presences of covered telecommunications or video surveillance equipment or services in the entity's supply chain and a phase-out plan to eliminate such covered telecommunications or video surveillance equipment or services from the entity's systems.

(2) DIRECTOR OF NATIONAL INTELLIGENCE.—The Director of National Intelligence may provide a waiver on a date later than the effective dates described in subsection (c) if the Director determines the waiver is in the national security interests of the United States.

Closing Thoughts

Pelco products are used and trusted by numerous governments and enterprises in numerous vertical markets on a global basis. We hope this document helps clarify Pelco's position and status as it pertains to NDAA.

Cybersecurity is an important consideration for a video surveillance system, please see Pelco's Cybersecurity webpages for additional information. Please also refer to related Pelco NDAA documents and content: FAQs, videos, and a compliance list.

To make the Pelco camera selection process easier with respect to NDAA compliant products from Pelco versus banned named video surveillance camera and system suppliers, please see our equivalent product conversion list from Dahua and Hikvision to the Pelco equivalent.

Pelco would like to correct any misinformation or technical errors stemming from third-party products or representatives. If you receive information contrary to what has been stated in this document with respect to the origin of a Pelco product or NDAA compliance of Pelco products, please let us know via a feedback form available on Pelco.com or your Pelco sales representative.