



Troels Lund Poulsen
Acting Minister of Defence
Ved Stranden 8
1061 Copenhagen K

20 June 2023

Dear Minister

Hikvision is writing to you in response to recent parliamentary questions raised about our company and we would like to take the opportunity to provide you with more details and facts and correct any misperceptions about our company that exist in Denmark.

Ownership

Hangzhou Hikvision Digital Technology Co., Ltd. (“Hikvision”) has grown from a 28-person start-up in 2001 to a global technology company, providing products in more than 150 countries and regions around the world. Hikvision is committed to serving our customers and communities worldwide, with a longstanding record of protecting people and their property.

Hikvision is an independent, global, publicly-traded company listed on the Shenzhen Stock Exchange with a diverse set of shareholders. The company’s ownership structure is publicly available. According to the Quarterly Report of Q1 2023, 40.76% of Hikvision’s shares are jointly owned by a State-Owned Enterprise (SOE), and 10.28% is privately owned by Mr. Gong Hongjia, an overseas private investor. The remaining is owned by the company’s founders and executives, and A-shares investors. Neither the Chinese Government, nor the SOE, is involved in the day-to-day operations of Hikvision.

National Security

Some of the parliamentary questions raised a concern about Hikvision being a threat to national security in Denmark. Hikvision is not a threat to national security in Denmark and in anywhere else around the world. No respected technical institution or assessment has come to this conclusion. In fact, an [October 2022 report](#) from the Atlantic Council found that, “Currently, there is no empirical evidence from the ground that demonstrates the systematic coordination between Beijing and Hikvision in the purposeful theft of personal data.” Hikvision products are fully compliant with the applicable laws and regulations in Denmark. The company strictly follows all applicable data protection laws, regulations and norms of operating in the world and the European Union.

To be clear, Hikvision products do not have a “backdoor”, technological or otherwise. Hikvision products do not send data to China. Hikvision has never conducted, nor will it conduct, any espionage-related activities for any government in the world. Fears of espionage are far-fetched and utterly unsupported by any evidence.

As a manufacturer, Hikvision has no visibility into end-users' video data and cannot access end users' video data. In overseas markets, the company’s customers are distributors and security integrators/installers, not the end-user. Based on this business model, the end-user has full ownership of the data. Therefore, Hikvision cannot transmit data from end-users to third parties.



In April 2023, after an extensive review the Irish parliament [declared that Hikvision cameras were not a safety risk](#) as there ‘was no potential for images to be transmitted’.

Vulnerabilities and Cybersecurity

Hikvision believes it is our responsibility to be vigilant about cybersecurity threats. Over the past several years, Hikvision has prioritized and invested significant resources into expanding its cybersecurity efforts. Hikvision products currently meet industry-leading standards including: ISO 27001, ISO 9001:2008, CMMI Level 5, AICPA SOC and ISO 28000:2007. Hikvision has also achieved CC EAL3+ Certificate for network cameras, which represents the highest level of Common Criteria security certification that has ever been granted to video security products in the industry.


Vulnerabilities are a common and accepted occurrence in coding, and technology more broadly. Regarding the two specific vulnerabilities referenced by PET, Hikvision has made a public [disclosure](#) on its website on March, 2017. To further illustrate that, Richard Driggers, Deputy Assistant Secretary for DHS’ Office of Cybersecurity and Communications, responded to the relevant questions in a [January 30, 2018 House of Representatives Small Business Committee](#) hearing 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 is a CVE Partner, one of approximately 300 in the world, who manage the CVE database of known vulnerabilities. Hikvision is committed to continuing to work with third party white-hat hackers and security researchers to find, patch, disclose and release updates to products in a timely manner that is commensurate with our CNA partner companies' vulnerability management teams. Here is the link to the [CVE website](#) that will provide more detailed information. Hikvision is proud to be part of this global solution to make products and the Internet, a safer place.

We look forward to continuing to support the security and growth of Danish companies, local authorities, and private citizens with our innovative products and solutions.

Please let us know of any further questions.

Sincerely,

Nathan Zheng 
General Manager of Hikvision Nordic