



ONE HUNDRED EIGHTEENTH CONGRESS
REPRESENTATIVE CHRISTOPHER H. SMITH, CHAIR
SENATOR JEFF MERKLEY, COCHAIR

October 31, 2023

Rob Aarnes
President
ADI Global Distribution
275 Broadhollow Road, Suite 400
Melville, NY 11747

Dear Mr. Aarnes:

We write to express concerns about your company's sale of Hangzhou Hikvision Digital Technology ("Hikvision") and Dahua Technology ("Dahua") video security equipment to American schools, hospitals, and other public and private entities in the United States. The telecommunication and surveillance equipment manufactured by these companies is a recognized threat to American users as the equipment is manufactured according to standards that could be leveraged by intelligence agencies of the People's Republic of China (PRC), where private sensitive information of Americans is likely stored. In addition, the sales of Hikvision and Dahua cameras to U.S. federal agencies, including U.S. military sites, is prohibited by the National Defense Authorization Act (NDAA). Despite this, we found that ADI's U.S. website still lists nearly a dozen Hikvision or Dahua security equipment as NDAA compliant, apparently marketing to those covered by the ban.

In addition to concerns about privacy, Hikvision and Dahua are both implicated by the U.S. government as enablers of genocide and crimes against humanity. In October 2019, the Department of Commerce placed both companies on its "Entity List" for their role in providing equipment to PRC government facilities used to arbitrarily detain over one million ethnic Uyghurs and other predominantly Muslim ethnic minorities in the Xinjiang Uyghur Autonomous Region (XUAR).

Leaked PRC government documents, known as the "Xinjiang Police Files," detailed how Hikvision cameras in particular are used to arbitrarily identify specific innocent individuals for detainment, including Uyghurs returning from abroad. Dahua is linked to the PRC's genocide through its development of "Uyghur alert" and tracking technology which identify so-called "hidden terrorist inclinations" through discriminatory facial recognition, and for its creation of "ethnicity tracking" standards within China.

If nothing else, we should all agree that American consumers should not be subsidizing the Chinese Communist Party's atrocities.

In November 2022, the Federal Communications Commission (FCC) deemed that telecommunications and surveillance equipment from Hikvision and Dahua posed an "unacceptable risk" to national security and announced that additional equipment sales in the United States would not be authorized until the companies submitted a plan for approval. Only Dahua submitted a plan, though the FCC did not approve it. New rules

issued in February 2023 state that the FCC will no longer approve plans from five different entities including Hikvision and Dahua and their respective subsidiaries and affiliates.

The above prohibitions recognize the need to secure our communications networks and supply chains from equipment that poses an unacceptable risk to the national security of the United States or the security and safety of American citizens. Analysis of Hikvision and Dahua security equipment found they are vulnerable to spying from hackers and information requests from PRC intelligence entities. These findings are especially concerning given that Hikvision cameras use the servers of Chinese service providers from major Chinese companies Tencent, Alibaba, and state-owned enterprise Chinanet.

As recently as this year, experts found vulnerabilities in Dahua products, including unauthorized viewing of video and audio feeds and archives, as well as unauthorized network access and remote tampering with settings. U.S. consumers, schools and private businesses should not have to worry about how their data is stored and whether it will be accessed by foreign governments. The cybersecurity of your U.S. customers, which includes large and small companies, schools, and remote working professionals, should be of paramount concern.

Best Buy, Lowe's, and Home Depot dropped the sale of Hikvision and Dahua security equipment, citing human rights and supply-chain concerns. Your competitor Wesco/Anixter announced plans to drop cameras from Dahua and Hikvision because of "applicable U.S. laws and regulations."

We noticed ADI has not made a similar announcement, even after news broke that U.S. Department of Defense documents describe Hikvision as a partner of "Chinese intelligence entities" and "using relationships with resellers to disguise its products for sale to government suppliers."¹ These documents also claim that as of January 2023, rebranded Hikvision products were still available to customers in the U.S. government. If your company is engaged in such practices, we ask that you detail them for us thoroughly in your response.

In the current global context, the partnerships between U.S. companies and PRC entities are a congressional concern, particularly if those partnerships threaten national security, the private sensitive information of American citizens, or the freedoms guaranteed to both the Chinese and American people. Given your company's ongoing relationship with Hikvision and Dahua, we ask that you respond to our questions below, as we are compiling information for future reports and a hearing where we may request your testimony.

Questions

1. Given that major retailers and your competitor are no longer selling Dahua or Hikvision products, and given concerns about consumer safety and supply-chain problems, what is the rationale for your continued marketing of these products to American customers? What is your plan to comply with FCC restrictions on the sale of telecommunications and security equipment manufactured by Hikvision and Dahua moving forward?
2. How is the sale of security equipment from Hikvision and Dahua compliant with NDAA restrictions, as stated on your website?

¹ Tessa Wong, Paul Adams, and Peter Hoskins, "Hikvision: Chinese Surveillance Tech Giant Denies Leaked Pentagon Spy Claim," *British Broadcasting Company*, April 18, 2023, <https://perma.cc/6F2A-RWWW>.


3. Is your company aware that the U.S. Department of Defense reportedly concluded that Hikvision is a partner with Chinese intelligence entities, and do you make this information available to your clients? If not, why not? If so, can you give us examples of how your clients are explicitly informed of this fact?
4. The U.S. Department of Defense also reportedly concluded that Chinese security equipment companies are “using relationships with resellers to disguise its products for sale to [U.S] government suppliers.” Is ADI disguising products made by Dahua and Hikvision for sale to federal agencies? What evidence can you provide the Commission to rule out this possibility? If you are rebranding such equipment for sale, what brand names are they sold under? Are you selling to U.S. government customers and are they aware that the security equipment being bought is simply Hikvision and Dahua equipment sold with a different label?
5. Has ADI done an analysis of the security risks associated with Hikvision and Dahua security equipment? If so, is this analysis and any associated warnings easily available to customers? Are your customers aware of the security risks more generally and offered assistance for ways to protect their sensitive personal data?
6. Given that schools and school systems are a major customer of your security cameras, what extra steps are you taking to ensure the personal and data privacy of American children and students?
7. Are you selling to U.S. military personnel for personal and/or private business use? If so, are they made explicitly aware of the NDAA restrictions on the security equipment at military facilities and the security risks associated with this equipment, particularly from the People’s Republic of China?
8. Has your company done an assessment of the material and reputational risks associated with the sale of brands linked to genocide and crimes against humanity in the PRC? If not, why not, and do you think consumers should be made aware of the links?
9. Does your company have a compliance department and have they assessed the risks associated with a failure to disclose those risks resulting from your association with Hikvision or Dahua? If so, can you share with us that assessment?
10. Does your company accept or has it ever accepted discounts or other incentives from Hikvision or Dahua?

Thank you for your consideration. We look forward to your response.

Sincerely,



Representative Chris Smith
Chair



Senator Jeffrey A. Merkley
Cochair