

STATES OF DENIAL VS. STATES OF MOMENTUM:

DANGEROUS CHINESE TECHNOLOGY
IN U.S. STATE GOVERNMENT
SYSTEMS AND RISING EFFORTS TO
PROHIBIT CONTRACTS SUPPLYING IT

FEBRUARY 23, 2023



EMBARGOED UNTIL FEBRUARY 23, 2023

REFRESH OF RESEARCH ORIGINALLY PUBLISHED IN MARCH 2020

TABLE OF CONTENTS

EXECUTIVE SUMMARY:	2
THE CHINESE GOVERNMENT IS PENETRATING U.S. STATE TECHNOLOGY ECOSYSTEMS, BUT STATE MOMENTUM TO STOP IT IS BUILDING	2
THREE KEY FINDINGS	3
BACKGROUND: THE STATE-FEDERAL CHINESE TECH DISCONNECT	3
WHY DON'T STATES IMPLEMENT RESTRICTIONS?	4
PROGRESS IS HAPPENING.....	5
MAP: States Taking Action Against Chinese Government-Owned Tech Manufacturers.....	6
Lawmakers Must Be Aware of Efforts to Weaken Legislation	7
...YET STATES CONTINUE TO PURCHASE DANGEROUS CHINESE TECH AND DEPLOY IT IN CRITICAL AGENCIES.....	8
MAP: U.S. State Spending on Restricted Chinese Government-Owned Tech Manufacturers	9
RECOMMENDATIONS TO COUNTER CHINESE TECH THREATS IN STATES	11
#1. Restrict Chinese-Owned and Operated Technology Companies from Bidding on State Contracts	11
#2. Preclude or Close Loopholes to Stop State Purchases through Third-Party Vendors	12
#3. Grow and Strengthen State Cybersecurity Workforces	12
#4. Increase Cooperation Between Congress and States to Enforce Export Control Laws	13
#5. Broaden Efforts to Include All U.S. Adversarial Nations	13
BACKGROUND ON SELECT CHINESE TECHNOLOGY MANUFACTURERS	14
LENOVO: LAPTOPS, LIES, AND LARCENY	14
LEXMARK: A BACKDOOR FOR MALIGN CYBER ACTIVITY	15
HIKVISION: A DE FACTO CHINESE GOVERNMENT SPY AGENCY	16
DJI: UNDERMINING AND MANIPULATING U.S. LAW ENFORCEMENT.....	17
APPENDIX A: NASPO-Authorized Lenovo Resellers.....	19
APPENDIX B: NASPO-Authorized Lexmark Resellers	20

Full Compilation of Resources Can Be Found at

www.StatesStopChinaTech.com

- Revised white paper with links and sources
- State-by-state contract summaries
- Details of actions taken in Georgia, Florida, and other states
- List of 2023 pending legislation and sponsors
- Link to Model Policy adopted by the American Legislative Exchange Council
- Articles, videos, and other materials

EXECUTIVE SUMMARY:

THE CHINESE GOVERNMENT IS PENETRATING U.S. STATE TECHNOLOGY ECOSYSTEMS, BUT STATE MOMENTUM TO STOP IT IS BUILDING

This paper updates a March 2020 China Tech Threat [paper](#) detailing how 40 U.S. state governments had entered into contracts to purchase millions of dollars worth of Lenovo and Lexmark products. The revised findings from states presented in this paper will be expanded with data from the remaining states in spring 2023.

This report also spotlights the presence of state contracts with two additional Chinese companies which were not covered in the 2020 paper – surveillance equipment manufacturer Hikvision and drone aircraft manufacturer DJI. A research report with a state-by-state analysis of DJI and Hikvision will come later this year.

Various U.S. state government bodies – whether offices, schools, or law enforcement agencies – have purchased products by each of these companies, and some in substantial quantities. By doing so, they have created threats to the American people. As companies either domiciled in China or substantially owned by China-based entities, they are bound by Chinese law to do what the Chinese Communist Party commands under China's 2017 National Intelligence Law. Lexmark, Lenovo, Hikvision, and DJI can variously collect or steal sensitive personal data or proprietary intellectual property, be deployed as conduits for cyberweapons, and conduct surreptitious surveillance on Americans.

The good news is that there is evidence of a shift at the state level to take these threats more seriously. **When we published our March 2020 study, only one U.S. state restricted contracts with Chinese-owned or operated tech manufacturers. Today five states have laws or restrictions governing state contracts, with 11 additional states currently considering legislation as of this writing.** In sum, states have acknowledged the seriousness of this problem and are pursuing solutions.

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



Arizona Board of Fingerprinting



Delaware Department of Elections



Idaho Military Division



Massachusetts Public Safety/Homeland Security



Legislatures in Alaska, Colorado, Kansas, North Carolina, New Hampshire, New York, and Utah

THREE KEY FINDINGS

1. **Chinese companies that have been banned or restricted from U.S. military and national security networks – e.g. Lenovo, Lexmark, Hikvision, and DJI – can still contract with state governments.** Lexmark and Lenovo can access sensitive personal and financial information held by courts, police departments, elections departments, education departments, children and family services, and other social service providers and agencies. In the case of Hikvision and DJI, they can also collect facial recognition and critical infrastructure data.
2. Despite escalating threats from China and greater awareness of national security vulnerabilities at the state level, **state government contracts and purchases from Lexmark and Lenovo have continued, and in some cases increased significantly** since China Tech Threat issued its first state contracts report in 2020.

Our latest review of contract information and public databases from 28 states found that states have cumulatively awarded a total of \$230 million worth of contracts for Lexmark or Lenovo since 2015, with individual states spending as much as \$47 million.

It is not just the volume of purchases that are of concern, but the types of state agencies using them. Numerous state government offices responsible for stewarding sensitive personal information have wired products made by Chinese-owned or operated companies into their networks. To give a few examples, the Delaware Department of Elections, the Hawaii Department of Taxation, and the South Dakota Department of Emergency Management have all used products by Lexmark or Lenovo.

3. **Actions such as Georgia [Senate Bill 346](#) and Florida [Executive Order 22-216](#) have inaugurated a new wave state government action to ban Chinese ICTS** (information and communications technology systems) from state government contracts. 2023 is poised to be a transformative year for states tackling Chinese tech threats.

BACKGROUND: THE STATE-FEDERAL CHINESE TECH DISCONNECT

In March of 2022, cybersecurity firm Mandiant reported that hackers operating at the direction of the Chinese government had penetrated six state government computer networks. Mandiant noted that the intruders were able to conduct this cyber breach by exploiting, in the words of the Associated Press, “a previously unknown vulnerability in an off-the-shelf commercial web application used by 18 states for animal health management.”¹ It’s clear China is targeting U.S. states through ordinary technologies, and not just the six identified by Mandiant. As cybersecurity expert Joseph Steinberg commented on the report, “If we know that six states were breached by Chinese spies, it means we know 44 states probably have Chinese spies operating on their network that we don’t know about.”²



Huawei says it would never hand data to China's government. Experts say it wouldn't have a choice

By Arjun Kharpal
MAR 5 2019

<https://www.cnbc.com/2019/03/05/huawei-would-have-to-give-data-to-china-government-if-asked-experts.html>

AP

**Cyber firm: At least 6
US state governments
hacked by China**

By Eric Tucker
MAR 8 2022

<https://apnews.com/article/technology-business-china-united-states-hacking-ffa2120239eb687ce1979bf9599dfea5>

State governments should know that Chinese malign actors are gaining access to their systems through loopholes in ordinary, commercially available technologies, whether they are Chinese-owned and operated or not. But Chinese companies are especially dangerous, because the institution of China's 2017 National Intelligence Law increases the risk of Chinese companies funneling sensitive American data to Beijing. Under Article 7 of the 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 user, financial, and health information. This 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.

It is for this reason dozens of countries around the world have blocked Chinese telecom company Huawei from their 5G networks, in spite of Huawei’s denial that it would hand over information Beijing requests. “There is no way Huawei can resist any order from the (People’s Republic of China) Government or the Chinese Communist Party to do its bidding in any context, commercial or otherwise,” said New York University professor Jerome Cohen.³ The same goes for other Chinese companies. And any company that is a supplier or partner with firms in China could also be subject to the law.

Companies controlled by China-based entities such as Lenovo, Lexmark, Hikvision, and DJI have proliferated their products throughout state government technology systems. That raises the question – why have states allowed it?

WHY DON'T STATES IMPLEMENT RESTRICTIONS?

While the U.S. federal government has taken admirable (if imperfect) strides to tackle high-profile Chinese tech threats in recent years, states have not kept up. Consequently, a misalignment of federal and state policies regarding Chinese technologies continues to grow. For instance, Section 889 of the National Defense Authorization Act prohibits the federal government from purchasing or using information and communications technology and services (ICTS) items from Chinese companies Huawei, ZTE, Hikvision, Dahua, and Hytera. Yet a study done by Georgetown University’s Center for Security and Emerging Technology (CSET) has found that “In recent years, nearly 1,700 public entities have purchased ICTS covered under Section 889, introducing potential vulnerabilities into the networks of public schools, universities, hospitals, prisons, public transit systems, and government offices nationwide.”⁴

1,700

Number of U.S. state and local governments that purchased Chinese technologies restricted by the federal government.

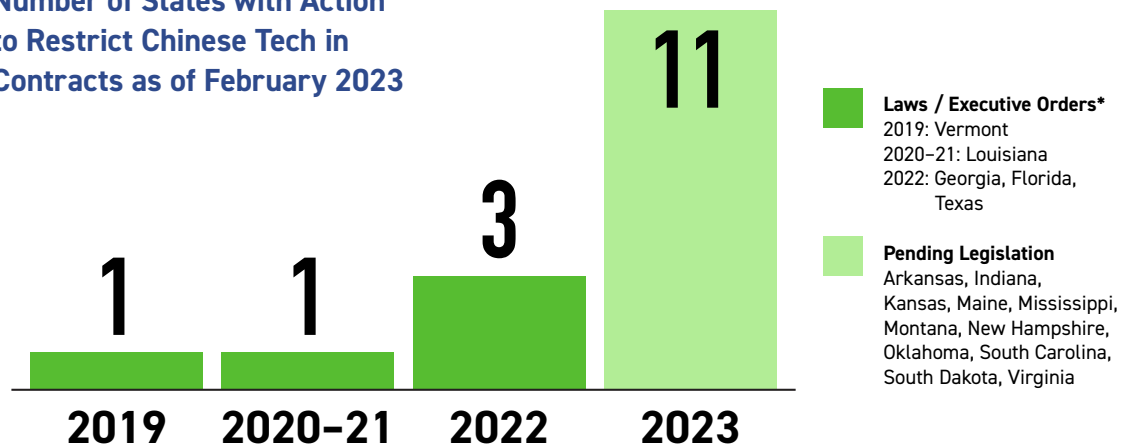
Why states have lagged the federal government is mostly a question of money, ignorance, and political will. The lack of uniform best practices across U.S. states to mitigate the danger from these companies has allowed the threat to go relatively unchecked. State technology and procurement officers may believe that products recommended by the National Association of State Procurement Officials (NASPO) have legitimacy, but NASPO does not consider security in its vendor recommendations, even in an age when states have become more vulnerable. Additionally, state governments – many of them acting under tight budget constraints – are disincentivized from choosing technologies that are typically more expensive than their Chinese counterparts. “Rip and replace” campaigns to eliminate Chinese gear from their systems are also expensive.

Even in an age where bipartisan consensus about the threat of China continues to grow, few state legislators have comprehended the national security implications of Chinese malign activity in their states, seeing national security as the preserve of the federal government. In spite of incidents like the hack of six U.S. states, threats can also seem abstract. Nor do state legislators – many of whom serve part-time – have clear political incentive or the appropriate technical knowledge to write effective legislation at the intersection of both technology and procurement rules. But state governments must close the federal-state restriction gap, because Sacramento and St. Paul are equally ripe targets for the Chinese government as Washington, D.C.

PROGRESS IS HAPPENING...

Thankfully, some states have started to act. Comprehensive actions in Georgia ([S.B. 346](#)) and Florida ([Executive Order 22-216](#)) last year (covered further in the Key Recommendations section) have helped raise the profile of the problem and the need for states to follow suit. Louisiana, Texas, and Vermont have also taken steps to stop Chinese companies from participating in state contracts. The American Legislative Exchange Council (ALEC) likewise adopted [model policy](#) in July of 2022 to help states stop using funds to “purchase technology products, and/or services from manufacturers or other providers that are owned by, affiliated with, and/or unduly influenced by the People’s Republic of China (PRC).”⁵ While some experts suggest that each of these approaches should be improved, the urgency of stopping the Chinese government from gaining further footholds in state government tech ecosystems is evident.

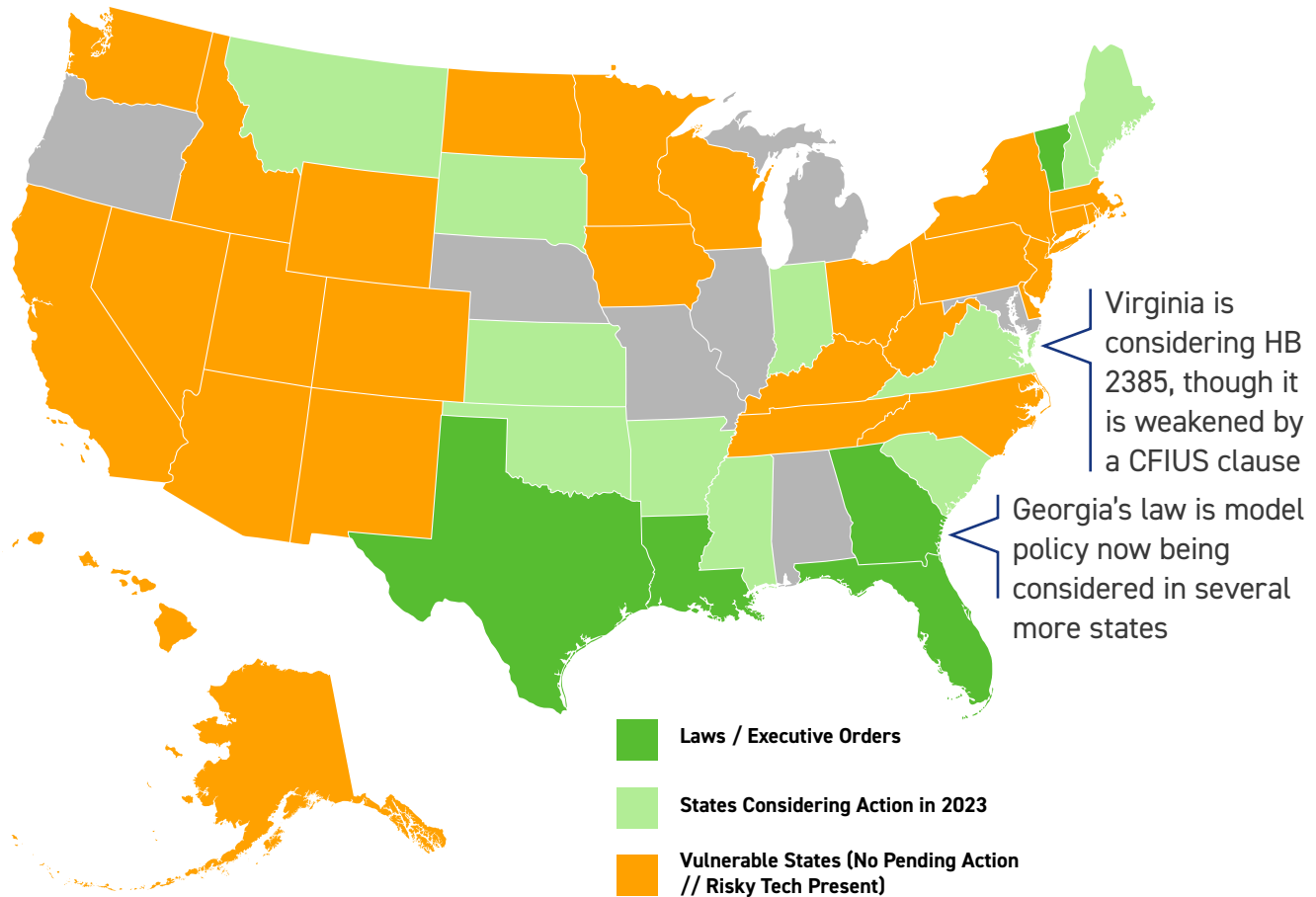
Number of States with Action to Restrict Chinese Tech in Contracts as of February 2023



*Sources are: Heritage Foundation, 7/27/22; CSET, 10/22

Momentum will continue in 2023, with lawmakers in nearly a dozen additional states already introducing bills in the weeks preceding the release of this report in February 2023:

States Taking Action Against Chinese Government-Owned Tech Manufacturers



This map reflects legislative efforts as of February 2023

STATE	BILL #	SPONSOR	SHORT DESCRIPTION / PURPOSE
AR	TBD	Rep. Mindy McAlindon	Prohibit contracts with companies owned or operated by the Government of China
IN	SB 477	Sen. Justin Busch	"Amends the statute prohibiting the use of public funds to purchase equipment or services produced or provided by certain prohibited persons determined to be a national security threat to communications networks or supply chains to also prohibit the use of public funds to purchase communications equipment"
KS	TBD	Rep. Chris Croft	TBD
ME	LR 1814	Sen. Lisa Keim	An Act to Prohibit State Contracts with Companies Owned or Operated by the Government of the People's Republic of China.
MS	SB 2046	Sen. Angela Burks-Hill	Prohibit "technology-related equipment manufactured within the borders of a hostile foreign nation or by a company headquartered within the borders of or having significant corporate or political ties with a hostile foreign nation"

MT	HB 602	Rep. Steven Galloway	"An Act prohibiting state contracts with Chinese government-owned or affiliated technology manufacturers"
NH	NB 86	Rep. Terry Roy	"Prohibiting the state from contracting with Chinese government owned or affiliated technology manufacturers"
OK	SB 43, SB 107	Sen. Micheal Bergstrom	"No state agency shall purchase any goods or services from or enter into contracts with any company owned or operated by the Government of China"
SC	H 3119	Rep. Doug Gilliam	"Prohibit certain contracts with certain foreign-owned companies in connection with critical infrastructure"
SD	SB 189	Sen. Jim Stalzer	"Prohibit state agencies from contracting with companies owned or controlled by" China and select additional countries
VA	HB 2385	Rep. Emily Brewer	"Prohibits state agencies from entering into a contract for goods or services with a scrutinized company, defined in the bill as any company owned or operated by a foreign adversary" <i>*weakened by CFIUS clause exemption</i>

Lawmakers Must Be Aware of Efforts to Weaken Legislation

Even as lawmakers take on Chinese tech threats, they must be vigilant against corporate lobbying to weaken their bills. Both Chinese companies and American resellers of Chinese equipment are looking to water down legislation.

Helpfully, the 2022 Georgia law (S.B. 346) broadly defined scrutinized companies as those "owned or operated by the Government of China."⁶ This comprehensive definition leaves little room for ambiguity.

In contrast, Virginia HB 2385 provides less stricter standard of scrutiny. That bill only bans equipment from "any company owned, controlled, or operated in whole or in part by a foreign adversary, other than a company for which the Committee on Foreign Investment in the United States (CFIUS) has determined that there are no unresolved national security concerns regarding the transaction that created such ownership or permitted such operation."⁷

The CFIUS clause opens a massive loophole. Many national security policymakers believe that CFIUS judgments are not a reliable barometer of which companies are national security threats. For instance, Congress and defense and intelligence agencies argued against CFIUS approval of Lenovo's 2014 acquisitions of IBM and Motorola business lines. Writing in 2020 with former Congressman Robert Pittenger (the sponsor of 2018 CFIUS reform), China Tech Threat contended that "with the new cybersecurity and personal information factors CFIUS must consider, the Lenovo acquisitions would not be approved today."⁸ In just one cautionary example, the U.S. Air Force decided to rip-and-replace hardware because of "security reasons following the sale of IBM's computer server product line to Chinese-owned Lenovo."⁹ Tethering state-level restrictions to CFIUS determinations assumes those that those determinations are flawless (they aren't) and also ignores the potential for entities CFIUS has previously approved to evolve in to threats (as the case of Lenovo shows). State lawmakers would be wise to end contracts with all Chinese-owned and operated companies.

...YET STATES CONTINUE TO PURCHASE DANGEROUS CHINESE TECH AND DEPLOY IT IN CRITICAL AGENCIES

China Tech Threat's original 2020 research found that nearly 40 states had contracts with and payments to Chinese government-owned technology manufacturers Lenovo and Lexmark. (See the summaries on why both companies are dangerous on pages 14-16 of this paper.)

Beginning in Fall 2020, we began to re-examine data from each state to determine if the states have made payments to either company, for how much, and where those products were deployed. **As of February 2023, we verified payments from 28 states totaling more than \$230 million since 2015, with some states spending as much as \$47 million on Lexmark or Lenovo products.** Several states appear to have significantly increased spending on Lexmark and Lenovo equipment in the past few years, including Arizona, Georgia, Florida, Hawaii, Idaho, Kentucky, Utah, and Wisconsin.

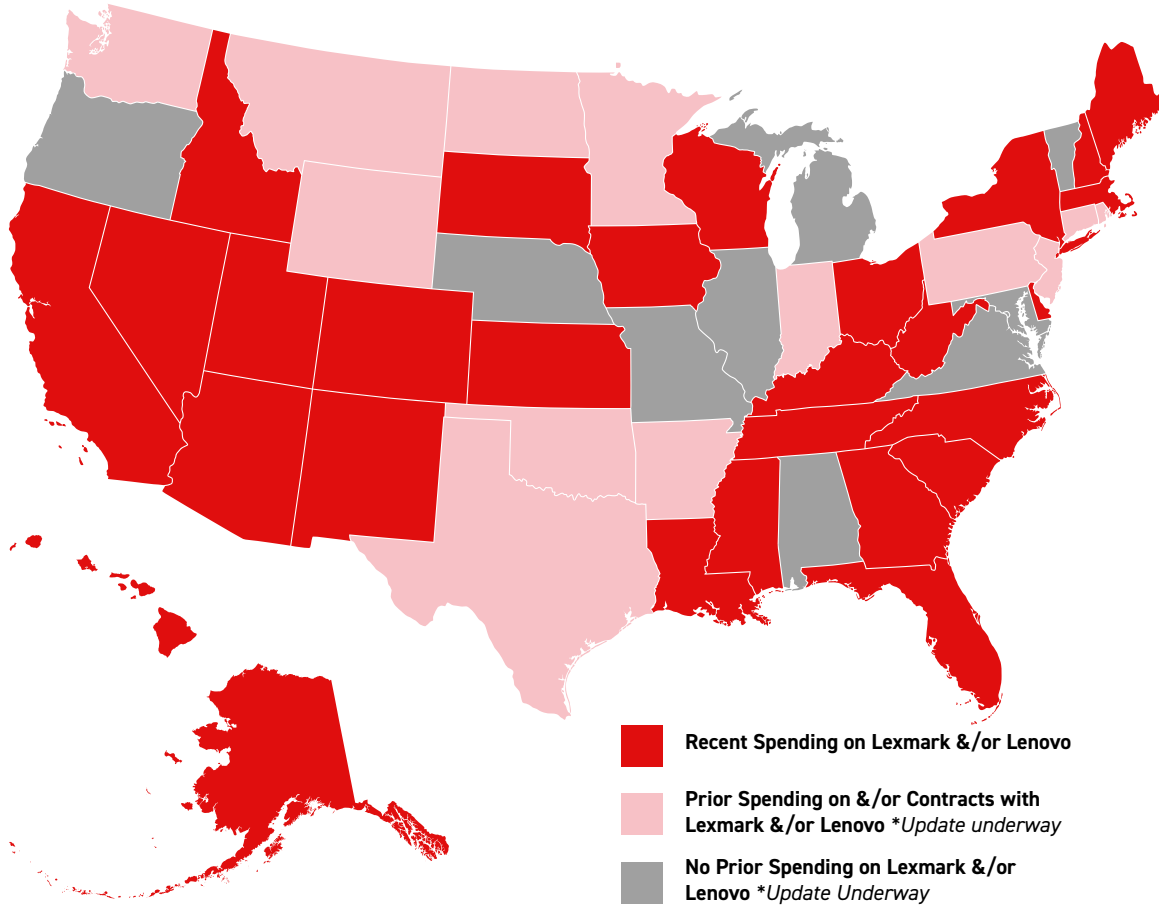
Just as important as the amount of taxpayer money being spent are the state agencies using these products. The introduction of Lexmark and Lenovo gear into state tech ecosystems means Beijing's intelligence-gathering operation is better able to access some of these states' most sensitive pools of citizen information. Agencies that have purchased technology from Lexmark and/or Lenovo include the Arizona Board of Fingerprinting, Kentucky State Police, Delaware Department of Elections, Wisconsin Supreme Court, Ohio Department of Public Safety, the Idaho Military Division, the South Dakota National Guard Armory, and the legislatures in Alaska, Colorado, Kansas, and New Hampshire.









\$230 million may sound like an incredible amount of money, but the total states are spending on dangerous Chinese technologies may be in fact understated. One important measure currently missing from most of our state calculations is payments through resellers. State government agencies do not always buy directly from Chinese-owned and operated companies, choosing instead to rely on American technology supply firms such as CDWG, Woodward Technologies / TwoTrees, Arey Jones, GovConnection, FireFly, Trinity3 Technology, and SHI. The National Association of State Procurement Officers has identified dozens of resellers offering Lenovo and Lexmark products and, like NASPO itself, these resellers do not consider the security implications of products manufactured by Chinese-owned or operated manufacturers. (See lists of NASPO-approved Lenovo and Lexmark resellers on pages 21-22.)











Below is a list of each state's spending as of February 2023, including a few agencies in each state. Much more state-by-state data is available at www.StatesStopChinaTech.com.

We will post additional state analysis on a rolling basis this spring.

U.S. State Spending on Restricted Chinese Government-Owned Tech Manufacturers



STATE	SPENDING	YEARS	PARTIAL LIST OF AGENCIES
 Alaska	\$1,273,408	2020-2023	The Legislature, Office of the Governor, Department of Labor and Workforce Development
 Arizona	\$7,315,675	2016-2023	Board of Fingerprinting, Department of Public Safety, Department of Education
 California	\$2,910,769	2019-2022	Department of Social Services, Department of Water Resources
 Colorado	\$4, 702,700	2016-2023	State Legislature, Department of Corrections
 Delaware	\$479,918	2017-2022	Justice Information System, State Policy Headquarters, Department of State, Office of the Attorney General, University of Delaware, Department of Elections
 Florida	\$29,149,590	2015-2022	State's Attorney General, Board of Elections, Department of Corrections, Public Utilities
 Georgia	\$47,259,946	2020-2022	Bureau of Investigation, Department of Public Safety, Superior Court Clerk, Fort Benning and Fort Stewart
 Hawaii	\$15,904,416	2015-2019	Department of Human Services, Department of Taxation, Attorney General's office

	Idaho	\$33,157,990	2015-2022	Idaho Supreme Court, Military Division, Lottery, Department of Lands
	Iowa	\$1,834,509	2021-2022	Department of Public Health, Department of Corrections, Department of Education
	Kansas	\$3,626,106	2016-2022	Department of Health, Office of State Bank Commissioner, Legislature, Department of Commerce, Board of Nursing
	Kentucky	\$5,762,445	2016-2022	Auditor of Public Accounts, Judicial Department, Department of Revenue, Kentucky State Police
	Louisiana	\$41,241	2019-2023	Attorney General
	Maine	\$5,350,803	2015-2023	Bureau of Informational Services
	Massachusetts	\$10,226,739	2015-2023	Office of Public Safety and Homeland Security, State Ethics Commission, Supreme Judicial Court
	Mississippi	\$442,109	2018-2022	Supreme Court
	Nevada	\$2,706,054	2019-2022	Department of Motor Vehicles, Department of Health and Human Services, Attorney General
	New Hampshire	\$204,765	2016-2022	Legislative Branch, Treasury Department, Judicial Branch
	New Mexico	\$1,043,136	2018-2022	Administrative Office of the Courts, Department of Ethics Commission
	New York	\$2,440,090	2018-2022	Attorney General, State Police, Legislative Bill Drafting Committee
	North Carolina	\$17,896,776	2021-2023	Department of Revenue, Administrative Office of the Courts, General Assembly, Department of Public Safety, Office of State Auditor, Department of Insurance
	Ohio	\$240,194	2016-2022	Department of Rehabilitation and Correction, Bureau of Workers Compensation, Department of Natural Resources, Department of Public Safety
	South Carolina	\$3,854,722	2018-2023	Department of Revenue, Education Department, Department of Health and Environment
	South Dakota	\$29,808	2016-2022	Department of Criminal Justice, Department of Emergency Management, Department of Health, National Guard Armory
	Tennessee	\$336,476	2019-2022	Department of Education, Department of Finance and Administration, Department of Treasury, Housing Development Agency, Court System
	Utah	\$34,401,444	2018-2021	Utah Legislative Branch, University of Utah, Board of Education
	West Virginia	\$482,606	2016-2023	Regional Jail and Correctional Facility Authority, Division of Motor Vehicles
	Wisconsin	\$4,751,370	2019-2023	Wisconsin Supreme Court, Department of Health Services, Department of Corrections, University of Wisconsin System

RECOMMENDATIONS TO COUNTER CHINESE TECH THREATS IN STATES

#1. Restrict Chinese-Owned and Operated Technology Companies from Bidding on State Contracts

Exemplary Action: Georgia Legislature Passed and Governor Brian Kemp Signed [S.B. 346](#) in May 2022; Florida Governor Ron DeSantis Signed [Executive Order 22-216](#) in September 2022.

Policy Guidance: In May 2022, Georgia Governor Brian Kemp signed S.B. 346, prohibiting Chinese “owned or operated” companies from bidding on state contracts. In July 2022, two task forces of the American Legislative Exchange Council unanimously adopted this law as the basis for [model policy](#) for U.S. states. As of February 2023, nearly a dozen states are currently considering legislation which includes elements of the ALEC model policy.

Similarly, Gov. DeSantis’ executive order prohibits Florida state and local government entities from procuring technology products and services from companies owned by, controlled by, or domiciled in China. The executive order directs the Department of Management Services to promulgate rules and take any additional action necessary to ensure commodities and services used by state and local governments are not susceptible to exploitation by foreign countries of concern.

It’s important that states do not focus legislative efforts on banning specific Chinese companies, because they are adept at conducting business under various subsidiaries or shell companies. As Michael Cunningham of the Heritage Foundation has written, “For the most part, state legislation related to Chinese technology purchases largely follows the federal government’s approach of prohibiting purchases from a pre-defined list of particularly egregious Chinese companies... As the legislatures of states around the country move to tackle the threats posed by involvement of Chinese companies in public contracts, they would be wise to follow the examples of Texas and Georgia in extending their ban beyond a negative list of predefined companies.”¹⁰

[When companies are] “wholly owned by the Chinese government we know they have a motivation, without a doubt, based on their past performance, to steal information from the United States government, from state governments, and from individuals and corporations.”



– GA State Rep.
Martin Momtahan

“There is the cybersecurity part and the acquisitions part. The way this is successful is when they work in tandem. Setting the cybersecurity standards is critical.”



– Pedro Allende,
Florida DHS Secretary

#2. Preclude or Close Loopholes to Stop State Purchases through Third-Party Vendors

Certain states have banned contracts with companies owned or operated by China – a helpful measure. But state government agencies do not always buy directly from Chinese owned and operated companies, choosing instead to rely on American technology supply firms such as CDWG, Woodward Technologies / TwoTrees, Arey Jones, GovConnection, FireFly, Trinity3 Technology, and SHI. Like NASPO, these resellers do not consider the security implications of offering products from Chinese-owned or operated manufacturers; their goals are to win contracts.

See [Appendix A](#) of this report for NASPO's list of vendors selling Lenovo products.

See [Appendix B](#) of this report for NASPO's list of vendors selling Lexmark products.

Permitting third-party vendors to sell Chinese equipment to state government entities defeats the purpose of China-focused ICTS legislation. As scholars at CSET have written, it is often the case where “Purchasing a Hikvision surveillance camera directly from Hikvision would be illegal, but purchasing the exact same camera from a local vendor would not.” Georgia’s S.B. 346 includes a provision restricting the awarding of contracts to “affiliates of such entities or business associations” – meaning Chinese companies.¹¹ But there is concern that it is not sufficient to stop Chinese technology from getting into state government systems via third-party sellers.

While Georgia’s decision to pass one of the first laws in the nation restricting Chinese technology contracts is a praiseworthy event, independent reviews by CSET and the Heritage Foundation expressed concern that third-party vendors may continue to sell restricted Chinese equipment.

Policy Guidance: States must work to close loopholes in legislation that allow states to purchase equipment from Chinese-owned and operated companies via third-party vendors.

#3. Grow and Strengthen State Cybersecurity Workforces

Exemplary Action: As part of Idaho Governor Brad Little’s “Leading Idaho” plan, the legislature approved \$12 million for a new Cyber Response and Defense Fund.

Policy Guidance: America’s cyber workforce is not large or skilled enough to address the rate and sophistication of cyberattacks. States need to assess their cyber workforce, identify priorities and gaps, and recruit and strengthen cyber workers accordingly. In March 2022, Governor Little’s [Cybersecurity Task Force Report](#) published 18 recommendations to defend sensitive personal and financial information held by courts, police departments, elections departments, education departments, children and family services, and other social service providers and agencies. Other states would do well to take on these recommendations.

#4. Increase Cooperation Between Congress and States to Enforce Export Control Laws

Exemplary Action Needed: In January 2022, two New York members of Congress, John Katko and Andrew Garbarino, issued a letter asking the Department of Homeland Security and Commerce Department to “support States to ensure they are not unwittingly procuring products that will create vulnerabilities at the State level.”¹² Governors should exert similar pressure on federal agencies to ensure compliance with regulations.

Policy Guidance: The federal government employs tools like export controls to protect America's strategic technologies from falling into the hands of adversaries. Mitigating threats at the state level requires a cooperative effort by state and congressional leadership to call on federal agencies, including the Departments of Commerce, to honor the export control regime. In doing so, they should also call for ChangXin Memory Technologies (CXMT) to be added to the Department of Commerce Entity List, and an expansion of export controls targeting Semiconductor Manufacturing International Corporation (SMIC).

#5. Broaden Efforts to Include All U.S. Adversarial Nations

Exemplary Action: Some critics claim that China-focused national security measures are driven by xenophobia, but FBI Director Christopher Wray clearly disagrees: “The greatest long-term threat to our nation's information and intellectual property, and to our economic vitality, is the counterintelligence and economic espionage threat from China.”¹³ China's strategy for eroding American power and economic competitiveness depends in large part on its ability to exploit existing technology systems. No adversary has more companies that have already penetrated American systems than China (see the background information on Chinese companies of concern below). No adversary has the technological prowess of China. And no adversary has more power to compel those companies to do its bidding than the Chinese Communist Party.

Texas SB-2116 wisely precluded state agencies from awarding infrastructure contracts not just to China, but Russia, Iran, and North Korea as well. While the bill was drafted to preponderantly address contracts with Chinese companies, it has also had the effect of demonstrating a holistic commitment to keeping American adversaries away from state government contracts.

Policy Guidance: Include products from other foreign adversaries, not just China, in technology bans. While technologies from China are overwhelmingly the main problem, as Michael Cunningham of the Heritage Foundation has written, such efforts will “pre-emptively disprove allegations that laws are passed for any reason other than to keep states and communities safe.”¹⁴ Legislators should also be vigilant against Chinese lobbying efforts which attempt to persuade state legislators that China-focused actions “hurt the feelings of the Chinese people” – a common phrase Beijing employs to forestall action against the Chinese Communist Party's interest.¹

1 See, for example, the Wilson Center's analysis of this phrase. <https://www.wilsoncenter.org/blog-post/hurting-the-feelings-the-chinese-people>

BACKGROUND ON SELECT CHINESE TECHNOLOGY MANUFACTURERS

LENOVO: LAPTOPS, LIES, AND LARCENY

Lenovo is the world's largest manufacturer of personal computers, with headquarters in China and a U.S. headquarters in Morrisville, North Carolina. What has become Lenovo today was founded in China in 1984 by Chinese computer scientist Liu Chuanzi and ten of his colleagues from the Chinese Academy of Sciences (CAS). 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."¹⁵ But Legend Holdings, like all companies in China, is only nominally private. Legend Holdings lists the 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.¹⁶ 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,¹⁷ which has supplied voiceprint recognition technologies to the Xinjiang Bureau of Prisons.¹⁸

The Chinese Academy of Sciences is not the equivalent of entities like the National Academy of Sciences in the U.S. or the Royal Society in the UK. The U.S. government put the Chinese Academy of Sciences' computing division on its Entity List in December 2022, and with good reason. CAS is not a normal research institute producing knowledge for civilian application. According to the congressional U.S.-China Economic and Security Review Commission, CAS has "connections to Chinese military, nuclear, and cyberespionage programs."¹⁹ It supports and owns whole companies building technologies for the Chinese military such as hypersonic spaceplanes, robotic submarines, underwater platforms and missile technology.²⁰

Consistent with its strategy to acquire PC, server, and mobile communications divisions from major American corporations, Lenovo solidified its position as an international computer hardware leader in 2005 with the company's purchase of IBM's ThinkPad division. By 2022 Lenovo controlled roughly 16% of the U.S. PC market,²¹ and as recently as 2019 boasted of supplying more than 900 state and local governments.²² Relatively unknown in the global marketplace before the purchase, Lenovo found itself among major players in the technology sphere, relying on the brand and name recognition of its newly acquired ThinkPad product line to compete for government contracts. Shortly after the acquisition, the United States Department of State moved to purchase Lenovo laptops for employees. Congressman Frank Wolf, a critic of the IBM-Lenovo deal, quickly moved to ensure the State Department understood the risks associated with using the Chinese-made machines. Eventually, the State Department banned Lenovo systems from its classified network in 2006.²³

The Department of Defense also took 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.²⁴

“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 incident 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,²⁵ and it ditched Lenovo routers in 2016.²⁶

In 2019, the Department of Defense Office of the Inspector General released an audit regarding the purchase of Commercial Off-the-Shelf (COTS) items by employees and the security ramifications of those purchases. Referenced in that report was the purchasing of Lenovo laptops. The report, which called Lenovo products “known cybersecurity risks,” referenced the persisting vulnerabilities present in Chinese technology, including the well-known Superfish software that was pre-installed on Lenovo laptops sold in the United States in 2014. This software billed itself as a medium for advertisement targeting, but in reality served as an information aggregator to identify user trends, surveil user credentials, and funnel user data to data storage centers on the Chinese mainland.²⁷

LEXMARK: A BACKDOOR FOR MALIGN CYBER ACTIVITY

Though nominally an American company with headquarters in Lexington, Kentucky, Lexmark is 49% owned by a consortium of companies based in China, including Legend Holdings, the same Chinese state-financed company with a large stake in Lenovo.²⁸ Lexmark has long been the subject of various reports regarding cyber threats and espionage risk, with the printer company facing allegations from various technology experts and conglomerates that the company's printers could be used as a medium for cyber intrusion. Printers, one of the least secure Internet of Things devices, store sensitive data on internal hard drives derived from the various printing jobs executed on a day-to-day basis. This sensitive data can be accessed through various software vulnerabilities in the printer, making sensitive documentation visible to adversaries and foreign actors.

As they have done with Lenovo, various federal government agencies have moved to restrict Lexmark products from their enterprises. The Social Security Administration, determined to mitigate supply chain risks in procurement practices, won its argument in a federal court in 2018 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.²⁹ Some in the federal government clearly worried about Beijing's access to Americans' Social Security data, which U.S. states no doubt also have on record.

Lexmark's products were also labeled "known cybersecurity risks," in the 2019 DOD Inspector General report examining commercial off-the-shelf products, which found that the U.S. Army and Air Force had purchased 8,000 Lexmark printers. The Department of Defense Inspector General stated that Lexmark has "connections to Chinese military, nuclear, and cyberespionage programs." It continued:

The National Vulnerabilities Database lists 20 cybersecurity vulnerabilities for Lexmark, including storing and transmitting sensitive network access credentials in plain text and allowing the execution of malicious code on the printer. These vulnerabilities could allow remote attackers to use a connected Lexmark printer to conduct cyberespionage or launch a denial of service attack on a DoD network."³⁰

Inexplicably, when it comes to Lexmark, the federal government suffers from the same incoherence that state governments do. The U.S. government's General Services Administration has recognized Lexmark as a "process and content management solution provider for federal agencies."³¹ This signals to both federal and state agencies that Lexmark is a perfectly fine supplier – even though other parts of the federal government have raised a red flag!

"You can have the best cyber program in your company and you can hire a private cybersecurity firm who has the best software, but if your procurement and acquisition folks are not part of the team, you will fail...Our adversaries, that's how they get us, through procurement and acquisition programs.



– Bill Evanina, former director of the National Counterintelligence and Security Center (NCSC) in the Office of the Director of National Intelligence

HIKVISION: A DE FACTO CHINESE GOVERNMENT SPY AGENCY

Hikvision, a manufacturer of surveillance equipment, is a subsidiary of the Chinese state-owned China Electronics Technology Group Corporation. The Commerce Department wisely added Hikvision to the Entity List in 2019 for complicity in the genocide (the legal term the U.S. government has applied) the Chinese Communist Party has perpetrated against Uyghur Muslims in Xinjiang, China. The FCC has also added Hikvision to its covered list, meaning Hikvision products are prohibited from accessing the American radio frequency spectrum. The Pentagon has also banned Hikvision from its systems. In 2019, the federal government was banned from purchasing Hikvision products, and the Treasury Department was reported to be considering high-level economic sanctions on the company in 2022.³²

These designations have been made for good reason. In April, surveillance industry trade publication IPVM published a video entitled "Hikvision Cameras in My Concentration Camp Cell." In it, a former concentration camp prisoner named Ovalbek Turdakun described how a Hikvision camera watched over him and 22 other prisoners held in a cramped cell, with devices even positioned over the toilet. When IPVM showed him the Hikvision logo, he instantly said "it is the same logo [of the cameras] which is in the cell."³³

The atrocities in Western China conducted with the aid of Hikvision products aren't the only reason the company remains dangerous. Last year, IPVM documented Hikvision's "top supplier status" for

the Chinese military and role in “collaborating on PLA (People’s Liberation Army) research.” The Wall Street Journal picked up on the IPVM report, writing:

“According to public documents and online materials found by IPVM, Hikvision sold drones and other accessory equipment to the Chinese air force in 2019 and was considered a top-tier supplier to the nation’s military in 2014...Hikvision’s website also carried a report on how the company’s technology could improve the performance of Chinese missile, tank and other weapons systems, citing a study done jointly with commanders and weapons experts from the People’s Liberation Army. The study proposed the use of Hikvision cameras to record drills and improve weapons accuracy.”³⁴

Yet the United States’ actions to restrict Hikvision products amounts to playing catch-up. Hikvision had already captured 12% of the North American surveillance camera market by 2017, including 750,000 devices in the U.S., and even has even managed to place products in U.S. military bases and diplomatic facilities.³⁵ A more recent estimate by the Massachusetts Institute of Technology Review puts the number of Hikvision cameras in the U.S. at 600,000.³⁶ It often gains penetration through a U.S. subsidiary, EZVIZ, whose products Best Buy and Home Depot only stopped carrying in 2021.

Sadly, U.S. law enforcement agencies have been eager buyers of Hikvision equipment. Police departments throughout U.S. states, including those in Massachusetts, Colorado, and Tennessee, have used Hikvision products extensively. Shockingly, the city of Memphis, Tennessee received a “Homeland Security Award” from Government Security News in 2016 for deploying 600 Hikvision cameras as crime-fighting tools.³⁷ IPVM has documented multiple school districts spending hundreds of thousands of dollars on Hikvision products,³⁸ and two public school districts in Arkansas have also each spent more than \$1 million dollars on them.³⁹ These are just microcosms of Hikvision’s reach across the United States at the state level, despite a federal government acquisition ban.

“No company from the People’s Republic of China is truly ‘independent.’ So, when these American entities buy this equipment, they should know that not only are they supporting companies facilitating repression in China, but that the data gathered via this surveillance gear can be shared with the Chinese Communist Party... We need to educate Americans, including local government entities, on the risks of buying this type of equipment and its moral and security implications.”



– Senator Mark Warner (D-Virginia)

DJI: UNDERMINING AND MANIPULATING U.S. LAW ENFORCEMENT

Founded in 2006 Chinese drone manufacturer Da Jiang Innovations, or DJI for short, has quickly become a behemoth, controlling approximately 54% of the global drone market as of 2021,⁴⁰ and 77% of the hobby drone market as of 2020.⁴¹ While not state-owned, it has taken investment funds from China Chengtong Holdings Group, which is directly administered by Beijing’s State-owned Assets Supervision and Administration Commission (SASAC).⁴² Its dominance in the commercial drone space has helped lead many of America’s police and fire departments to turn to DJI as their supplier of

choice. In 2020, The Wire China reported that more than 900 U.S. state and local governments and emergency services used DJI products.⁴³ Just as Huawei, state-backed chipmaker YMTC, and Lenovo have done in their respective industries, DJI prices its products far below its competitors' in hopes of driving its rivals from the space. DJI has also helped carry out in the acts of genocide the Chinese Communist Party is perpetrating in Xinjiang by providing equipment to the Xinjiang Public Security Bureau, thus landing the company on the Commerce Department's blacklist in 2021.⁴⁴

The federal government knows DJI is dangerous. In 2021 the Department of Homeland Security warned that DJI is "a national security threat," and assessed with "moderate confidence" that it was "providing U.S. critical infrastructure and law enforcement data to the Chinese government."⁴⁵ The U.S. Bureau of Customs and Immigration enforcement also issued a warning in 2017 assessing with high confidence that "the critical infrastructure and law enforcement entities using DJI systems are collecting sensitive intelligence that the Chinese government could use to conduct physical or cyber attacks against the United States and its population."⁴⁶ In 2018, the Department of Defense banned the purchase of all off-the-shelf drone technology, and in 2021 stated that "systems produced by Da Jiang Innovations (DJI) pose potential threats to national security."⁴⁷

Despite these clear threats, state governments continue to purchase DJI drones in mass quantities (as have the Secret Service and the FBI, reports Axios).⁴⁸ As of August 2021, 90% of U.S. public safety organizations using drones used a DJI-built product,⁴⁹ with the New York Police Department just one law enforcement agency to rely on them.⁵⁰ DJI and its lobbyists have co-opted the Law Enforcement Drone Association advocacy group to defend its interests in Washington, often flying in local law enforcement officials from across the nation to beg Congress to stay away from banning DJI (and what politician wants to cross the nation's sheriffs and commissioners?). Writes national security expert Klon Kitchen, "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."⁵¹ Local law enforcement officers must be wary that they do not become pawns in the Chinese Communist Party's game.

"This is the latest example of how the CCP uses the swamp against us...There is bipartisan recognition that Congress needs to act to mitigate threats posed by DJI drones, but these efforts have been undermined by lobbyists who'd rather sell out the country than lose a lucrative contract."



- Rep. Mike Gallagher (R-Wisconsin),
Chair of the House Select Committee on China

APPENDIX A: NASPO-AUTHORIZED LENOVO RESELLERS⁵²

STATE:	QUALIFIED NASPO VALUEPOINT RESELLERS AS OF 3/22/2021
Alaska	CDWG
Arizona	CDWG, SHI, Better Direct, QCM Technology, Riverside Technologies (RTI), Insight, Key Information Systems, All Covered, DHE
Arkansas	CDWG, GovConnection, SHI, Next Step, Complete Computing
California	CDW Government LLC; Datel Systems Incorporated; Omnipro Systems, Inc.; PC Specialists, Inc. (dba Technology Integration Group); Broadway Typewriter Company, Inc. (dba Arey Jones) ; Insight Public Sector, Inc.; Golden Star Technology Inc.; FireFly Computers LLC; Enterprise Networking Solutions, Inc.; ConvergeOne, Inc.
Colorado	CDWG, DHE, Y&S Technology, Nelowet, Insight, Woodard Technologies (dba TwoTrees)
Delaware	SHI
Devereux Foundation	CDWG
Florida	CDWG, SHI, GovConnection, PCMG, Broadway Typewriter Company aka Arey Jones, UDT, All Covered, Insight, PC Solutions, ProLogic ITS, WWT
Hawaii	CDWG
Idaho	CompuNet, ConvergeOne, CDWG, Ednetics Inc., Core Technologies, Sterling Computer Corporations
Iowa	EmbarqIT, CDWG
Kansas	CDWG, Woodard Technologies (dba TwoTrees), SHI
Kentucky	CDWG

STATE:	QUALIFIED NASPO VALUEPOINT RESELLERS AS OF 3/22/2021
Louisiana	CDWG, CMA, SHI, Kynetic Technology, Woodard Technologies (dba TwoTrees), GovConnection, Firefly, Broadway Typewriter Company, Inc. (dba Arey Jones), General Informatics, LATG, Trinity3 Technology
Maine	CDWG, GovConnection, SHI
Minnesota	CDWG, Firefly, TSG
Montana	CDWG
New Jersey	CDWG, GovConnection, Vcom, SpinCube, SHI, TechXtend, Palisades, CSAM, Micro Strategies, Insight, MTG IT Professionals
New Mexico	CDWG, SHI, QCM, Riverside Technologies (RTI), Abba Technologies, Inc., PC Specialists, Inc. (dba Technology Integration Group), Education Technologies, Inc.
Oklahoma	Woodard Technologies (dba TwoTrees), Trinity3 Technology
South Carolina	CDWG, A3 Communications, SHI, Alphanumeric, BridgeTek Solutions, Data Network Solution, Pinnacle, Virtucom, FireFly, Trinity3 Technology
Tennessee	CDWG, SHI, GovConnection, Insight, Unistar Sparco
Utah	CDWG, SHI, Summit Partner, DHE, Trinity3 Technology, Firefly
Washington	CDWG, ConvergeOne, GovConnection, Micro K-12, Ovation Technology, Trinity3 Technology, Firefly, Jones & Associates
Wisconsin	Insight, Vanguard, BusinessIT Source
Wyoming	SHI

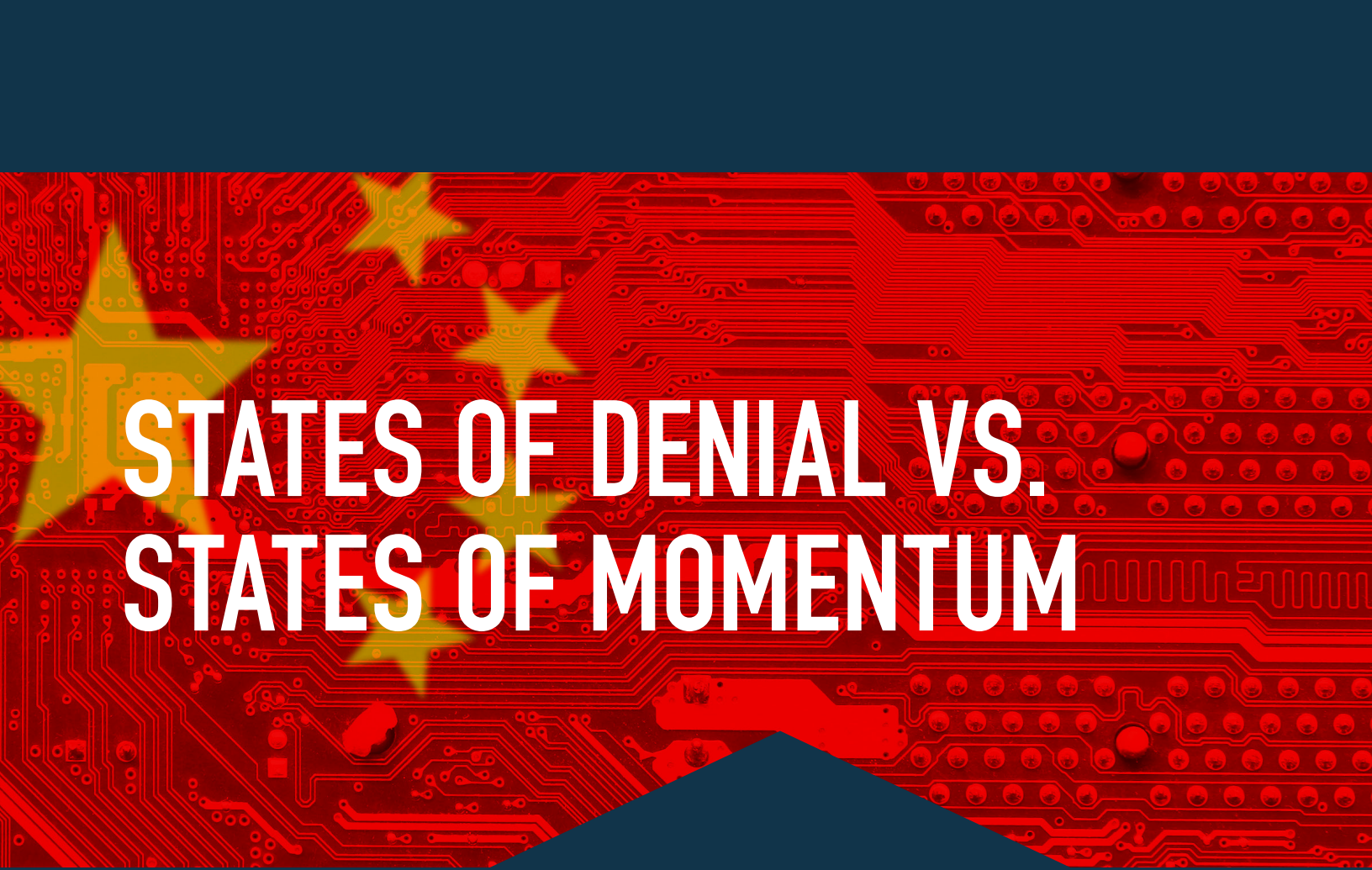
APPENDIX B: NASPO-AUTHORIZED LEXMARK RESELLERS

STATE:	STATE CONTRACT #	QUALIFIED NASPO VALUEPOINT RESELLERS AS OF 3/22/2021	STATE:	STATE CONTRACT #	QUALIFIED NASPO VALUEPOINT RESELLERS AS OF 3/22/2021
California	140601	GovConnection, Inc., Granite Data Solutions, Zones, LLC, JJR Enterprises Inc. dba Caltronics Business Systems, PRA International, Pacific Office Automation, Fruth Group, John Galt Inc. dba Duplicated Business Systems, Harris Technologies, Inc.	Louisiana	406370	Allfax Specialties, Inc., Automated Imaging Systems, Inc., C.F. Biggs Company, Inc., CDW Government, Inc., Classic Business Product, Dempsey Business Systems of LA, Emco Technologies, Staples Technology Solutions, WJS Enterprises, Inc.
Colorado	140601	GovConnection, Inc., Nelowet Business Machines, LTD, Pacific Office Automation, Zones, LLC, Harris Technologies, Inc., Frontier Business Products	Missouri	140601	Harris Technologies, Inc., SHI International Corp
Connecticut	140601	American Copy Service Center		CT202797005	Lakeland Office Supplies, Macro Technologies LLC, Harris Technologies, Inc.
Florida	140601	BLM Technologies of Florida LLC dba EvolvTec, Zones, LLC, RJ Young, GovConnection, Inc., Dove Print Solutions, Inc., Harris Technologies, Inc., SHI International Corp	Nevada	140601	GovConnection, Inc., High Sierra Business Systems Inc., Zones, LLC, SHI International Corp,
Hawaii	140601	Zones, LLC, Trafera, LLC, Harris Technologies, Inc., SHI International Corp,	New Mexico	140601	GovConnection, Inc., Harris Technologies, Inc., Sparks Office Solutions, Pacific Office Automation
Idaho	PADD1054	Allied Business Solutions	Oklahoma	B27169	Fuzzell's Business Equipment, RK Black Inc.
Iowa	140601	Marco Technologies LLC, M&M Sales Company D.B.A. MMIT, Gordon Flesch Company	Rhode Island	140601	Automated Business Solutions Inc., GovConnection, Inc.
Kansas	12520	CDW Government, Inc., Century United Companies, Inc, PCMG, Inc, World Wide Technology, Inc.	South Dakota	140601	Harris Technologies, Inc., SHI International Corp
Kentucky	140601	American Business Systems Inc., Prosource, Duplicator Sales and Service, Electronic Business Macines, Inc., GovConnection, Inc., RJ Young, Trafera, LLC, SHI International Corp	Utah	140601	PCF, Inc., Zones, LLC, GovConnection, Inc., Pacific Office Automation, Harris Technologies, Inc., SHI International Corp
			Vermont	140601	GovConnection, Inc.
				B27169	CDW Government, Inc.
			Wisconsin	15-20400-905	CDW Government, Inc., Corporate Business Systems, Gordon Flesch Company

ENDNOTES

- 1 <https://apnews.com/article/technology-business-china-united-states-hacking-ffa2120239eb687ce1979bf9599dfea5>
- 2 <https://www.youtube.com/watch?v=9rN00wC3oCE>
- 3 <https://www.cnbc.com/2019/03/05/huawei-would-have-to-give-data-to-china-government-if-asked-experts.html>
- 4 <https://cset.georgetown.edu/wp-content/uploads/CSET-Banned-in-D.C.-1.pdf>
- 5 <https://alec.org/model-policy/an-act-to-prohibit-state-contracts-with-chinese-government-owned-or-affiliated-technology-manufacturers/>
- 6 <https://legiscan.com/GA/bill/SB346/2021>
- 7 <https://lis.virginia.gov/cgi-bin/legp604.exe?231+ful+HB2385EH2>
- 8 <https://chinatechthreat.com/cfius>
- 9 <https://spacenews.com/u-s-military-doubles-down-on-gps-despite-vulnerabilities/>
- 10 https://www.heritage.org/sites/default/files/2022-07/SR259_0.pdf
- 11 <https://legiscan.com/GA/text/SB346/2021>
- 12 <https://www.axios.com/2022/01/18/lawmakers-katko-garbarino-warn-states-chinese-tech>
- 13 <https://www.fbi.gov/news/speeches/the-threat-posed-by-the-chinese-government-and-the-chinese-communist-party-to-the-economic-and-national-security-of-the-united-states>
- 14 https://www.heritage.org/sites/default/files/2022-07/SR259_0.pdf
- 15 http://www.legendholdings.com.cn/Introduction_en/index.aspx?nodeid=1043
- 16 <http://ir.legendholdings.com.cn/media/1192/2022-interim-report-e.pdf>
- 17 https://www.uscc.gov/sites/default/files/2021-03/March_19_2021_Hearing_Transcript.pdf
- 18 <https://www.reuters.com/article/us-china-xinjiang-mit-tech-insight/risky-partner-top-u-s-universities-took-funds-from-chinese-firm-tied-to-xinjiang-security-idUSKCN1TE04M>
- 19 https://www.uscc.gov/sites/default/files/Research/Interos_Supply%20Chain%20Vulnerabilities%20from%20China%20in%20U.S.%20Federal%20ICT_final.pdf
- 20 <https://www.thebulwark.com/the-chinese-threat-thats-hiding-in-plain-sight/>
- 21 <https://www.gartner.com/en/newsroom/press-releases/2022-10-10-gartner-says-worldwide-pc-shipments-declined-19-percent-in-third-quarter-of-2022>
- 22 <https://www.thebulwark.com/the-chinese-threat-thats-hiding-in-plain-sight/>
- 23 <https://www.nytimes.com/2006/05/23/washington/23lenovo.html>
- 24 <https://www.bloomberg.com/features/2021-supermicro/?leadSource=uverify%20wall>
- 25 <https://spacenews.com/u-s-military-doubles-down-on-gps-despite-vulnerabilities/>
- 26 https://www.washingtonpost.com/business/economy/how-an-email-sparked-a-squabble-over-chinese-owned-lenovos-role-at-pentagon/2016/04/22/b1cd43d8-07ca-11e6-a12f-ea5aed7958dc_story.html
- 27 <https://www.aei.org/technology-and-innovation/new-pentagon-reports-shows-how-restricted-chinese-it-products-routinely-make-their-way-into-us-military-networks/>
- 28 <https://chinatechthreat.com/wp-content/uploads/2020/02/CTT-Report-Stealing-From-States-Chinas-Power-Play-in-IT-Contracts.pdf>
- 29 <https://federalnewsnetwork.com/reporters-notebook-jason-miller/2018/05/ssa-bid-protest-win-demonstrates-power-of-acquisition-to-protect-the-supply-chains/>
- 30 <https://www.aei.org/technology-and-innovation/new-pentagon-reports-shows-how-restricted-chinese-it-products-routinely-make-their-way-into-us-military-networks/>
- 31 https://www.lexmark.com/en_us/solutions/government/accessibility-gsa-schedules.html
- 32 <https://www.reuters.com/technology/us-plans-impose-sanctions-chinas-hikvision-ft-2022-05-04/>
- 33 <https://ipvm.com/reports/hikvision-cell>
- 34 <https://www.wsj.com/amp/articles/chinese-surveillance-gear-maker-hikvision-has-ties-to-countrys-military-report-says-11621941983>
- 35 <https://www.theatlantic.com/ideas/archive/2021/10/china-america-surveillance-hikvision/620404/>
- 36 <https://www.technologyreview.com/2022/06/22/1054586/hikvision-worlds-biggest-surveillance-company/>
- 37 <https://www.newswire.ca/news-releases/hikvision-video-surveillance-solution-wins-homeland-security-award-for-memphis-police-department-569256351.html>
- 38 <https://ipvm.com/reports/hik-faye>

- 39 <https://www.axios.com/2022/10/26/governments-chinese-telecom-bans>
- 40 <https://www.reuters.com/markets/asia/dji-is-more-elusive-us-target-than-huawei-2021-12-17/>
- 41 <https://www.washingtonpost.com/national-security/2022/02/01/china-funding-drones-dji-us-regulators/>
- 42 Ibid.
- 43 <https://www.thewirechina.com/2020/10/04/are-chinese-drones-national-security-threat-or-require-for-national-interest/>
- 44 <https://www.theverge.com/2021/12/16/22839970/dji-chinese-military-industrial-complex-investment-blacklist>
- 45 <https://www.axios.com/2021/09/22/federal-law-enforcement-china-drone>
- 46 <https://info.publicintelligence.net/ICE-DJI-China.pdf>
- 47 <https://www.defense.gov/News/Releases/Release/Article/2706082/department-statement-on-dji-systems/>
- 48 <https://www.axios.com/2021/09/22/federal-law-enforcement-china-drone>
- 49 <https://www.droneresponders.org/post/dji-domination-of-public-safety-drone-sector-continues-as-autel-robotics-surges-to-second-position>
- 50 <https://theintercept.com/2021/10/12/nypd-chinese-drones-surveillance/>
- 51 <https://www.aei.org/articles/red-china-backs-the-blue/>
- 52 <https://imlive.s3.amazonaws.com/Idaho/ID301139842186554984703624925615599126585/Lenovo-Reseller-List-5-26-22.pdf>



STATES OF DENIAL VS. STATES OF MOMENTUM

DANGEROUS CHINESE TECHNOLOGY
IN U.S. STATE GOVERNMENT
SYSTEMS AND RISING EFFORTS TO
PROHIBIT CONTRACTS SUPPLYING IT



www.chinatechthreat.com

James Marks
China Tech Threat
LD 877

Over the course of my military career, I have served our country in a variety of roles, including as a senior intelligence officer during Operation Iraqi Freedom in 2003 and as Commanding General of the U.S. Army Intelligence School in Fort Huachuca, Arizona. Early in my Army intelligence career, I served as a foreign area officer in Asia where I was privileged to be able to study Chinese affairs alongside an outstanding group of civilian and military analysts.

Drawing on my decades of observing China's behavior, I also have the opportunity to serve as the principal of China Tech Threat, an organization that studies the problems of technology produced by the People's Republic of China and offer policy solutions to protect America's security and prosperity.

It is through this role that I submit this testimony in support of LD 877, An Act to Prohibit State Contracts with Companies Owned or Operated by the Government of the People's Republic of China. Consideration of this bill could not come at a more important time as we learn about China's threat, strategies and intentions highlighted by Chinese President Xi Jinping's meeting with Vladimir Putin this week to discuss their shared goals.

I am submitting this testimony to reinforce that China is a threat to America's economic and national security not just at the federal level but importantly at the state and local level as well. We remain vulnerable to Chinese influence operations at all levels of governance.

Just last month, China Tech Threat released a report analyzing state use of technology manufactured by Chinese owned or operated companies that have already been banned or restricted at the federal level. Our research revealed that 28 states have cumulatively bought a total of at least \$230 million worth of dangerous equipment since 2015, with individual states spending up to \$47 million. The State of Maine has spent \$5,350,803 on restricted Chinese technology from Lenovo, Inc. These purchases were made by the Bureau of Information Services, but the technology has likely been distributed throughout state agencies.

This means that technology manufactured by Lexmark or Lenovo, which has been banned by the Department of Defense, U.S. Intelligence agencies and others due to their connections to the Chinese military, is still being plugged into Maine's state networks.

It is important to specify that unlike other states, Maine does not disclose where purchased technology is being used. For example, we know that Delaware Department of Elections, the Hawaii Department of Taxation, and the South Dakota Department of Emergency Management are just a few state government entities to have purchased these products. That same level transparency does not exist in Maine. Our February report was released as an update to the original 2019 report on state spending, where China Tech Threat was also unable to obtain state procurement and purchase information from Maine officials despite multiple attempts. I provide this background because it is important that Maine's leaders fully recognize their potential risks and vulnerabilities.

The fact that Chinese-owned and operated Lenovo technology is being purchased by the state of Maine is so alarming because China's 2017 National Intelligence law mandates information sharing between "private" businesses and intelligence agencies, even for Chinese businesses operating in other countries, like Lenovo.

Fortunately, there is momentum building across in the states to combat this threat. With this bill, State Senator Lisa Keim is establishing Maine as an early leader, along with nearly a dozen other states who are also considering bills to prohibit contracts with this dangerous technology.

Over the course of my career in the U.S. military, U.S. military planners went from assessing China as a second-tier challenge to a "pacing" threat today. The Chinese Communist Party is using all elements of national power – diplomacy, economics, military development, information flows, and technology – to undermine American security, prosperity, and freedom.

China Tech Threat certainly recognizes that states don't have the same resources or

bench of staff expertise to analyze and track these types of technology threats. We hope our research and analysis can serve as a resource to help state leaders assess their vulnerabilities and what they can do to better protect residents, businesses, infrastructure and the vast amounts of sensitive data housed within government agencies. If there is a single weak point in our national cyber defenses especially at the state and local levels, China will find and exploit it. We are all vulnerable to Chinese influence operations.

With this testimony, I am also uploading a copy of the China Tech Threat report I referenced above.

Thank you for attention to this important issue.
U.S. Army General (Retired) James Marks