Hanwha Techwin America
Frank W. Burr Blvd., Suite 43
Teaneck, New Jersey 07666
877.213.1222 | Fax: 201.373.0124
Insidesales@hanwha.com

February 28, 2022

To Whom It May Concern:

Hanwha Techwin continually provides the best in video surveillance products and technology. Per a recent request regarding NDAA compliance here is a statement from the NDAA bill to explain what products are not compliant:

Section 889 of the 2019 National Defense Authorization Act prohibits the federal government, government contractors, and grant and loan recipients from procuring or using certain "covered telecommunication equipment or services" that are produced by Huawei, ZTE, Hytera, Hikvision, and Dahua and their subsidiaries as a "substantial or essential component of any system, or as critical technology as part of any system."

We have certified that the following product requested meets the NDAA requirement.

WRR-P-E200W2-8TB – Server: https://www.hanwhasecurity.com/product/wrr-p-e200w2/

QNV-6082R- Vandal 2MP Camera: https://www.hanwhasecurity.com/product/qnv-6082r/

PNM-9022V- 8MP Panoramic Camera: https://www.hanwhasecurity.com/product/pnm-9022v/

These item can also be confirmed on our NDAA website page: https://www.hanwhasecurity.com/resources/ndaa/

If you have any questions or require additional information, please contact your local Hanwha Techwin sales person or myself.

Best Regards,

Todd Wysocki
Regional Sales Director – Southeast
Hanwha Techwin America
500 Frank W. Burr Blvd., Suite 43
Teaneck, NJ 07666
Cell: 815-353-2004
Todd.wysocki@hanwha.com
www.hanwhasecurity.com

and the President signed into law, the National Defense Authorization Act for Fiscal Year 2018 (2018 NDAA). The 2018 NDAA, among other things, bars the Department of Defense from using "[t]elecommunications equipment [or] services produced . . . [or] provided by Huawei Technologies Company or ZTE Corporation" for certain critical programs, including ballistic missile defense and nuclear command, control, and communications.[3]

4. In 2018, Congress passed, and the President signed into law, the National Defense Authorization Act for Fiscal Year 2019 (2019 NDAA).[4] Section 889(b)(1) of the 2019 NDAA prohibits the head of an executive agency from using federal funds to procure or obtain equipment, services, or systems that use "covered telecommunications equipment or services" as a substantial or essential component of any system, or as critical technology as part of any system.[5] Section 889(f)(3) of the 2019 NDAA subsequently and generally defines "covered telecommunications equipment or services" as (1) telecommunications equipment produced by Huawei or ZTE or any subsidiary or affiliate of such entities; (2) for certain safety and security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation (Hytera), Hangzhou Hikvision Digital Technology Company (Hikvision), or Dahua Technology Company (Dahua) or any subsidiary or affiliate of such entities; (3) telecommunications or video surveillance equipment services provided by such entities or using such equipment; or (4) telecommunications or video surveillance equipment or services produced by an entity that the Secretary of Defense, in consultation with the Director of 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, where "covered foreign country" is defined as the People's Republic of China.[6]

5. Like Congress, the President and the Executive Branch have undertaken numerous efforts to secure our country's communications supply chain. For example, in December 2018, the Federal Acquisition Security Council, which includes seven Executive Branch agencies, was established pursuant to the SECURE Technology Act.[7] The Council is charged with developing a government-wide strategy to address communications supply chain risks and may recommend that other agencies remove insecure communications services or equipment.[8] On September 1, 2020, the Council issued an interim final rule to "standardize processes and procedures for submission and dissemination of supply chain information" and "facilitate the operations of a Supply Chain Risk Management Task Force under the [Council]."[9] It also provided the "criteria and procedures by which the [Council] will evaluate supply chain risk."[10] In May 2019, the President signed Executive Order 13873, declaring a national emergency with respect to the security, integrity, and reliability of information and communications technology and services, and granting the Secretary of Commerce the authority to prohibit transactions of information and communications technology or services when, among other things, the transaction would pose undue risks

[3] *See* Pub. L. 115-91, 131 Stat. 1283, 1762, § 1656.

[4] *See* Pub. L. 115-232, 132 Stat. 1636.

[5] *Id.* at 1917, § 889(a)-(b)(1).

[6] *Id.* at 1918, § 889(f)(2)-(3).

[7] *See* Pub. L. 115-390, 132 Stat. 5173.

[8] *See id.*

[9] Office of Management and Budget, Federal Acquisition Supply Chain Security Act, 85 Fed. Reg. 54263 (Sept. 1, 2020).

[10] *Id.*