

January 12, 2022

The Honorable Robin Carnahan  
Administrator  
General Services Administration  
1800 F Street NW  
Washington, D.C. 20405

Dear Administrator Carnahan:

I write with regard to recent reports<sup>1</sup> that, as recently as May and July 2021, the Drug Enforcement Agency (DEA), the U.S. Department of Defense's Defense Finance and Accounting Service (DFAS), and the Department of the Army purchased hard drives and video surveillance equipment manufactured by Lorex, a wholly owned subsidiary of China-based Dahua Technology. Pursuant to Section 889 of the Fiscal Year 2019 National Defense Authorization Act, executive agencies are prohibited from purchasing or obtaining equipment, systems, or services provided by Dahua and its subsidiaries, given concerns that it could assist the Chinese Communist Party (CCP) in ongoing espionage efforts. Also, as you may know, the U.S. Department of Commerce has added Dahua to its Entity List because of its ties to ongoing, CCP human rights abuses, including genocide and forced labor, against Uyghurs and other predominantly Muslim ethnic groups in the Xinjiang Uyghur Autonomous Region.

According to December 2021 reporting,<sup>2</sup> the DEA purchased nine Lorex hard drives for surveillance systems in May 2021 via a General Services Administration (GSA) portal called GSA Advantage, while DFAS bought Lorex video surveillance cameras via Focus Camera, a vendor also listed in the GSA Advantage catalog. The Army purchased Lorex cameras via Focus Camera, as well as through vendors I. S. Enterprises and JLogistics. I am aware that the GSA is planning a new, verified products portal to ensure the compliance of commercial-off-the-shelf (COTS) products listed on GSA Advantage with current law and regulations, but it is nonetheless unacceptable that Dahua/Lorex products were not banned from the site before August 13, 2019, when the prohibition timeframe was widely known. There is no excuse for a nearly two-year gap during which contractors could have purchased dangerous Chinese goods and equipment.

The CCP holds tight reins on Chinese technology companies and requires these companies' involvement in state-sponsored espionage activities. Under Article 7 of the PRC's 2017 National Intelligence Law and the 2014 Counter-espionage Law, Chinese technology companies are not allowed to refuse CCP requests to turn over any data to which they have

---

<sup>1</sup> [US Military & Gov't Break Law, Buy Banned Dahua/Lorex, Congressional Committee Calls For Investigation \(IPVM\)](#)

<sup>2</sup> [Us Government Agencies Bought Chinese Surveillance Tech Despite Federal Ban \(TechCrunch\)](#)

access. Fears about the susceptibility of Dahua users to wiretapping have been repeatedly raised, with senior U.S. Department of Defense officials expressing in 2019 that they are “concerned” by the tremendous cybersecurity vulnerabilities.<sup>3</sup> That federal agencies purchased Dahua COTS products on GSA Advantage through May 2021 exposes a critical gap in U.S. national security, affording the CCP a potential pathway into the daily activities of U.S. federal agencies who utilize this technology, including sensitive military information.

I urge you to take immediate action to ensure that COTS products sold by blacklisted Chinese companies are blocked from GSA Advantage’s portal. Given the clear national security concerns at hand, I also request answers to the following questions:

- Have all products covered under Section 889, including Lorex and Dahua hard drives and surveillance technology, been removed from GSA Advantage, including direct listings or ones listed through vendor partners?
- What criteria does the GSA use to vet suppliers connected with and products listed on GSA Advantage?
- If the technology in question has been banned since one year after the passage of the FY19 NDAA – over two years ago from today – why was it still available for purchase on GSA Advantage as late as summer 2021?
- What actions will the GSA take to track banned products sold since being blacklisted on the NDAA or Entity Lists, such that these kinds of cases can be brought to light?
- Should a GSA vendor represent itself as not providing or using covered products, current GSA rules appear to direct GSA contracting officers to take the offeror or contractor at its word, barring any “independent reason” to question it. Will the forthcoming verified products portal function differently and apply a higher level of scrutiny?

I appreciate your attention to this important matter.

Sincerely,



Marco Rubio  
U.S. Senator

---

<sup>3</sup> [US DoD Comments on Huawei, Hikvision, Dahua Cyber Security Concerns \(IPVM\)](#)