Questions for the Record

China's Economic Espionage and Subnational Influence in the United States

6/25/2026

Representative Zach Nunn – District IA-03

Witness – David Shedd

1. **During my time as NSC Cybersecurity Director at the White House, I worked on counterintelligence efforts, particularly in holding bad actors like Huawei accountable—which used a shell company, Sophgo to covertly procure nearly 3 million chiplets directly into Huawei's Ascend 910B processor. I worked to sanction Huawei, but it remains prime example of how the CCP can bypass U.S. restrictions, steal advanced US IP, and accelerate its efforts to close the AI gap. At the same time, we also need to recognize that the US doesn't have the domestic capabilities to immediately produce what we need domestically to maintain a competitive edge over China.**

"Thank you for your question, Rep. Nunn. Even as your inquiry suggests, there is no single "magic bullet" for responding to China's continued theft of our technology, innovation, data, and associated know-how.

As a starting point, I advocate for a partial economic decoupling from China. We should identify a relatively small number of technologies and capabilities that we must protect at all costs. Put another way, the technologies and intellectual property we need to protect from the PRC/CCP should be treated like a small yard with high walls and 50-caliber guns protecting it.

The United States needs a dual-track strategy: strengthen export controls while rapidly expanding our domestic and allied technological capabilities and diversifying supply chains away from dependence on China.

We need to modernize U.S. export controls. Today, controls are often reactive and vulnerable to evasion through shell companies and third countries. The United States should shift from static product-based export bans toward entity- and behavior-based controls. We need to target export-evasion networks and front companies established by our adversaries to circumvent export restrictions. The Department of Commerce, supported by sound intelligence from the Intelligence Community, should significantly enhance end-use verification, traceability, and audits for the key technologies and capabilities we seek to protect within these "small yards," including semiconductor production and AI-enabling chips.

The United States should work much more closely with allies such as Japan, the Netherlands, South Korea, Taiwan, and many others to strengthen export restrictions and re-export enforcement.

We should sanction not only targeted firms, but also the logistics, financial, and procurement networks that enable circumvention of our updated export-control regime.

We also need to expand domestic and allied semiconductor capacity. The goal is not complete self-sufficiency, but rather a reduction in dependence on vulnerable supply chains.

We should continue to focus on semiconductors and chips and increase investment in advanced packaging and chiplet technologies, which can scale more quickly than new leading-edge fabs. In addition, we should refine CHIPS Act-style investments by emphasizing security-critical production and trusted supply chains. Finally, we should build a trusted manufacturing ecosystem with key allies through shared standards and coordinated security measures.

Our success depends on more than hardware. The U.S. government needs to ensure the private sector has the right regulatory framework to support U.S.-led AI

models, software frameworks, and toolchains. At the same time, we must get our domestic regulatory framework right, including our cybersecurity policies, so we can promote the adoption of U.S. AI technologies and governance standards globally.

We also need to strengthen our counterintelligence efforts, which I will address in more detail in response to your second question. Protecting technology, intellectual property, innovation, and data is just as important as developing them.

It is essential that we expand efforts to detect and prevent technology theft, including theft of semiconductor and AI intellectual property. At the same time, we need to identify and disrupt procurement networks that evade sanctions while continuing to improve our insider-threat and workforce-security programs in sensitive industries and technologies.

We should apply adaptive, targeted sanctions. Overly broad, permanent bans can accelerate China's drive toward self-sufficiency. The fundamental point is that we should focus controls on the most advanced and strategically important technologies. We should use flexible, evolving restrictions that adapt to changing capabilities. In support of partial decoupling from China, we should maintain limited commercial engagement where it supports U.S. competitiveness without advancing Chinese military capabilities or leading-edge AI development."

2. **If China's strategy is conducting large-scale, rapid, and intense economic espionage and United Front operations at all levels of our society, how can the United States build an equally coordinated defense? Specifically, how do we move from deploying counterintelligence capabilities at the national level to ensuring these same defensive tools are delivered directly to small businesses, startups, and farmers on the ground in places like Iowa?**

“Thank you for this additional question. In my view, the response calls for thinking about counterintelligence differently than we traditionally have within the Intelligence Community. Just as we have pushed counterterrorism threat information from the national level to state, local, and tribal partners, we should adopt a similar approach for counterintelligence aimed at the economic espionage China has long pursued in the United States.

The federal government should treat counterintelligence less as a narrow federal specialty and more as a distributed public-safety function. Washington should set national standards, but threat detection, training, and response support should be pushed to local chambers of commerce, cooperatives, extension offices, universities, and industry groups. The goal is to build a federated defense network in which federal agencies provide intelligence, playbooks, and rapid alerts, while state and local partners translate them into practical protections for firms of all sizes, startups, and even farmers.

China’s economic espionage is not a single tactic but an ecosystem that includes cyber intrusions, insider threats, front companies, talent-recruitment programs, and commercial partnerships. Our defense therefore must be equally layered, rather than siloed in Washington or left primarily to the FBI. A useful analogy is public health: the federal government tracks outbreaks, but local clinics, pharmacies, and county systems deliver protection where people live.

We should turn federal counterintelligence warnings into plain-language sector advisories for manufacturing, academia, biotechnology, software, agriculture, and logistics. Those advisories should be routed through state universities, extension services, Small Business Development Centers, and agricultural associations so that an Iowa startup or farm understands the risks in terms of seed genetics, machinery design files, customer lists, drone data, or supplier contracts. Each advisory should include a short checklist covering insider-risk controls, vendor vetting, secure document handling, travel and contact guidance, and incident reporting. We should also pair these warnings with subsidized cyber-hygiene support, since cybersecurity remains one of the most common entry points for trade secret theft.

Small businesses and farmers usually will not call a federal counterintelligence office first, so the delivery system must run through trusted intermediaries. That means training local bankers, insurance agents, county extension specialists, trade groups, and startup accelerators to recognize suspicious recruitment, coercion, and partnership offers.

The federal government, led by the Department of Justice and the FBI and working in tandem with the Department of Homeland Security, should publish sector-specific threat templates, fund regional counterintelligence liaison teams, and require incident debriefs that feed lessons back into local guidance. It should also align intelligence priorities with economic-espionage forecasting, so the warning system is proactive, not merely reactive after the theft has already occurred.

Success is not measured by how many threats Washington spots on its own. It is measured by whether a farm cooperative in Iowa, a biotech startup in North Carolina, or a machine shop in Ohio can recognize an approach, harden its systems, and report it quickly. In practice, that means a national counterintelligence backbone, state-level translators, and local delivery partners working as one system.

I believe this is, in essence, a requirement for a of U.S. whole-of-society response, and it is needed with urgency."