MEMO

China TECH THREAT

TO: STATE POLICYMAKERS

DATE: MAY 19, 2022

FR: ROSLYN LAYTON, PHD; CO-FOUNDER

RE: **FOUR STATE POLICY IDEAS TO COUNTER CHINA'S TECH THREATS**

In March, the *Associated Press* reported that "hackers working on behalf of the Chinese government broke into the computer networks of at least six state governments in the United States in the last year." The report did not identify which states were targeted.

Subsequently, cybersecurity expert Joseph Steinberg warned: "If we know that six states were breached by Chinese spies, 44 states probably have Chinese spies operating on their networks that we don't know about."

While federal policy constrains malicious products for federal agencies, these restrictions are not automatically adopted at the state level. For example, a 2019 Pentagon report warned against using Lenovo and Lexmark products, but a review by China Tech Threat revealed that 40 states continue to use this equipment.

In a speech earlier this year, FBI Director Chris Wray cited more than 2,000 investigations focused on the Chinese government trying to steal our information or technology and stated "there is just no country that presents a broader threat to our ideas, our innovation, and our economic security than China."

Finally, some states are heeding these warnings. Several governors and state policymakers are taking action to protect the security and integrity of government agencies, infrastructure, financial institutions and the personal data of residents. Below are four policy ideas for state governments to reduce tech threats from China:

#1. Restrict Chinese Government Owned Companies from State Contracts

Exemplary Action: Georgia Governor Brian Kemp signed SB 346 in May 2022

Policy Guidance: State policymakers should prohibit Chinese Government owned or operated companies from providing tech products to state governments, universities and local school districts. In a recent interview, SB 346 sponsor Rep. Martin Momtahan said, "we have a $31 billion budget, we're buying computers, we're buying technology, but there is no state-side regulation on the purchasing of these kinds of devices." Instead, Rep. Momtahan suggested that states "recognize that the Department of Defense, and other national security departments within the federal government have already adopted" the bans.

#2. Restrict University Partnerships that Arm the Chinese Military

Exemplary Action: Florida Governor Ron DeSantis signed HB 7017 in June 2021. The law prohibits specific agreements between state/public entities and China along with six other countries of concern, and strengthens disclosure of foreign support for public entities and postsecondary institutions.

Policy Guidance: Implementing US technology and expertise gained from US universities has enabled China's military to meet or even exceed the US military in many areas. State policymakers should restrict partnerships with Chinese universities that support China's civil-military fusion strategy. In order to combat such illicit alliances, Senator Marco Rubio sent letters to 22 U.S. universities in 17 states urging them to terminate their partnerships with Chinese universities because they "support the development of Chinese military technologies."

#3. Growing and Strengthening the Cybersecurity Workforce

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 May 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.

#4. Cooperation Between Congress and States to Ensure Federal Agencies Enforce Export Control Laws

Exemplary Action Needed: In January 2022, two New York Members of Congress issued a letter asking the Homeland Security and Commerce Department to "support States to ensure they are not unwittingly procuring products that will create vulnerabilities at the State level." Governors could exert similar pressure.

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 known Chinese military end users like Yangtzee Memory Technologies Corporation (YMTC), Hua Hong Semiconductor and ChangXin Memory Technologies (CXMT) to be added to the Department of Commerce Entity List.