POLICY MEMO

China TECH THREAT

TO: INTERESTED PARTIES

DATE: SEPTEMBER 25, 2023

FR: CHINA TECH THREAT

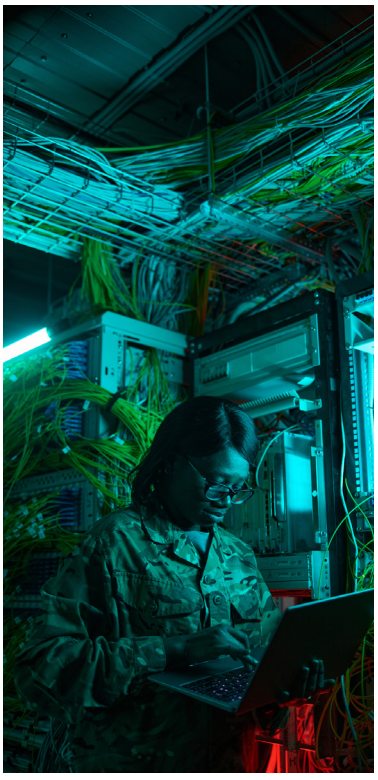
RE: **HOW A PENTAGON-RESTRICTED CHINESE TECH COMPANY HAS INFILTRATED U.S. NAVY BASES + FOUR RECOMMENDATIONS TO FIX THE VULNERABILITY**

The Problem: High-Risk Chinese Tech Products in Government Networks

At a time when the House Select Committee on the Chinese Communist Party is investigating how Chinese nationals have gained access to U.S. military installations, it should put an equal focus on how companies substantially owned by Chinese entities have successfully and legally deployed their products inside the Department of Defense. This strategy was brazenly put on display at the Naval Air Station Oceana air show this month in Virginia Beach, VA.

Companies owned and operated by China-based entities are required to do what the Chinese Communist Party (CCP) commands. Under Article 7 of China's 2017 National Intelligence Law, all businesses registered in China are obligated to hand over whatever information the Chinese Ministry of State Security demands of them—and that could very well include sensitive American user, financial, and health information. The law requires network operators, including all companies headquartered in China, to store select data within the country and allow Chinese authorities to do "spot-checks" on a company's network operations. The Party's control over Chinese owned and operated companies creates the potential for Chinese companies to serve as state-directed conduits for cyberattacks, data theft, and surreptitious surveillance. Governments around the world have already acted on these fears by banning Chinese companies Huawei and ZTE from telecommunications systems.

Unfortunately, the Pentagon has been lethargic in acting on its own recommendations to restrict Chinese companies such as Lexmark and Lenovo from its own systems. In 2019, a U.S. Department of Defense Inspector General report warned that products made by both of these companies boasting Chinese ownership presented "known security risks." Other government agencies are also aware of the dangers of both companies. For example, in 2018, The Social Security Administration won a federal court case when it contended that printers manufactured by Lexmark presented "an unacceptable supply chain risk to the government" due to the company's Chinese ownership and ties to the Chinese government.



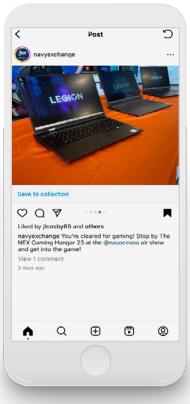
The federal government has also become wary of Hikvision, the Chinese surveillance gear giant. The Pentagon has already banned it, and multiple news reports have implicated the company in the CCP's genocide of Uyghur Muslims in western China. Technology news site IPVM has documented Hikvision's "top supplier status" for the Chinese military and role in "collaborating on PLA (People's Liberation Army) research." But many state law enforcement agencies, and even school districts, have purchased Hikvision products.

Another concerning Chinese company is Chinese drone manufacturer DJI, which the Pentagon has banned. Yet as of August 2021, 90% of U.S. public safety organizations using drones used a DJI-made product for their drone needs, and states continue to buy them in substantial quantities. These purchases run contrary to DOD's assessment that "systems produced by Da Jiang Innovations (DJI) pose potential threats to national security." National security expert and former Heritage Foundation scholar Klon Kitchen has stated, "DJI's manipulation and use of local and state law enforcement is part of a broader political influence campaign inside of and targeting the United States." Foundation for American Innovation researcher Lars Schönander recently documented how 85% of the drones bought by state agencies from 2010 to 2022 were Chinese.

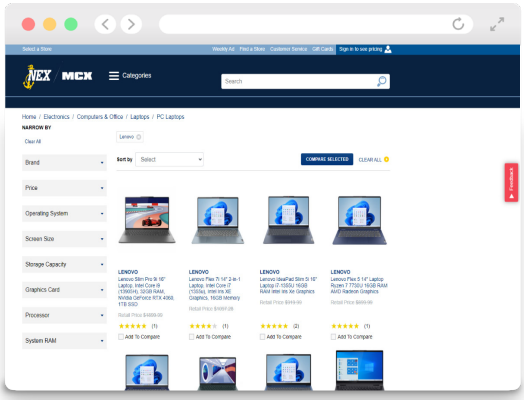
Lenovo's Infiltration of U.S. Navy Bases

The U.S. Navy continues to maintain a relationship with Lenovo, even selling its products through the Navy Exchange. Naval Air Station Oceana, located in Virginia Beach, VA, hosted the 2023 NAS Oceana Air Show on September 16 and 17, 2023. We know that Lenovo was an official sponsor of the Navy Exchange's (NEX) Gaming Hangar, a forum for the video gaming community.

Furthermore, the Navy Exchange's Instagram post below documents that Lenovo was promoting its Legion line of laptops at its booth inside the Gaming Hangar.



Additionally, a simple search of the Navy Exchange's website on September 19, 2023, reveals a variety of Lenovo laptops for sale through the exchange:



Background on Lenovo

Lenovo is the world's largest manufacturer of personal computers, with headquarters in China and a U.S. headquarters in Morrisville, North Carolina. According to its own financial filings, a company called Legend Holdings owns a 32.5% equity interest in Lenovo. Legend Holdings boasts that it is "ranked in the top 10 among the 'Top 500 Private Enterprises in China' by the All-China Federation of Industry and Commerce." But Legend Holdings, like all companies in China, is only nominally private. Legend Holdings lists the government-run Chinese Academy of Science Holdings as "a substantial Shareholder," and in fact CAS owns 63% of Legend's domestic shares and 29% of total issued shares. Consequently, the Chinese government is Lenovo's largest shareholder. The venture capital arm of Legend Holdings, Legend Capital, has been an investor in the Chinese company iFlytek, which has supplied voiceprint recognition technologies to the Xinjiang Bureau of Prisons.

Lenovo products have already been banned, investigated, or deemed vulnerable by the State Department in 2006, the Department of Homeland Security in 2015, the Joint Chiefs of Staff Intelligence Directorate in 2016, and the DoD Information Network in 2018.

The Department of Defense has already taken steps to keep Lenovo products away from its systems. In 2008, the U.S. Marine Corps in Iraq discovered that Lenovo products altered through the inclusion of secretly planted chips were transmitting data to China, forcing the Corps to ditch the company's wares.

> "A large amount of Lenovo laptops were sold to the U.S. military that had a chip encrypted on the motherboard that would record all the data that was being inputted into that laptop and send it back to China....That was a huge security breach. We don't have any idea how much data they got, but we had to take all those systems off the network."
>
> *— Lee Chieffalo, Marine network operations officer in Iraq*

That incident wasn't the only one reflecting the U.S. military's concern with Lenovo. In 2015, the U.S. Navy replaced $378 million worth of its IBM servers after Lenovo purchased them, out of fear China could access data on U.S. ballistic missile technology. The Air Force was also forced to ask Raytheon to rip-and-replace IBM hardware after the Lenovo purchase, and it ditched Lenovo routers in 2016.

State Momentum to Ban Risky Chinese Tech Products Is Rising

Momentum to ban products made by Chinese companies such as Lenovo, Lexmark, Hikvision, and DJI has also increased at the state government level. As China Tech Threat has documented in a May 2023 report, more than ten U.S. states have either barred Chinese equipment from state contracts, or are in the process of doing so. In one ironic moment on March 21, 2023, State Senator Lisa Keim of Maine noted that a committee staff analyst on the dais was using a Lenovo computer during a hearing on restricting Chinese tech products from state contracts. Senator Keim said, "If Chinese technology is being used anywhere in our state, the Chinese government has access to our private information. Maine is vulnerable in at least in one known way: Lenovo laptops, which are used throughout state government."

On the whole, however, as CTT's original research demonstrates, states have unfortunately followed the U.S. government's lead, counting on Lenovo (and Lexmark) to store sensitive information on areas including military, state police, election security, and state legislatures.

SAMPLE OF STATE AGENCIES USING TECHNOLOGY RESTRICTED BY U.S. NATIONAL SECURITY AGENCIES:

Election Oversight (Secretaries of State) – Delaware, Florida, New Jersey, Washington

Military Agencies – Georgia, Idaho, South Dakota, Texas, Virginia

State Police / Public Safety – Arkansas, Georgia, Massachusetts, Missouri, Nebraska, New York, North Carolina, Ohio, Oklahoma, Virginia

Legislatures – Alaska, Arkansas, Colorado, Kansas, Missouri, New Hampshire, New Jersey, New York, North Carolina, Texas, Utah, Washington, Wyoming

Recommended Actions

The Department of Defense must sever ties with companies owned or operated by Chinese entities, such as Lenovo, Lexmark, DJI, Hikvision, and others. Here are several recommendations:

1. Congress should ban the Pentagon from acquiring or selling products made by Chinese-owned and operated companies, or from partnering with them in any way.
2. The House Select Committee on the CCP should call the Under Secretary of Defense for Acquisition and Sustainment to brief Congress on whether (and how) the Pentagon is following up the recommendations made in the 2019 IG report on mitigating risks from commercial off-the-shelf technologies (COTS) made by Chinese-owned or operated firms.
3. The Committee should call the DOD's Chief Information Officer to brief Congress on how the DOD can identify and remove products made by Chinese-owned and operated companies already in its systems.
4. With support from the federal government and Congress, states must follow the lead of Georgia, Florida and others – including four states just in 2023 (Arkansas, Idaho, Indiana, and South Dakota) – that have restricted PRC-owned companies from bidding on contracts to supply technology to state government entities. (For more information visit www.StatesStopChinaTech.com.)