

House Permanent Select Committee on Intelligence

July 15, 2026

How to Empower States to be the Front Line of American Homeland Defense for the hearing to examine how states are on the frontlines of combatting the counterintelligence threats facing the United States.

Testimony by **Michael Lucci**

Founder and CEO, State Armor

Chairman Crawford, Ranking Member Himes, and Members of the House Permanent Select Committee on Intelligence, thank you for the opportunity to testify today. My name is Michael Lucci. I am the founder and CEO of State Armor. Our mission is to win the American homeland by working state-by-state to protect critical infrastructure, protect state government supply chains, and counter malicious foreign influence operations.

I will focus on three points to describe the counterintelligence challenge we face from the Chinese Communist Party, and the opportunity to enhance our national security through enhanced federal-state partnerships.

1. First, America's open society and federalist system allows for strategic gaps in our counterintelligence efforts.
2. Second, the evidence of CCP-affiliated infiltration at the subnational level, including entities pre-positioning near critical infrastructure and military bases and infiltrating state institutions, provide a cause for alarm and concerted action.
3. Third, the 50 American states can and should be transformed into a strategic asset for countering broad societal infiltration. The federal government should view the states as the first lines of defense against CCP intelligence, as powerful force multipliers of federal efforts, and as laboratories for homeland security experimentation.

Strategic gaps in the American governance system

America is a massive continental power, an open society, and we operate on a federalist government system. Meanwhile, China takes a broad approach to infiltrating American society, which includes elite capture of leaders at the state and local government level. Therefore, even if Washington, D.C. functioned perfectly on all its counterintelligence objectives, America would

still be best served if leaders at the subnational level operate as the first layer of defense against the CCP's broad attempts at societal infiltration. States have manpower and localized knowledge to amplify federal efforts and to furthermore develop novel security solutions.

State Armor works with governors, attorneys general, state legislatures, law enforcement, and other agencies of jurisdiction to counter CCP subnational influence operations. We built State Armor after a series of federal warnings to states that have accelerated since our 2023 founding. A few examples of the significant warnings include:

1. Jamestown Foundation's 2019 warning on China's economic outreach to states via united front entities to undermine changes in U.S. trade policy.¹
2. Secretary of State Mike Pompeo's 2020 warning at the National Governors Association that China is targeting all 50 governors' offices.²
3. President Biden's 2022 warning on the need to protect subnational governments from PRC influence operations.³
4. President Biden's 2024 warning to all 50 governors on disabling cyberattacks striking water and wastewater systems.⁴
5. President Trump's 2025 executive order declaring it the policy of the United States for state and local governments to play a more active and significant role in national resilience and preparedness.⁵
6. The New York Times' 2025 report on how China influences elections in New York City, noting how the Chinese consulate and 53 non-profits mobilize community groups to defeat candidates that don't align with the CCP.⁶
7. And finally, Jamestown Foundation's 2026 report on the nearly 1,000 U.S.-based organizations amplifying the CCP's 'united front' influence activities across the country.

These warnings provide essential information. States would additionally benefit from regular updates on these warnings. Currently, many federal warnings come to state policymakers in an ad hoc manner. Regular updates would allow for broader distribution and absorption at the state level. In addition, if federal leaders outlined and even endorsed baseline solutions for states to consider, that would help clarify strategic options. President Biden's 2022 memo and President Trump's 2025 executive order sketch some solutions. Other solutions can be as simple as enacting a state version of what you all in the federal government have already done, such as

¹ <https://jamestown.org/china-explores-economic-outreach-to-u-s-states-via-united-front-entities/>

² <https://2017-2021.state.gov/u-s-states-and-the-china-competition/>

³ https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/PRC_Subnational_Influence-06-July-2022.pdf

⁴ https://www.epa.gov/system/files/documents/2024-03/epa-apnsa-letter-to-governors_03182024.pdf

⁵ <https://www.whitehouse.gov/presidential-actions/2025/03/achieving-efficiency-through-state-and-local-preparedness/>

⁶ <https://www.nytimes.com/2025/08/25/nyregion/china-consulate-new-york-elections.html>

divesting public pensions from China, which we believe states should do for both fiduciary and national security reasons.⁷

CCP-Affiliated infiltration at the subnational level

The Chinese Communist Party attempts broad infiltration and subversion of American society. These efforts go beyond what can be mitigated by federal laws and investigatory powers acting alone. Two of the most acute examples of infiltration are the positioning of Chinese assets, entities and individuals near military bases and critical infrastructure, and the infiltration of state institutions.

There have been widely reported cases of Chinese positioning near Laughlin Air Force Base, Grand Forks Air Force Base, Whiteman Air Force Base and Barksdale Air Force Base. These cases are but a sampling of the problem rather than an exhaustive list, and in each case, the problem was mitigated by a state or local government solution.⁸ We are aware of at least two more cases of potential PRC positioning near critical military bases that are currently being investigated, and we are confident there are many more instances in states where State Armor is not currently active.

The threats to critical infrastructure are far broader. The Washington Post has reported that Chinese-made solar inverters can be remotely accessed and sabotaged to cause rolling blackouts across the U.S.⁹ The Senate Intelligence Committee has reported Chinese cryptocurrency miner Bitmain to be a threat to the security of electrical grids¹⁰, and the Senate Committee on Banking, Housing and Urban Affairs is investigating for more information on these threats.¹¹

The CCP also targets a variety of state institutions. But in our experience, they target state university systems and state governments most heavily. The CCP Select Committee's seminal "Fox in the Henhouse" report described how American universities are taking Pentagon grants and partnering with entities in China linked to the Chinese military for research on developing advanced military technologies.¹² Over two years, over 1,400 research papers funded by the Pentagon were conducted in partnership with Chinese entities. In over half of these examples, the Chinese entity was affiliated with China's defense research and industrial base. In addition, the Select Committee's "Containment Breach" identified 4,350 research papers that were funded by

⁷ <https://statearmor.org/ccp-divestments/>

⁸ <https://www.congress.gov/119/meeting/house/119385/witnesses/HHRG-119-ZS00-Wstate-LucciM-20260625.pdf>

⁹ <https://www.washingtonpost.com/business/2025/12/10/us-energy-grid-china-threat-blackouts/>

¹⁰ <https://www.intelligence.senate.gov/2025/07/29/report-to-accompany-s-2342-intelligence-authorization-act-for-fiscal-year-2026/>

¹¹ https://www.banking.senate.gov/imo/media/doc/letter_to_secretary_lutnick_re_bitmain.pdf

¹² <https://chinaselectcommittee.house.gov/media/reports/fox-in-the-henhouse>

the Department of Energy and executed in partnership with PRC entities. In half the cases, the partnership was with an entity within China's defense research and industrial base. There are many examples of work done with one of China's 'Seven Sons of National Defense.' These papers were funded by the Department of Energy over a period of just two years.

These reports provide valuable information to state leaders who control the universities involved. This past spring, Louisiana State Senator Adam Bass passed the nation's most comprehensive state law on protecting campus research from the CCP and countering their influence operations. And aside from the law passed, Senator Bass made clear that he expected Louisiana's universities would exit the troubling partnerships revealed in your reports.

Furthermore, congressional leaders have called for Chinese Student and Scholar Associations (CSSAs) to be treated as foreign missions on American campuses.¹³ The CSSAs are ubiquitous across large American campuses, and according to our State Department, they are leveraged by the Party to suppress campus dissent against the CCP regime and to steal intellectual property to support China's rise.¹⁴

State legislatures that take on counterintelligence challenges are confronted with layers of legislative interference. The first layer is often from an American business or business association that has alignment with Chinese interests, as warned about by President Biden's ODNI memo. Then Chinese businesses themselves lobby heavily in statehouses. Another layer includes united front-associated influence operations that flood state houses with Chinese government propaganda. These pressure campaigns even include threats to state lawmakers and Chinese-American dissidents who speak against the CCP regime.

States as the first line of defense

The United States has a unique system of federalist government to provide for checks and balances in the use of power, and allow for policy experimentation in the states. We should leverage our system by leveraging our co-sovereign states which have the power to address security problems in our state universities, local utilities, state pension investments, procurements, law enforcement, and consumer fraud.

Here are some ideas on how an enhanced state-federal partnership can work.

First, state leaders would benefit from regular and iterative federal messaging on national security threats they might confront at the state level. I provided powerful examples of federal warnings earlier in this testimony. It would be even more useful if there could be regularly scheduled updates, perhaps through a single source that aggregates this open-source information across the federal government and synthesizes it and presents it through one messaging entity or

¹³ <https://chinaselectcommittee.house.gov/media/press-releases/chairmen-moolenaar-mast-walberg-ask-rubio-to-act-on-the-chinese-students-and-scholars-association>

¹⁴ <https://www.state.gov/wp-content/uploads/2020/09/CCP-on-campus-FINAL.pdf>

web portal with an audience of state and local officials in mind. Such information will empower state authorities to figure out problems that are described by federal authorities.

One example comes to mind. On March 5th, 2025, Congressman Krishnamoorthi held up a TP-Link router and told Americans not to use it. We printed that image and distributed it. State leaders asked important questions such as:

‘Do we use these routers in our offices?’

‘Do our employees use these routers at home?’

‘Do state contractors use these routers?’

‘Are these routers violating state consumer fraud laws?’

Since then, several states have prohibited use of those routers on state systems, and Texas’ Attorney General Ken Paxton filed the first state consumer fraud lawsuit against TP-Link.

In addition, new state-federal partnerships would be valuable to leverage state powers under federal guidance. For example, state attorneys general have partnered with the FCC to understand Chinese technological threats and how they might violate state consumer fraud laws.¹⁵ Texas Governor Greg Abbott worked with the state legislature to create Texas Cyber Command, which builds upon federal cyber assets in San Antonio to help secure Texas. States including Florida, Texas and Nebraska have considered the creation of counter-intelligence units, which can be encouraged and supported by federal authorities.

Federal leaders should also invite state lawmakers to participate in homeland security exercises that contemplate homeland security threats that would manifest in the event of a regional or global conflict with one of America’s adversaries. Nebraska and Texas have established working committees that prepare for these threats, and other states have also begun to make similar preparations. Federal exercises that occur with these threats in mind would help state leaders understand how such events might unfold, and how they can prepare for these dangers ahead of time.

Of course, the federal government can dedicate resources to help states mitigate such threats or even establish counterintelligence operations. And federal leaders should observe experimentation at the state level, including what is being done in Nebraska, Florida, and Texas, and amplify, fund, and perhaps even nationalize the most effective resilience policies.

Next, federal leaders can encourage states to match federal actions, especially when that encouragement can be bipartisan. The federal Thrift Savings Plan divested from China. Yet states in aggregate have larger pension funds than the federal Thrift Savings Plan, and only a handful of states have taken action to divest. The Pentagon releases and updates the 1260H list of Chinese

¹⁵ <https://www.foxnews.com/politics/fcc-state-ags-join-forces-crackdown-china-linked-communications-technology>

Military Companies operating in America. These companies are banned from Pentagon contracts, and defense contractors are ineligible for Pentagon contracts if they have a lobbyist who represents a 1260H firm.¹⁶ This can be replicated at the state level for procurement. An amended version of the federal foreign agent law can be implemented at the state level without the federal loopholes that allow bona fide foreign agents to escape transparency. We recommend these laws be enacted with an exclusive focus on agents of federally defined foreign adversaries and terrorist organizations. The Pentagon and National Science Foundation have prohibited use of their funds in research partnerships with 1286H entities, which are Chinese research institutions that present research security threats. States can apply similar safeguards to their state-funded research institutions.

Finally, united front influence operations are becoming more pernicious at the subnational level. Just in Texas, I am aware of lawmakers and members of the Chinese diaspora community being threatened and harassed by Chinese nationals inside the state capitol. This happens across states, and these statehouse interference operations are often directed by Chinese nationals who graduated from universities associated with the Chinese military. They leverage domestic organizations that openly partner with the Chinese government and united front institutions, such as the 53 organizations described in New York Times reporting as interfering in New York's elections.¹⁷ Regular federal guidance and case studies on how to recognize these united front operations and organizations and distinguish them from understandable concerns from the Chinese-American community would be valuable. So would training on recognizing and countering transnational repression.

America's strongest response to the counterintelligence threat presented by the Chinese Communist Party is to turn our federalist system from a source of strategic confusion into a national strategic asset. Partnering with and empowering states with federal expertise, resources, policy guidance, and data flows will result in our state governments solving national security problems that may seem distant from Washington, D.C., but which are right in the back yards of state leaders. And federal leaders will learn that empowering our state laboratories of democracy will result in lessons and solutions that are only possible from unleashing 50 units of American state government to innovate on how to protect their citizens and assets.

¹⁶ <https://www.war.gov/News/Releases/Release/Article/4023145/dod-releases-list-of-chinese-military-companies-in-accordance-with-section-1260/>

¹⁷ <https://www.nytimes.com/2025/08/25/nyregion/china-consulate-new-york-elections.html>