Lisa M. Keim
Senator, District 19
Assistant Republican Leader

THE MAINE SENATE
131st Legislature

3 State House Station
Augusta, Maine 04333

Testimony of Senator Lisa Keim before the Joint Standing Committee on State and Local Government

LD 877, An Act to Prohibit State Contracts with Companies Owned or Operated by the Government of the People's Republic of China

March 21, 2023

Good Afternoon Senator Nangle, Representative Stover and honorable members of the Joint Standing Committee on State and Local Government. I am Lisa Keim, and I proudly represent the citizens of Senate District 19, which includes much of Northern Oxford County and 15 communities in Franklin County. I am proud to sponsor LD 877, "An Act to Prohibit State Contracts with Companies Owned or Operated by the Government of the People's Republic of China."

The People's Republic of China has always been a threat to national security, but there is renewed public interest in protecting against their interference. Federal policy directs information security at the federal level, and states must also determine their own security standards.

Making headlines through Huawei, ZTE in 5G networks, and TikTok, China is well known for collecting massive amount of information on US Citizens, and for stealing intellectual property, but they are also targeting our Government at every level, Federal, State and Local.

China's 2017 National Intelligence Law mandates Chinese government access to information collected by equipment that is produced by Chinese-owned companies, and the disclosure of that data to the Chinese Communist Party (CCP) upon request. 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. Chinese companies have no choice- they must provide an information pipeline for the CCP.

Recognizing part of the risk, as of February 2023, MaineIT banned the social networking service TikTok from all state-issued or Bring Your Own Device (BYOD) mobile devices connected to state equipment and systems. The Directive states that Maine must keep pace with rapidly evolving national security risks to infrastructure, "including the sensitive and confidential information that we are entrusted to protect for our citizens."[i]

However, if Chinese technology is being used anywhere in our state government, the CCP has access to our private information upon request. Maine is vulnerable in at least in one known way: Lenovo laptops which are used throughout State Government.

According to Maine Open CheckBook, between 2015 and 2023, the state of Maine spent $5,350,803 on Chinese technology from Lenovo, Inc. In fact, the computers currently used by Legislative staff are Lenovo. This is extremely concerning because through Lenovo, depending on which state agencies are using these PCs, the CCP can access personal information held by courts, police departments, elections

departments, education departments, children and family services, or other social service providers and agencies.

Unlike other states, Maine does not disclose where purchased technology is being used. While it is unclear which specific agencies are using Lenovo technology, it is clear is that sensitive and confidential information held by certain government offices and agencies has been made vulnerable to Chinese intrusion through this dangerous technology, which is already restricted by U.S. military and intelligence agencies due to its connection to the Chinese government and military.

In March of 2022, American cybersecurity firm Mandiant reported that at least six state governments had been hacked by a group linked to the Chinese government called APT41. Additionally, in 2020 the Justice Department indicted five members of this group for hacking more than 100 U.S. companies.

Some states have already taken steps to protect their data. With this measure, Maine could join the wave of 11 states taking action to ban the purchase and deployment of Chinese technology by state agencies. Among these are Georgia Senate Bill 346 and Florida Executive Order 22-216 which have banned Chinese information and communications technology systems from state government contracts. In fact, the sponsor of the Georgia bill has agreed to testify by zoom today.

Maine is vulnerable to intrusion. The disturbing fact we must face is that our greatest foreign adversary- Communist China- controls large technology companies whose devices are used throughout our state government.

Others much more knowledgeable about this topic will be speaking after me today. I urge this committee to listen to their testimony; they are taking their time to join us because they care to protect our nation. This is not a partisan issue.

We are already years behind in addressing this reality. The CCP passed their Internet Security Law, as no secret, in 2017. It is past time for us to take action. The duty to be vigilant and pass protective measures for the good of Maine people is ours.

I'll end with a quote from John Demers, Assistant Attorney General for National Security, "The threat from China is real, it's persistent, it's well-orchestrated, it's well-resourced, and it's not going away anytime soon."[ii]

Going forward, it is time to make different decisions with our state's technology purchases and stop the hemorrhaging of information to the CCP.

---

[i] STATE OF MAINE DEPARTMENT OF ADMINISTRATIVE AND FINANCIAL SERVICES MAINE OFFICE OF INFORMATION TECHNOLOGY (MaineIT) , https://htv-prod-media.s3.amazonaws.com/files/cybersecurity-directive-23-01-tiktok-002-v2-002-1674166182.pdf.

[ii] Cimpanu, Catalin. "FBI Is Investigating More than 1,000 Cases of Chinese Theft of US Technology." *ZDNET*, ZDNEY, 8 Feb. 2020, https://www.zdnet.com/article/fbi-is-investigating-more-than-1000-cases-of-chinese-theft-of-us-technology/.

Q1: Why does this bill single out China alone?
A1: The disturbing fact is, no other foreign adversary controls large tech companies that hold such significant market share to support their global ambitions. China's 2017 Internet Security Law gives the Chinese government access to information collected by equipment provided by Chinese-owned companies and the disclosure of that data to the Chinese Communist Party upon request. If vulnerable technology is being used anywhere by a state, this could mean the Chinese government could have access to information. To be clear, this bill does not apply to private companies. Private American companies should not be punished or penalized for making risky purchases unknowingly when these government-affiliated Chinese companies have created quite an ownership labyrinth to disguise their government connections.

Q2: What will it cost taxpayers to enact this legislation.
A2: There are negligible administrative costs associated with reviewing certifications and this cost could be offset by fines issued when the state's purchasing agency determines that a company has submitted a false certification. However, such protections help support business growth and attract new businesses to states that know their security concerns are being addressed.

Q3: How should we address the millions Maine has already spent on Lenovo products which would cost a lot to replace?
A3: The main purpose of this bill is to stop any new purchases of this risky China-owned technology. Yes, Maine has already spent money on this risky tech and "rip and replace" comes at a cost to taxpayers. Unfortunately, that technology already in use will need to be addressed, but that should not be a factor to slow down passage of this bill. If anything, it is a reason to pass it swiftly.

Q4: Does this bill apply to private companies?
A4: No. Private American companies should not be penalized for unknowingly purchasing equipment from government-affiliated Chinese companies, as they are frequently disguised by American subsidiaries.

Q5: What defense & intelligence agencies have banned the kinds of companies that will be restricted by this legislation?
A5: In July 2019 the Department of Defense Inspector General highlighted some $33 million in purchases by the Pentagon of commercial off the shelf (COTS) Lexmark and Lenovo products, which have been noted on the National Vulnerability Database because of security deficiencies. Like Huawei and ZTE, Lexmark and Lenovo are Chinese-owned and banned by multiple military and intelligence agencies in the U.S. and around the globe.

Q6: If these products have been banned by defense & intelligence agencies, why are states, local governments, & schools still buying them?
A6: While federal policy directs information security for federal agencies, states determine their own information security standards. There is no central state/local vetting agency, so states & local governments just don't have the expertise and know the risk. Furthermore, the National Association of State Procurement Officers (NASPO), which is regarded as the "gate keeper" for state government purchasing across the United States, does not account for security vulnerabilities.

Q7: Should this bill be limited to China, or should it also apply to other countries, like Russia, for example?
A7: This bill builds off of identified threats and restrictions that already exist at the federal level to bolster our defense again a country that has national laws created to take advantage of backdoor access to sensitive American data. That doesn't mean to say we shouldn't take a close look at how it could be applied to other adversarial nations, but that consideration should not slow our efforts already underway to hold of China right now.