# PUBLIC STATEMENTS ABOUT CURRENT HIKVISION ISSUES

## HIKVISION ON HUMAN RIGHTS

### 2019 ENVIRONMENTAL, SOCIAL & GOVERNANCE (ESG) REPORT'S SECTION ON HUMAN RIGHTS GOVERNANCE

**Corporate Governance**

Over the past two years, there have been many media reports related to human rights and cybersecurity concerns related to video surveillance products. In October 2019, we were included on the U.S. Department of Commerce' s Entity List for alleged human rights violations in China's Xinjiang region. In January 2019, Hikvision retained the services of Arent Fox, led by former U.S. Ambassador Pierre-Richard Prosper, to conduct a review of the Company' s human rights compliance process. The Company has recently received a draft version of Arent Fox's final report and is reviewing it. The Company is already in the process of implementing some of the recommendations provided, such as establishing a global Advisory Committee.

**Human Rights Governance**

In our business practice, we respect human rights as stipulated in the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, the International Covenant on Economic, Social and Cultural Rights, and the ILO Declaration on Fundamental Principles and Rights at Work. At the same time, with reference to the United Nations Guiding Principles on Business and Human Rights, we endeavored to incorporate such provisions into our operational processes and policies to guide our business activities and management behaviors and to improve the compliance of our business activities with those rules and regulations. We continue reviewing and updating our policies, processes and management systems to continuously improve our human rights governance capabilities.

In our Code of Ethics and Business Conduct, it is expressed that respect for and protection of human rights is one of the basic values of our business operation. We are committed to complying with the applicable laws and regulations of the jurisdictions where we operate, as well as international norms, to better respect and protect human rights in business activities. At the same time, we have established a complaint-reporting mechanism to enable our employees and others affected by our business operation to report issues of concern, including suspected human rights violations. We will also review and improve the mechanism on a regular basis.

- The company's 2019 ESG Report was published in English on May 5, 2020.
- 2019 ESG Report PDF Link: http://static.cninfo.com.cn/finalpage/2020-05-09/1207722486.PDF

## SELECT HIKVISION HUMAN RIGHTS PRESS STATEMENTS

**PBS Frontline (March 25, 2020):**

As the security industry's global leader, Hikvision's mission is to keep people, organizations and property safe and secure. It takes its responsibility to also protect human rights seriously, and in January 2019, Hikvision retained human rights expert and former U.S. Ambassador Pierre-Richard Prosper to advise the company on human rights compliance.

**The Guardian, a major daily publication in the UK (February 13, 2020):**

Hikvision strongly opposes the decision by the U.S. Government. As the security industry's global leader, Hikvision respects human rights and takes our responsibility to protect people seriously. Hikvision has been engaging with officials in the U.S., U.K. and EU over the past 12 months to clarify misunderstandings about the company and address their concerns.

**IDC Research, a major analyst firm (March 15, 2020):**

As the security industry's global leader, Hikvision respects human rights and takes our responsibility to protect people seriously. Our mission is to keep people, organizations and property safe and secure. In 2019, Hikvision began a sustained engagement with public officials in the U.S., U.K. and EU to clarify misunderstandings about the company and address their concerns. In January 2019, Hikvision retained human rights expert and former U.S. Ambassador Pierre-Richard Prosper to advise the company on human rights compliance.

## HIKVISION STATEMENT ON ENTITY LIST DESIGNATION

Hikvision strongly opposes the decision by the U.S. Government and it will hamper efforts by global companies to improve human rights around the world. Hikvision, as the security industry's global leader, respects human rights and takes our responsibility to protect people in the U.S. and the world seriously. Hikvision has been engaging with Administration officials to clarify misunderstandings about the company and address their concerns. In January 2019, Hikvision retained human rights expert and former U.S. Ambassador Pierre-Richard Prosper to advise the company on human rights compliance. Punishing Hikvision, despite these engagements, will deter global companies from communicating with the U.S. Government, hurt Hikvision's U.S. businesses partners and negatively impact the U.S. economy.

## HIKVISION PRESS STATEMENT ON NDAA SECTION 889

Hikvision is gravely disappointed that the 2019 NDAA provision has taken effect without a review or investigation to warrant the video surveillance technology restrictions outlined in Section 889. We believe this provision targets Hikvision without reason or evidence of wrongdoing. Meanwhile, we are evaluating every option available to contest this groundless inclusion and protect the rights and interests of the Company and our partners.

Since 2001, Hikvision's products have safeguarded people, communities, property and assets around the world. We have made great efforts to ensure the security of our products adhere to all that is mandated by the U.S. Government, including the Federal Information Processing Standard (FIPS) 140-2 certification from the National Institute of Standards and Technology.

## THE DEPARTMENT OF DEFENSE, U.S. INTEGRATORS, MAJOR U.S. TRADE ASSOCIATIONS, INDUSTRY THOUGHT LEADERS ADVOCATE AGAINST PORTIONS OF NDAA; REQUEST IMPLEMENTATION DELAY

- On June 11, 2020, The Honorable Ellen Lord, Under Secretary of Defense for Acquisition and Sustainment at the Department of Defense, testified at a House Armed Services Committee that *"The Department of Defense is a bit concerned about the two-year deadline. We believe we need to extend it in terms of time for compliance so that we do not have any unintended consequences. I am very concerned about being able to implement it in August as well as totally comply within two years. I am concerned that we might have some unintended consequences with shutting down major portions of our DIB because of one infraction of a camera in a parking lot somewhere at a level 4 supplier."*

- According to a June 10, 2020 Bloomberg article, *"Companies want delay, narrowing of scope in next stimulus bill."* The article goes on to say, *"The business community is asking Congress to insert language into the next coronavirus stimulus package to delay the implementation and then clarify the scope when the next Defense authorization bill comes up for debate, according to people familiar with the deliberations. … Some administration officials are aware of the potential negative consequences for U.S. businesses and the government, but they are also wary of the optics in the current political environment should they intervene to narrow the scope of the law, people familiar with the internal deliberations said. … In recent months, trade groups that represent companies like Lockheed Martin Corp., Amazon.com Inc., Apple Inc., 3M Corp. and Ford Motor Co., have been pushing the Trump administration and lawmakers to fix the wide-ranging provision. They also want to delay its implementation to ensure firms can comb through their supply chains to comply, a task made more difficult by the global pandemic."*

- On April 15, 2020, a coalition of prominent U.S. associations, including the U.S. Chamber of Commerce, sent a letter to Members of Congress requesting a one-year delay in implementing part B of section 889. This would allow more time to fully address some of the confusion caused by the scenarios many customers are facing. To view this letter, click here. According to the letter, *"If part B is implemented as written, many businesses with international and domestic operations will be forced to halt their work providing key products and services to agencies, including equipment that is needed to fight the coronavirus pandemic today and in the coming months."*

- According to Reuters, at a July 19, 2019 Town Hall with U.S. General Services Administration, Rick Williams, the general manager of Selcom, a 10-person company based in Selma, Alabama, said at the meeting that small companies like his *"need guidance."* Williams said he's *"worried about losing business with schools, which receive federal funding."*

- Peter Micek, general counsel at digital rights group Access Now, told Politico that he *"agrees that the U.S. should be looking at the video surveillance industry across the board and not just singling out companies from specific countries. Politically motivated restrictions like this one don't provide the comprehensive, human rights-based frameworks that we need and deserve."* He also indicated that *"the government should set security standards or assessments for all companies that provide the government with surveillance equipment."*

- According to Politico, *"Industry executives and representatives say the nature of most video surveillance systems makes it difficult, if not impossible, to manipulate in a way that would allow the Chinese government to spy on U.S.facilities. What's more, they say, most of the equipment operates on a closed-circuit network and does not connect to the Internet."*

## HIKVISION WORKING WITH THE U.S. GOVERNMENT & U.S. GOVERNMENT OFFICIALS ON HIKVISION'S CYBERSECURITY

- According to The Wall Street Journal published on August 16, 2019:
  A Hikvision executive this year repeatedly asked the GSA to remove the company's products from the GSA Advantage platform, according to emails reviewed by The Wall Street Journal. He told GSA the equipment had been listed with false country-of-origin data four or five times in recent years. GSA officials responded by saying they removed some of the items and that an automated solution was on the way, according to the emails.

- Previous reporting by The Wall Street Journal with specific statements showing that Army officials didn't deem Hikvision's equipment to be a security risk:
  The Wall Street Journal, Surveillance Cameras Made by China Are Hanging All Over the U.S., November 12, 2017
  *Chris Nickelson, NexGen's owner, says none of his customers have raised any issues about Hikvision gear. The army base referred questions to the U.S. Army's installation management command public affairs office, which said it doesn't discuss equipment or capabilities, but added that "any equipment or software that goes on a military network is thoroughly tested for security vulnerabilities."*

- The Wall Street Journal, Army Rips Out Chinese-Made Surveillance Cameras Overlooking U.S. Base, January 12, 2018
  *"We never believed [the cameras] were a security risk. They were always on a closed network," Col. Beck said. The decision to replace the cameras was meant to "remove any negative perception" surrounding them following media reports, he added, without elaborating.*

- The Wall Street Journal, Bill Moves to Block U.S. From Buying Chinese Surveillance Equipment, May 25, 2018
  *"The company's cameras were present in Fort Leonard Wood, a U.S. Army base in the Missouri Ozarks, and at one time in the U.S. Embassy in Kabul, The Wall Street Journal reported last year. Officials at Fort Leonard Wood later removed the devices, though the base's chief of staff said that he didn't deem the cameras to be a security risk."*

- U.S. House of Representatives Small Business Committee Hearing from January 2018:
  On January 30, 2018 the U.S. House of Representatives Small Business Committee held a hearing where then-Chairman Steve Chabot and representatives from the Department of Homeland Security (DHS) and Federal Bureau of Investigation (FBI) highlighted the need for increased cybersecurity support for small businesses.

- As a part of the hearing, discussing a previously discovered vulnerability, Richard Driggers, Deputy Assistant Secretary for DHS' Office of Cybersecurity and Communications, responded to questions about the vulnerability by saying:
  *"With regards to this particular flaw, we did work with the research community. We discovered the vulnerability. We worked with the company. And they put out a software update that mitigated the impacts of this particular exploitation. That's, kind of, standard practice that we do at the Department of Homeland Security across many different companies' devices and software."*

## HIKVISION ON CYBERSECURITY

- In March 2018, opened a Source Code Transparency Center for U.S. and Canadian government and law enforcement officials to review the source code for products sold in the market.

- Hikvision has received FIPS 140-2 certification, the NIST standard for encryption, for our IP cameras and NVRs.