S. HRG. 119–168

INNOVATION IN THE CROSSHAIRS: COUNTERING CHINA'S INDUSTRIAL ESPIONAGE

HEARING

BEFORE THE

COMMITTEE ON SMALL BUSINESS AND ENTREPRENEURSHIP

OF THE

UNITED STATES SENATE

ONE HUNDRED NINETEENTH CONGRESS

FIRST SESSION

JULY 23, 2025

Printed for the use of the Committee on Small Business and Entrepreneurship

Available via the World Wide Web: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE

61–657 WASHINGTON : 2026

COMMITTEE ON SMALL BUSINESS AND ENTREPRENEURSHIP

ONE HUNDRED NINETEENTH CONGRESS

JONI ERNST, Iowa, *Chair*
EDWARD J. MARKEY, Massachusetts, *Ranking Member*

JAMES E. RISCH, Idaho
RAND PAUL, Kentucky
TIM SCOTT, South Carolina
TODD YOUNG, Indiana
JOSH HAWLEY, Missouri
TED BUDD, North Carolina
JOHN R. CURTIS, Utah
JAMES C. JUSTICE, West Virginia
JON HUSTED, Ohio

MARIA CANTWELL, Washington
JEANNE SHAHEEN, New Hampshire
CORY A. BOOKER, New Jersey
CHRISTOPHER A. COONS, Delaware
MAZIE K. HIRONO, Hawaii
JACKY ROSEN, Nevada
JOHN W. HICKENLOOPER, Colorado
ADAM B. SCHIFF, California

MEREDITH WEST, *Republican Staff Director*
SEAN MOORE, *Democratic Staff Director*

CONTENTS

JULY 23, 2025

OPENING STATEMENTS

WITNESSES

ADDITIONAL LETTERS/STATEMENTS FOR THE RECORD

QUESTIONS FOR THE RECORD

INNOVATION IN THE CROSSHAIRS: COUNTERING CHINA'S INDUSTRIAL ESPIONAGE

WEDNESDAY, JULY 23, 2025

UNITED STATES SENATE,
COMMITTEE ON SMALL BUSINESS
AND ENTREPRENEURSHIP,
Washington, DC.

The committee met, pursuant to notice, at 2:32 p.m., in Room 428A, Russell Senate Office Building, Hon. Joni Ernst, chairwoman of the committee, presiding.

Present: Senators Ernst [presiding], Young, Hawley, Curtis, Justice, Husted, Markey, and Shaheen.

OPENING STATEMENT OF SENATOR ERNST

CHAIR. I call the Committee on Small Business and Entrepreneurship to order. Before we get started with the business before us, I would like to take a moment to present a Senate 20-year Service Award to the committee's clerk, Kathryn Eden. Would you come forward, please, Kathryn.

Kathryn came to the Senate in 2005 to serve as the scheduler for her home state Senator, and later served as the operations director for the Senate Committee on the Environment and Public Works. Kathryn has served as the Small Business Committee's chief clerk for 10 years under the leadership of numerous chairman and ranking members of the committee, including Senators Vitter, Cantwell, Shaheen, Rubio, Cardin, Paul, Markey, and Ernst.

As a non-designated staffer of the committee, the chief clerk works for both the Republicans and the Democrats, which can be extremely challenging to navigate. At times, Kathryn makes being non-partisan look easy, and we all appreciate her expertise, strong judgment, attention to detail, responsiveness, and dedication to our members, staff, and constituents.

On behalf of all of the members of the committee and our staffs, I want to thank Kathryn Eden for her service to the Senate. Congratulations, Kathryn.

[Applause.]

CLERK. Thank you.

CHAIR. You're very welcome. So, Ranking Member Markey, do you have any comments?

Senator MARKEY: I do have a few comments——

CHAIR. Wonderful.

Senator MARKEY [continuing]. To make while you make this presentation, and that is that the Democrats join the Republicans

in thanking you, Kathryn, for 20 years of service. Your attention to detail, your tireless work ethic, your years of experience have shaped the very way this committee operates. Nothing we do here is possible without you and your team.

You represent the very best public service; committed, capable, and always professional. And I know I speak for all of our members when I say that we are enormously grateful for your 20 years of service. It's been outstanding. We're grateful for all you've done, and we're looking forward to the years ahead.

CHAIR. So, thank you for pausing just for a moment as we've presented that award. 20-year pins are very hard to come by here. And so, Kathryn, thank you very much for your service.

Today's hearing comes at a pivotal moment. America has consistently been at the forefront of technological innovation. Nonetheless, our adversaries, especially China, are working overtime to undermine us. Over the past 100 years, the United States of America has catalyzed the world's most consequential technology breakthroughs, from putting mankind on the moon, to unlocking a whole new digital frontier.

Americans didn't just invent, we built. We turned those big dreams into real-world breakthroughs, securing a long and prosperous period of economic might and global leadership. But after a century of wins, we cannot become complacent. Over the past 20 years, those empowering Washington have looked the other way as China initiated a comprehensive industrial espionage strategy.

They're not hiding it either. The Chinese Communist Party through its Made in China 2025 plan has made crystal clear its goal: to eliminate U.S. technological leadership in critical industries. We need to be more clear-eyed folks. China desires nothing more than to surpass the United States technologically and militarily.

They want to impose their authoritarian ideology on the world and destroy the West. If we want any shot at preserving America's leadership and war fighting capabilities, we have to lock down our innovation pipeline. The truth is, America has left its door wide open, effectively inviting our adversaries to take advantage.

As a result, sensitive industries have become vulnerable to exploitation, allowing countries like China to use well-known techniques, including talent recruitment programs, to steal our innovations. The CCP forces innovators across our vibrant startup economy to hand over trade secrets and intellectual property as a cost of doing business. They invest in American firms not to help, but to scheme, snoop, and steal.

The United States Trade Representative and FBI estimate intellectual property theft by China costs our economy to $225 to $600 billion per year. The Small Business Innovation Research, or SBIR, and Small Business Technology Transfer, STTR, those programs are no exception. In 2021, the Pentagon first sounded the alarm revealing the pervasive exploitation of the SBIR program by foreign bad actors and recommended a foreign ties due diligence review process for applicants.

That's why through the SBIR and STTR Extension Act of 2022, I fought to establish a framework to identify the extent of foreign risk that each company coming through the doors and stop award-

ing awards to malicious actors. It was a strong start, but it isn't enough. Congress must take further action to secure the critical technologies being cultivated in these programs.

In fact, my recent report on this subject showed that 64 percent of applications flagged for foreign risk were still eligible to receive taxpayer dollars. That's unacceptable. I ask unanimous consent to enter this report into the record.

CHAIR. We cannot afford to keep investing taxpayer dollars to develop and deploy our best homegrown technologies while failing to safeguard them against theft by our adversaries. This is why earlier this year, I introduced the INNOVATE Act. It would tighten our defenses, standardizing foreign ties, due diligence in SBIR across participating agencies, and giving agencies more muscle to claw back award dollars when our national security is threatened. It's just common sense.

Let me be clear, this is only a first step. The disturbing reality is that China is already conducting economic warfare in our homeland by targeting our farmland and critical infrastructure. If we want to win the next century and beyond, we must protect our innovators, our intellectual property, and the technologies that will shape our future. I'm looking forward to hearing from our expert witnesses today on the scale of these threats and response measures for Congress to consider.

I now recognize Ranking Member Markey for his opening statement.

STATEMENT OF SENATOR MARKEY

Senator MARKEY. Thank you, Madam Chair, very much.

From the beginning of the Industrial Revolution, Massachusetts has been at the epicenter of innovation for our country. Although I will say that I'm only here because Thomas Markey left to go to Dovan New Hampshire, where the Industrial Revolution was raging and ultimately moved to Lawrence, Massachusetts, where even larger plants were being built.

And over the years, Massachusetts has been powered by the world's top universities, research institutions, strong public and private investments, and the best trained and brightest individuals that can be found in our country and around the world.

The biggest threat to our innovation ecosystem, both in Massachusetts and across the entire country, is not coming from abroad. It is coming directly from 1600 Pennsylvania Avenue. It is coming directly from the White House.

We all agree on the importance of research, security, and protecting our technology from China's espionage. There's no doubt that American technology needs to be protected from foreign adversaries, but right now it is President Trump himself who is killing American innovation and China is reaping the benefits of those decisions.

Over the past seven months, President Trump has launched an all-out attack on higher education, threatening to withhold billions of dollars from universities that do not bend to the will of the administration, proposed dismantling the Department of Education beginning with laying off half of the department's workforce, gutted programs, grants, and staff for research and development at the

U.S. Department of Agriculture, the Department of Energy, the Environmental Protection Agency.

Slashed the National Institutes of Health budget by 40 percent—that's research in Alzheimer's, and in Diabetes, and Parkinson's, Cancer research—and laying off thousands and thousands of researchers. And it has gutted the National Science Foundation by 57 percent, and NASA by 24 percent, repealed the Inflation Reduction Act for wind and solar, all electric vehicles battery storage technologies.

China looks at us and they're saying, "Why are you gifting us with the clean energy future for the world and the biotech future for the world? Those are the industries of the 21st century. Why? What did we do to deserve this gift from the Trump administration?"

And it has also even canceled previously awarded research grants including one to Boston Children's Hospital that was searching for a vaccine to fight all coronavirus viruses, and he is restricting foreign students from enrolling in universities and creating such a hostile environment that future innovators and researchers are choosing to take their talents elsewhere, including just staying in China. President Trump is taking America's crown jewel and handing it to China on a silver platter.

Federal government plays an outsized role in ensuring America has a competitive edge against the rest of the world, including China, whether that be through grants, contracts, funding for universities, friendly immigration, policies of robust agency funding. In 2022, 41 percent of basic research in the United States was federally funded, while only 35 percent was funded privately. Additionally, nearly a third of this federally-funded research was performed at universities.

These attacks and cuts to innovation will not result in a greater, stronger, wealthier America. In fact, President Trump's proposed 22 percent cut in research and development funding could shrink the U.S. economy by almost 4 percent. The last time we saw such a setback was during the Great Recession.

With China on our heels, instead of attacking universities, gutting science-based agencies, canceling research grants, and dissuading the best and the brightest from around the world from moving here, we should be doubling down to ensure that the United States can continue to lead the world in innovation.

So, yes, I agree with my Republican colleagues that we must protect our innovation and research that is being produced here in America, but we also must make sure that we have something to protect. And I look forward to hearing from our witnesses today about the importance of investing in and protecting American innovation.

And thank you, Chair Ernst, for holding this hearing.

CHAIR. Yes. And thank you, Ranking Member Markey. And again, my apologies to our witnesses. They have called a second vote, and because we don't have other members present, I think we will go ahead and recess. We will come back—have you voted, Josh?

Senator HAWLEY. I have voted.

CHAIR. You have voted. Would you rather we go ahead and do——

Senator SHAHEEN. Keep going.

CHAIR. Okay. We'll go ahead if—Senator Hawley, we'll hand the gavel to you so we don't have to recess, and we'll have the witnesses proceed. So, if you want to go ahead and vote, Ed. I'll read our introductions here so that we can start with our witnesses. I apologize, we've got a lot of votes lately.

Again, I want to extend a warm welcome to all of our witnesses, and I'll go ahead with introductions of those witnesses who are testifying here today. And I'm thankful that you did take time out of your schedules to join us.

First, Ms. Emily de La Bruyère is the senior fellow at the Foundation for Defensive of Democracies, with a focus on China policy. She is a co-founder of Horizon Advisory, a consulting firm focused on the implications of China's competitive approach to geopolitics.

Emily holds affiliations with think tanks focused on national security and competition with China, including as a senior visiting fellow at the Krach Institute for Tech Diplomacy at Purdue, and as a non-resident fellow at the National Bureau of Asian Research. Ms. de La Bruyère holds a bachelor's degree from Princeton University and a master's degree from Sciences Po, Paris.

Next, Dr. William Hannas—did I say that right? Hannas? I want to make sure we get everyone's names right. Is lead analyst and research professor at Georgetown Center for Security and Emerging Technology.

Previously, Dr. Hannas was a member of the Senior Intelligence Service at the Central Intelligence Agency. He started his career in the United States Navy as a cryptanalyst of foreign codes and ciphers and later served with a joint Special Operations Command at Fort Bragg. And thank you very much for your service to our country.

Dr. Hannas holds a bachelor's degree in Chinese history from Temple University, a master's degree in Chinese from the University of Chicago, and a PhD in East Asian languages and linguistics from the University of Pennsylvania.

And our minority witness today is Dr. Shivakumar. And Dr. Shivakumar directs the Renewing American Innovation Program at the Center for Strategic and International Studies, where he also serves as a senior fellow.

Previously, he directed the Innovation Policy Forum at the National Academies of Sciences Engineering and Medicine. And Dr. Shivakumar holds a bachelor's degree from Carleton University, and a PhD in economics from George Mason University. And thank you very much for joining us today.

So, we'll start with our testimonies. And in front of you, you will have a system of lights. Please press "speak" to speak, and that green means you're good. But once you hit that yellow button, you've got a minute left and we need to start wrapping up. And when we hit red, your time will be expired.

So, Ms. de La Bruyère, we are going to start with you. You are recognized for five minutes.

STATEMENT OF MS. EMILY DE LA BRUYÈRE, SENIOR FELLOW, FOUNDATION FOR DEFENSE OF DEMOCRACIES, SEWICKLEY, PENNSYLVANIA

Ms. DE LA BRUYÈRE. Thank you for the opportunity to testify today.

China is winning the technological competition against the United States. China is not winning by out-innovating the U.S. Beijing isn't besting us at the game we assume to be underfoot. Rather, the Chinese Communist Party is winning because they aren't racing.

The CCP weaponizes the interdependence of the global system in order to acquire advanced technologies at low cost and low risk. Beijing then focuses its resources on the areas where it sees actual competitive advantage. First, applying those technologies including to scale global systems and control international supply chains. And second, placing targeted risk-adjusted bets in potentially paradigm-shifting domains where first mover advantage actually matters.

The strategy is working and it is asymmetric. It plays perfectly to China's strengths, including of scale, centralization, and industrial capacity. China's strategy also converts core U.S. characteristics into weaknesses. Beijing is able to benefit from U.S. innovation and investment.

China preys on the openness of the American system for access and its decentralization for control. The risks and the threats of this approach are particularly acute today because, and this is core to the CCP's approach, the contemporary tech revolution is transforming the global order. Modern advances in technology are creating new markets, new methods of production, and new forms of control. If China can win the tech contest, it can capture production markets and control.

Avoiding as much requires first understanding Beijing strategic orientation and second fighting back. That orientation begins with access to technology from the academic and especially from the commercial sectors. To access the commercial technology, Beijing leverages illicit means like industrial espionage and in China forced data localization.

But Beijing, also and in particular, takes advantage of particular entirely illicit means. Beijing is manipulating not attacking the international business environment. Government-backed and government-guided Chinese entities go out into the international system to obtain technology through acquisitions, to ventures, direct and indirect investment, talent programs, and personnel recruitment, and even lawsuits.

Those Chinese entities benefit from government support and guidance, freeing them from market forces and therefore allowing them to redeem strategic value from counterparts who are bound by economic logics. Alongside those go out vectors of tech acquisition. Beijing deploys a parallel and compounding bring-in program, leveraging the appeal of the Chinese market and Chinese industrial base to attract foreign IP, research and development, data, personnel, even capital.

This strategy and positioning put all U.S. technology at risk. They ensure that the U.S. approach to tech development and lead-

ership is not only a losing one, but in fact, fuels America's strategic adversary. America needs to change its game. First, the U.S. government needs to shift from protecting American technology from China to defending the U.S. market from China. Washington needs to impose real and rigorous restrictions on Chinese commercial entities operating in the United States or seeking to access the U.S. market.

Such restrictions should cover direct and indirect investment, joint ventures, including minority stakes, and tech licensing. They should also cover construction and deployment of information systems, components, and software. Those restrictions should adopt presumptions of denial. They should also adopt definitions of Chinese entities that are robust enough that China cannot circumvent them through localization and shell companies.

Second, the U.S. needs to activate its private sector to stop forfeiting critical U.S. resources to China and to start investing in the actual competition at hand. The private sector should have to choose between the U.S. and Chinese markets.

Businesses that localize data research and development production in China, invest in Chinese entities, or maintain tech licensing deals with Chinese entities should not be eligible for federal procurement, defense industrial-based procurement, federal tax credits or other incentives. Those are all sticks.

At the same time, the U.S. government needs to ensure that those companies that are opting for America and for the American market can invest, produce, and partner profitably in the United States. To do so, Washington needs to provide the infrastructure necessary for production, including through expanded provision of domestic energy and upstream resources, a favorable regulatory environment, and a skilled workforce.

We have the chance to reclaim our core strengths and reset the playing field. America's market can serve America's interests if we protect it from China. American innovation can fuel us not our adversary if we direct it at the actual competitive arena. And our agility as a country can throw the deliberate, slow, centralized PRC system on its heels if we take the initiative. But all of that has to happen now. Thank you.

[The prepared statement of Ms. de La Bruyère follows.]

CONGRESSIONAL TESTIMONY: FOUNDATION FOR DEFENSE OF DEMOCRACIES

Senate Committee on Small Business and Entrepreneurship

Innovation in the Crosshairs:

Countering China's Industrial Espionage

EMILY DE LA BRUYÈRE

Senior Fellow
Foundation for Defense of Democracies

Washington, DC
July 23, 2025

Chair Ernst, Ranking Member Markey, thank you for the opportunity to testify today.

China is winning the technological competition against the United States. China is not winning by out-innovating the United States; by besting the United States in the race America assumes to be underway. Rather, Beijing is winning because it isn't racing. Beijing is playing a completely different game. The United States cannot recover by racing faster or smarter or by racing at all. The United States must start blocking and tackling instead — and start building.

China's Asymmetric Strategy

The Chinese Communist Party (CCP) weaponizes the interdependence of the global system to acquire advanced technology at low cost and low risk. Beijing then focuses its resources on the points where it sees real competitive advantage: first, *applying* technology, including to scale global systems and control value chains; and second, placing targeted and risk-adjusted bets in potentially paradigm-shifting domains, like materials science and cross-cutting disciplines, where first-mover advantage can be determinative.

This strategy is asymmetric. It plays to China's strengths — including scale, centralization, and industrial capacity. It lets Beijing benefit from American investments, namely in creating and proving cutting-edge technology, therefore freeing up China's resources for the real contest: the applications of that technology. China's strategy converts core U.S. characteristics, and presumed strengths, into weaknesses. Beijing preys on the openness of the American system for access and its decentralization for control.

And Beijing's strategy is working. China has proven its ability to acquire crown jewel technologies from the rest of the world — despite increasingly serious efforts to prevent as much. Beijing has also proven the strategic value of competing at the application stage.[1]

The first practical solar cell was made at Bell Labs in Murray Hill, New Jersey. But China now owns some 90 percent of the global solar supply chain. The global solar industry therefore depends on China for both production and technology. China decides the technological direction of the field. And Beijing is increasingly using this foothold to dominate in downstream and adjacent domains, like smart grids. The People's Republic of China (PRC) therefore claims control over not only a future energy source but also critical infrastructure.[2]

In communications, the United States led the world in developing 5G technology. But it was Beijing that built scaled, global 5G systems. It is therefore Beijing that has cemented access to the information on those systems; an advantage in the infrastructures, like smart cities and smart transportation, built on top of them; and leadership in the hardware inputs, like chips and modules, going into them.[3]

---

[1] Emily de La Bruyere and Nathan Picarsic, "Military-Civil Fusion: Crafting a Strategic Response," *CHIPS*, July 2019. (https://www.doncio.navy.mil/chips/ArticleDetails.aspx?ID=12635)
[2] "Out of China's Shadow," *Horizon Advisory*, February 2024. (https://www.horizonadvisory.org/solarsqueeze)
[3] Nathan Picarsic and Emily de La Bruyere, "Wiring a 6G World," *Hinrich Foundation*, September 19, 2023. (https://www.hinrichfoundation.com/research/article/us-china/wiring-6g-world)

OpenAI changed the game in artificial intelligence. But with DeepSeek, China matched the performance of American leaders at a fraction of the price. Beijing is therefore positioned to claim the algorithm layer of the AI era and to own the foundation on which vertical applications, the real reward of AI, will be built.[4]

The Stakes at Hand

The story repeats across technologies and sectors. The United States is playing a losing game.

This matters because technology matters — for economic prosperity and security, national sovereignty, and international influence. The stakes are particularly high today because, and this is key to the CCP's strategy, contemporary tech revolution is reshaping the global order. Modern advances in technology — including big data, artificial intelligence, and biotechnology — are creating new markets, new methods of production, and new means of control. If China can win today's tech competition, it can capture global markets, production, and control.

In a world where China wins, Beijing owns not only global supply chains but also core information networks, the rules and standards guiding them, and the data on them. Therefore, Beijing controls economic growth, opportunity, and future generations of technological innovation. In this world, countries, including the United States, will be reduced to vassal states, dependent on Beijing's tech empire. So will companies. Industrial and commercial activity will rely on Chinese systems and inputs, ensuring an advantage for Chinese companies.

If you are a tech worker in San Francisco, you will work for a Chinese big tech company, that company will answer to the CCP, and the value you create will flow to China. If you are a farmer in Iowa, you will rely on Chinese smart agriculture systems — as well as Chinese seeds and the Chinese market — such that China will be able to decide your economic future. Ultimately, Beijing will take over your farm. If you are an American and you have an idea, capitalizing on that idea will require building on a Chinese system. Therefore, it will be a Chinese entity that benefits.

This future may sound overblown. But it is already being made. And as long as the United States does not change its competitive approach, this future will materialize. Avoiding as much starts from understanding Beijing's strategic ambition and how Beijing pursues it.

China's Path to Tech Access

The CCP's asymmetric strategy begins with access to technology. Beijing secures that access in part through academic relationships but most of all through commercial ones. Leveraging its "State-led, Enterprise-driven" model of government-industry coordination, Beijing weaponizes the open, global nature of international markets — and the commercial research and development (R&D) they contain — to acquire innovation.

---

[4] Nathan Picarsic and Emily de La Bruyere, "What DeepSeek Taught Us about Gaps in US Tech Strategy," *Hinrich Foundation*, February 25, 2025. (https://www.hinrichfoundation.com/research/wp/tech/what-deepseek-taught-us-about-the-gaps-in-us-tech-strategy)

Beijing accomplishes some of this through illicit means: industrial espionage conducted via cyber and human vectors and, in China, forced data localization, for example.

However, much of China's tech acquisition is entirely licit, a manipulation of — but not an attack on — international business. Government, government-backed, and government-guided Chinese entities "Go Out" into the international system to obtain technology through acquisitions, joint ventures, direct and indirect investment, talent programs and personnel recruitment, and even lawsuits. Those Chinese entities benefit from government support and direction, freeing them from market forces, and therefore allowing them to redeem strategic value from counterparts bound by economic logics. Alongside those "Go Out" vectors of tech acquisition, Beijing deploys a parallel and reinforcing "Bring In" program, leveraging the appeal of the Chinese market and Chinese industrial base to attract foreign intellectual property (IP), research and development, data, and even capital necessary to fuel China's domestic tech program.

Across the board, Beijing preys on the constraints and incentives of commercial entities — and manipulates U.S. and international restrictions intended to prevent as much.

China's Vectors of Commercial Tech Access

Illicit mechanisms

- Cyber espionage
- Human espionage

Licit mechanisms

- Go Out
  - Investment (incl. via limited partnership stakes)
  - Joint ventures (incl. minority joint ventures)
  - Acquisitions (incl. out of bankruptcy)
  - Lawsuits (incl. that lead to discovery)
  - Talents programs and employee poaching
- Bring In
  - Market access restrictions (e.g., forced tech transfer, joint ventures, and data localization)
  - Incentives for localization of production, research, and development in China (e.g., through industry zones)
  - Incentives for investment in China
  - Conferences and industry fairs

For instance, Chinese tech acquisitions have been known to target distressed or bankrupt U.S. companies with cutting-edge intellectual property, including military-relevant and -funded IP.

These entities have strategic value but lack immediate commercial traction. They are therefore ripe for the taking. In 2017, for example, Chinese automotive group Zhejiang Geely Holding Group acquired struggling U.S. flying car start-up Terrafugia, a DARPA contributor. Terrafugia has since reportedly moved part of its operations and IP to China.[5]

And while the United States has deployed a host of policies, including investment review, intended to prevent China's tech poaching, Beijing has managed consistently to find and exploit loopholes. Chief among those are minority and limited partnership stakes not covered by U.S. regulation.[6] Take TuSimple, for instance. A self-driving truck startup, TuSimple launched in 2015, backed by Chinese capital, with a dual presence in both China and the United States. Its U.S. address granted it legitimacy in the American market. That, in turn, enabled fundraising and partnerships — at the expense of legitimate U.S. companies. TuSimple's presence in the United States also gave it access to technology and data. Both ultimately made their way to China.[7]

In those cases, Beijing leverages short-term economic incentives to "Go Out" into the international system and acquire technology. Beijing also uses those short-term economic incentives to bring companies, and their technology, into China. The PRC is the world's second-largest market and a rapidly growing one. International companies want access. Beijing grants them as much but with conditions — like forced technology transfer, joint ventures, and data localization — that make market access contingent on the surrender of technology. International companies get to sell into China for a few years. But in the process of doing so, they sow the seeds of their own demise: They arm Chinese competitors with the tools necessary to overtake, in China and internationally.

Similarly, Beijing incentivizes foreign companies to localize production, research, and development in China; to encourage their suppliers and customers to do the same, including through government-led industry zones; and to invest in Chinese tech entities. These policies generate favorable margins for production, access to low-cost Chinese suppliers, and profitable exits — in the short term. But these policies also lead to knowledge transfer and spillover, generate dependence on China that grants Beijing leverage over IP, and provide the PRC with the human and financial resources necessary to fund its tech offensive.

Take, for example, a case from the biopharmaceutical industry. In the early 2000s, driven by Chinese government incentives and low costs, Eli Lilly established a pharmaceutical service outsourcing company in Shanghai's Zhangjiang High-Tech Park and transferred part of its research and development footprint there. This move catalyzed the development of the contract research organization industry in China. Over the years that followed, a bevy of other multinational companies established footprints in the area, forming, as Chinese media puts it, "a

[5] Charles Alcock, "Terrafugia Owner Moves Transition Flying Car Program to China," *Aviation International News*, February 23, 2021. (https://www.ainonline.com/news-article/2021-02-23/terrafugia-owner-moves-transition-flying-car-program-china)
[6] Nathan Picarsic and Emily de La Bruyere, "The Weaponization of Capital: Strategic Implications of China's Private Equity/Venture Capital Playbook," *Foundation for Defense of Democracies*, September 15, 2022. (https://www.fdd.org/analysis/2022/09/15/the-weaponization-of-capital-chinas-private-equity-venture-capital)
[7] Heather Somerville, "The Self-Driving Truck Startup That Siphoned Trade Secrets to Chinese Companies," *The Wall Street Journal*, May 27, 2025. (https://www.wsj.com/tech/china-self-driving-trucks-tusimple-c20255e1)

unique new drug R&D ecosystem in Zhangjiang."[8] That new drug R&D ecosystem is increasingly dominated by Chinese companies, building on the technology brought in from abroad. Many of those Chinese companies have been founded by the very Eli Lilly, Merck, AstraZeneca, and Pfizer employees who led, and encouraged, those giants' moves to China. These new Chinese upstarts benefit from government funding, investment, and preferential policies that let them underprice and outproduce the international competitors that spawned them. And those international competitors? They continue to invest, partner, and produce in China. They continue to fuel their own destruction.

Or — in a case where the "Bring In" and "Go Out" programs overlap — take Suzhou Innolight, a Chinese optical module company that the Ministry of Industry and Information Technology designated as a "single champion" in 2022. Innolight's founder and CEO began his career in the United States before returning to China in 2008, as part of a government talents program, to launch the company. He did so with backing from both the Suzhou government and Acorn Campus Ventures, a venture capital firm with a presence in California and tied to Chinese sources of capital. Innolight has grown through Chinese government industrial policy support and state-backed investors on the one hand and U.S. investors, partners, and research facilities on the other. CapitalG, Alphabet's growth fund, has invested in the company.[9] Innolight has an R&D center in the United States. Chinese reporting indicates that the company is a key supplier of optical modules for Google and Amazon, among other international hyperscalers.[10] These U.S. relationships grant Innolight access to American technology and a cemented place in American data infrastructure — and American capital to fund the process. At the same time, Innolight's non-market Chinese government support ensures that it can continue to prevent any real challenge from international competitors.

The Scale of the Problem and Charting a Competitive Path

The Commission on the Theft of American Intellectual Property has estimated that Chinese tech theft costs the United States up to $600 billion a year.[11] The problem is so severe that the United States, and its allies and partners, have implemented an unprecedented raft of restrictions on Chinese entities and tech partnerships with them. Both that assessment and that response miss the point.

---

[8] "从和誉生物乔迁研发中心，看本土创新药企实力崛起 [From the Relocation of Abbisko Bio's R&D Center, We Can See the Rise of local Innovative Pharmaceutical Companies]," *Pharma Cube*, November 6, 2020. (http://www.360doc.com/content/20/1106/23/72280700_944506538.shtml); Wuhan Optics Valley plays a similar role in optoelectronics and third-generation semiconductor applications. See: "Chip Risk Monitor Monthly Note – December 2023," *Horizon Advisory*, December 2023. (https://www.chipriskmonitor.com/monthly-notes/december2023)

[9] Sonja Cheung, "Google Capital Makes First China Investment, Backs InnoLight," *The Wall Street Journal*, September 29, 2014. (https://www.wsj.com/articles/BL-VCDB-15564)

[10] Zhao Mianlu, "中际旭创-研报正文: 受益于北美CSP对ASIC服务器出货的乐观预期 [Zhongji Xuchuan-Research Report: Benefiting from North American CSP's Optimistic Expectations for ASIC Server Shipments]," *First Shanghai Securities*, June 18, 2025. (https://stock.finance.sina.com.cn/stock/view/paper.php?symbol=sh000001&reportid=803571720313)

[11] "Update to the IP Commission Report," *National Bureau of Asian Research*, 2017. (https://www.nbr.org/publication/update-to-the-ip-commission-report-february-2017)

China's strategy and positioning put all U.S. technology at risk. They ensure that the U.S. approach to tech development, and leadership, is fundamentally a losing one. If the United States does not change paths, Beijing will continue to hoover up cutting-edge technology. Beijing will industrialize and commercialize it at low cost and scale, undercutting international competition. In the process, the CCP will establish control over tomorrow's technological architecture, and therefore tomorrow's world. Beijing will do all of this backed by American innovation and capital.

The United States needs to change its game.

First, the U.S. government needs to shift from protecting American technology to protecting the American market. Washington needs to impose and enforce real, rigorous restrictions on Chinese commercial entities operating in the United States and their ability to access the U.S. market. Such restrictions should cover investment, both direct and indirect; joint ventures, including minority stakes, and tech licensing; and construction and deployment of information systems, components, and software that could give the PRC access to U.S. information and data. These restrictions should adopt definitions of Chinese entities that Beijing cannot circumvent through shell companies or localization — for example, the U.S. Commerce Department's definition of a "person owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary" — and presumptions of denial.

At the same time, the United States should not give up on efforts to slow China's access to critical technology — but should focus those efforts on strategic domains like military-relevant R&D and government funding. Such efforts should build on novel features of recently proposed legislation, like the INNOVATE Act introduced by Chair Ernst, to guarantee that R&D dollars are only doled out with appropriate due diligence and with capacity for funds to be clawed back in the event of fraud or negligence that results in adversarial access to U.S. government-funded technology.

Second, the United States needs to activate its private sector both to stop forfeiting critical U.S. resources to China and to start investing in the actual competition at hand. Such activation will require sticks. The private sector should have to choose between the U.S. and the Chinese markets. Because as long as a company operates in China, it will serve China's interests. Businesses that localize data, research, development, or production in China; invest in Chinese entities; or maintain tech licensing deals with Chinese entities should not be eligible for federal procurement, federal tax credits or other incentives, or defense-industrial base procurement. Such restrictions will send a strong signal. Those signals, necessary and long overdue, will, in turn, trigger accountability mechanisms throughout America's capital markets that can reinforce government market and tech protection edicts.[12]

[12] Nathan Picarsic and Emily de La Bruyere, "Commanding Heights; Ensuring US Leadership in the Critical and Emerging Technologies of the 21st Century," *Statement for the Record before the Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party*, July 26, 2023. (https://selectcommitteeontheccp.house.gov/sites/evo-subsites/selectcommitteeontheccp.house.gov/files/evo-media-document/scc-expert-written-testimony_20230726_emily-de-la-bruyere-and-nathan-picarsic.pdf)

There are carrots for Washington to provide, too. Restrictions on private sector engagement with China will incur short-term costs. The U.S. government will need to ensure that compliance with them generates opportunity to invest and produce in the United States, and in a way that is profitable. Washington should provide the infrastructure necessary for tech production, including through the expanded provision of domestic energy and upstream resources, a permissive regulatory environment, and a skilled workforce. This should include, for instance, access to training data and computing power for AI companies — if they are able to demonstrate intent and ability to protect that data and their technology from China. It should also include regulations that allow U.S. tech companies to form the consolidations and tie-ups necessary to compete with Beijing's scale — if their efforts align with downstream vertical markets and applications of national security and economic importance. And, relatedly, Washington should focus incentives on today's real, determinative contest: technological applications.

The United States is dangerously unaware of the state of the tech competition with China — and its stakes. We still think we're winning. We do not realize the degree to which our orientation fuels our competitor. And we certainly don't realize what will happen if we lose.

But there is a positive story too: Whether we recognize it or not, we are all too used to seeing our core characteristics turned against us; to playing a game that asymmetrically benefits our adversary. We have not internalized the *opportunity* at hand if we start playing a different game. America has the chance to reclaim our core strengths and reset the playing field. America's market can serve American interests — if we protect it from China. American innovation can fuel us, not our adversary, if it is directed toward the actual competitive arena. And our agility as a country can throw the centralized, slow, and deliberate PRC on its heels — if we take the initiative. But all of this must happen now.

Thank you for the opportunity to testify today.

Senator HAWLEY [presiding]. Thank you very much. Dr. Shivakumar, you are recognized for five minutes of testimony. The floor is yours.

STATEMENT OF DR. SUJAI SHIVAKUMAR, SENIOR FELLOW, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES, WASHINGTON, DC

Dr. SHIVAKUMAR. Thank you, Senator Hawley, and distinguished members of the committee. I'm honored to share my views on this important topic and concerning our nation's innovation strategy.

Just a quick note that CSIS is a bipartisan non-profit policy research organization dedicated to advancing practical ideas to address the world's challenges with the core mission to define the future of natural security. Please note that CSIS does not take any institutional policy positions, so the views represented here are my own.

So, as we begin our discussion today, I think it's important to keep in mind that the global strategic environment has changed fundamentally. In fact, the world's innovation landscape today is multipolar. Others can quickly grab U.S. ideas and run with them, as my colleague has just pointed out. Competitors and rivals are also rapidly developing their own ideas and have invested in scaling them up.

So, there's an important fact here; that we need to pick up our own pace in this global race. U.S. innovation leadership depends critically on our own country's ability to invest in research, make new discoveries, and then bring those to the market faster and at competitive cost. So, when competitive technologies aren't developed or can't reach scale because commercialization tools are underfunded, others will seek seize the opportunity. So, this means that we must reinforce key elements of our own innovation ecosystem.

A key point that I want to emphasize is that U.S. innovation and by extension, our competitiveness and national security, depends on sustained and substantial support to our federal R&D agencies and research institutions. Importantly, it also depends on our ability to convert the results of this research into products to meet the needs of the American people.

While the U.S. remains an innovation powerhouse, it produces more IP than through our research universities and corporations than any other country in the world. That edge is shrinking, and not least because our competitors and adversaries are advancing proposed cuts to our leading science agencies and research universities further erode that advantage.

In the past, there were few places where innovation inventions could be developed and, and rapidly commercialized that reality has changed. So, to maintain our competitive leadership and national security, we must surge investments into our domestic R&D technology, including scale up workforce development, advanced manufacturing, to ensure that the results of our research advantages U.S. security and everyday Americans.

My second key point is to affirm that the SBIR program is a proven natural security asset, and that we must continue to strategically support and expand it.

As someone who's directed multiple independent assessments of SBIR at the National Academies of Science and Engineering, I confirm that the program is sound in concept and effective in practice. It enables start startups and small businesses to bridge the valley of death, which is the gap between research or proof of concept and the commercial production.

It allows agencies like DOD to procure cutting edge innovations far faster than conventional programs that the Pentagon has. And SBIR has catalyzed the success of companies like Qualcomm, which have transformed our daily communications, and today continues to support breakthrough technologies, including drones, next generation, reconnaissance, quantum technologies, and missile propellants.

At a time of intensifying technological competition, SBIR awards contribute directly to our economic growth, technological leadership, and capabilities. Our adversaries and competitors have recognized the value of SBIR program for its proven outcomes and the technological leadership it has helped secure. As Chairman Ernst pointed out in her remarks, the DOD's internal report in 2021, documented efforts by state-sponsored Chinese firms targeting DOD's SBIR companies and that merits serious attention.

But let's be clear, if a competitor is stealing your playbook, it's probably because your playbook works. To be sure, steps should be taken to defend small companies against cyberattacks and foreign efforts to acquire ownership or to steal technology.

But SBIR supports small businesses that often lack the tools to protect themselves from this espionage, and they're often without in-house counsel, threat intelligence, or cybersecurity teams. So, we need to provide active support for their cybersecurity awareness and defense. In other words, our response should not be shut down or weaken the successful program, but in fact, to fortify it.

For SBIR to work, it needs to be safe, stable and substantial and yet flexible. First, it needs long periods of reauthorization. A strong program can't thrive in a climate of fiscal and legislative uncertainty. Secondly, we should strive to avoid overregulation. Micro-level legislative requirements on the program tend to be less effective than coordination and encouragement at the program manager level.

And third, we need to strengthen and encourage the transition to commercialization. SBIR companies help companies cross the valley of death in phase 1 and phase 2, but in many cases, that bridge ends halfway across the valley of death. There are different parts to add an additional arch, including perhaps an active agency-financed phase 3, particularly for agencies that don't have a procurement function.

So, in conclusion, I just want to say that innovation without commercialization is in fact a lost opportunity, and in a world of accelerating competition, potential gifts to our adversaries. SBIR works, but it must be buttressed with cybersecurity support, flexible flow on funding to facilitate commercialization and programmatic stability. Most importantly, it must remain embedded within a strong ecosystem, one that is supported by sustained and substantial investment in our federal R&D agencies and research institutions.

Thank you very much, and I look forward to your questions.

[The prepared statement of Dr. Shivakumar follows.]

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

Statement before the

Senate Committee on Small Business & Entrepreneurship

"Innovation in the Crosshairs: Countering China's Industrial Espionage"

A Testimony by:

Sujai Shivakumar, Ph.D.
Senior Fellow, Center for Strategic and International Studies
and Director, Renewing American Innovation

July 23, 2025
428A Russell Senate Office Building

Chair Ernst, Ranking Member Markey, distinguished Members of the Committee, my name is Sujai Shivakumar, and I am honored to share my views with you on this important topic concerning our nation's innovation strategy. I am a Senior Fellow at the Center for Strategic and International Studies, where I direct the program on Renewing American Innovation. CSIS is a bipartisan, nonprofit policy research organization dedicated to advancing practical ideas to address the world's challenges, with a core mission to define the future of national security. The program on Renewing American Innovation focuses on revitalizing the U.S. innovation system to enhance economic competitiveness and strengthen national security in today's challenging global environment. Please note that CSIS does not take institutional policy positions, so the views represented in this testimony are my own.

Thank you for the opportunity to testify today on why investment in and capacity of U.S. research and development (R&D) is crucial to build our economic competitiveness, global technological leadership, and national security. Universities, federal agencies, and the Small Business Innovation Research (SBIR) program all play vital and successful roles in that equation, enabling our R&D enterprise to grow new, strong clusters in the communities that need them most.

A key point, which I hope can be recognized on a bipartisan basis, is that U.S. innovation—and, by extension, our competitiveness and national security—depends on sustained, substantial support to our federal R&D agencies and research institutions and our ability to convert the results of this research into products that meet the needs of the American people.

While the United States is an innovation powerhouse that produces more intellectual property (IP) through our research universities and corporations than any other country in the world,[1] that edge is shrinking. In the past, there were few places where inventions could be developed and rapidly commercialized. That has changed. The current world economy is multipolar—others can quickly grab U.S. ideas and run with them[2]

Think of our innovation system as a set of interlocking gears. They have to work together. We can't block one of the gears and expect the same outcomes. We can't ask universities and small businesses to be able to expand due diligence while at the same time receiving dramatically fewer resources.[3] It will be hard for agencies to add new functions while their staff are undergoing significant reductions.

[1] Chris Borges, "Innovation Lightbulb: The U.S. IP Trade Surplus," CSIS, May 12, 2025, https://www.csis.org/analysis/innovation-lightbulb-us-ip-trade-surplus; Alexander Kersten and Chris Borges, "The United States' Trade Surplus in Intellectual Property Is a Strategic Asset," CSIS, June 25, 2025.
[2] Sujai Shivakumar, Charles Wessner, and Thomas Howell, Investing in Science and Technology (Washington, DC: CSIS, June 2024), https://www.csis.org/analysis/investing-science-and-technology.
[3] The President's FY26 budget proposal, released in May, requests a 22 percent cut to federal R&D funding, including a 36 percent decrease to non-defense R&D funding. The National Science Foundation (NSF) faces the steepest cuts at 56 percent, followed by the National Institutes of Health at 43 percent. Chris Borges, "Innovation Lightbulb: Visualizing Proposed Cuts to Federal R&D Funding," CSIS, July 17, 2025, https://www.csis.org/analysis/innovation-lightbulb-visualizing-proposed-cuts-federal-rd-funding.

Already, we are seeing warning signs, like universities cutting back PhD admissions and freezing research hiring.[4] Meanwhile, other countries are rapidly moving to poach U.S. talent by luring the country's best minds with offers of stable positions and serious funding.[5] And China's intensifying investment in new technologies, backed by aggressive trade policies, pose a generational challenge to the United States.[6] These majeures pose long-term risks to our global standing in innovation.

U.S. innovation leadership depends critically on our country's ability to invest in research, make new discoveries, and then bring them to market at competitive cost. When promising technologies aren't developed or can't reach scale because commercialization tools are underfunded, others will seize the opportunity.

In short, the investment and now qualitative challenge from China mean that we must reinforce key elements of our innovation ecosystem. To maintain our competitive leadership and national security, we must surge investment into our domestic R&D technology, including scale-up, workforce development, and advanced manufacturing, and ensure that the results of that research advantages U.S. security and everyday Americans.

My second key point is to affirm that the SBIR program is a proven national security asset that we must continue to strategically support and expand.

As someone who has directed multiple independent assessments of SBIR at the National Academies of Sciences and Engineering, I can affirm that the program is sound in concept and effective in practice. It is a low-profile but highly effective tool with an exceptional track record.[7] Around 70,000 patents and 700 public companies can trace their origins to SBIR-funded projects.[8] An independent study found that, across the entire U.S. economy, around 25 percent of *R&D Magazine*'s prestigious R&D 100 Awards in recent years went to SBIR-nurtured firms."[9]

SBIR has catalyzed the success of companies like Qualcomm, which have transformed our daily communications, and today continues to support breakthrough technologies including drones, next-generation reconnaissance, and missile propellants. In a time of intensifying technological competition, SBIR awards contribute directly to our economic growth, technological leadership, and defense capabilities.

---

[4] Deon Hampton, "Universities impose hiring freezes in face of uncertainty over federal funding," *NBC News*, March 10, 2025, https://www.nbcnews.com/news/us-news/universities-impose-hiring-freezes-face-uncertainty-federal-funding-rcna195697.

[5] Isobel Hamilton, "The poaching of American talent begins," *Politico*, April 28, 2025, https://www.politico.com/newsletters/digital-future-daily/2025/04/28/the-poaching-of-american-talent-begins-00313162.

[6] Sujai Shivakumar, Charles Wessner, and Thomas Howell, Investing in Science and Technology (Washington, DC: CSIS, June 2024), https://www.csis.org/analysis/investing-science-and-technology.

[7] Charles Wessner and Sujai Shivakumar, *Renew SBIR, Just Defend the Recipients Against China*, (Washington, DC: CSIS, September 2022), https://www.csis.org/analysis/renew-sbir-just-defend-recipients-against-china.

[8] Robert O'Shaughnessy, "Why Congress Should Reauthorize, Strengthen the SBIR Program," Federal News Network, April 18, 2022. https://federalnewsnetwork.com/commentary/2022/04/why-congress-should-reauthorize-strengthen-the-sbir-program/.

[9] Jay Lloyd, "Design Principles for American Industrial Policy," Issues in Science and Technology, April 26, 2021, https://issues.org/design-principles-american-industrial-policy-schrank/.

A highly effective partnership: SBIR is one of the most important and effective public-private partnerships in the country. Reflecting its success, it is currently one of the most emulated and extensively studied government R&D programs in the world.[10] It enables start-ups and small businesses to bridge the "Valley of Death," the gap between research or proof of concept and commercial production while allowing agencies like the Department of Defense (DOD) to procure cutting-edge innovations far faster than conventional Pentagon acquisition programs.

Like any ambitious endeavor, SBIR is not flawless. Not every idea succeeds if funded. But the program's value lies in its high-risk, high-reward nature. Think of it like basketball: you won't make every shot, but if you want to win the game you have to keep shooting. At its most modest, SBIR yields incremental improvements in mission-critical areas like defense, health, and energy. At its best, it shapes entire industries. When SBIR works, it can help transform whole sectors.

Our adversaries and competitors have recognized the value of the SBIR program for its proven outcomes and the technological leadership it has helped secure. The Department of Defense's 2021 internal report documenting efforts by state-sponsored Chinese firms targeting DOD SBIR companies merits serious attention. But let's be clear: if a competitor is stealing your playbook, it's probably because your playbook works.

To be sure, steps should be taken to defend small companies against cyberattacks and foreign efforts to acquire ownership or steal technology. SBIR supports small businesses that often lack the tools to protect themselves from espionage. These are firms without in-house counsel, threat intelligence, or cybersecurity teams. We cannot just focus on oversight but instead should provide active support for cybersecurity awareness and defense. In other words, our response should not be to shut down or weaken this successful program but to fortify it.

For SBIR to work, it needs to be stable and substantial yet flexible.

a) A strong program cannot thrive in a climate of fiscal and legislative uncertainty. Given SBIR's importance, we cannot subject it to whiplash in the budget process every few years. Without predictable funding and a stable policy environment, the program risks eroding trust and losing the very entrepreneurs it seeks to help.

b) We must also avoid overregulation. Some proposed reforms risk violating the dictum that "if it isn't broken, don't fix it." While in principle it is understandable to want to solicit more first-time applicants rather than deliver multiple awards to the same firm, in fact both those objectives can be met, with both new firms and proven firms receiving support. But more fundamentally, for a program run by program managers, micro-level legislative requirements are less effective than coordination and encouragement at the program manager level. Rather than legislate, why not first call up the managers and ask them why they are making multiple awards to a particular firm? And are multiple awards for a small company so different from multiple contracts for the big primes or multiple grants for well-performing universities? It is important to reinforce success and recognize the myth that just one award will beget one successful company for what it is.

[10] Gabrielle Athanasia, "RAI Explainer: the Small Business Innovation Research Program," CSIS, July 8, 2022, https://www.csis.org/blogs/perspectives-innovation/rai-explainer-small-business-innovation-research-program.

Furthermore, in sectors like quantum computing and communications, industries that are in the U.S. national security interest to grow, but where the community of capable inventors is relatively small, multiple awards may be a strategic necessity. This makes some companies ideal targets for multiple awards as this strategic industry begins to gain traction. Indeed, if anything, a forthcoming CSIS study suggests SBIR managers are underinvesting in quantum startups and early-stage companies.[11]

c) We need to strengthen and encourage the transition to commercialization. SBIR helps companies cross the Valley of Death in phase one and two, but in many cases, that bridge ends halfway. There are different paths to add an additional arch. Options include adding an active, agency-financed Phase III followed by a Phase IV, particularly for agencies without a procurement function, or drawing from the NSF model's Phase IIB which matches private capital investments up to a limit to encourage a smoother handoff to the private sector.

Most importantly, the SBIR program needs to be embedded in a strong innovation ecosystem. To truly protect and leverage SBIR technologies and their national security benefits, we must surge investment into domestic technology ecosystems and absorptive capacity, including scale-up, workforce development, and advanced manufacturing.[12] To stay ahead, we must not only double down on our R&D investments but also reinforce programs that enable our firms to commercialize these new technologies. SBIR plays a unique and vital role in that equation, enabling the contributions of our research enterprise to grow security-enhancing technologies, as well as clusters for new technologies around the communities that need them most. It is also noteworthy that given how SBIR programs are funded, current plans to significantly cut agency R&D budgets necessarily mean cuts to the SBIR budget, limiting the program's ability to capitalize on previous national investments in R&D.

In conclusion, **innovation without commercialization is a lost opportunity, and, in a world of accelerating competition, a potential gift to our adversaries**. SBIR works. But it must be buttressed with cybersecurity support, flexible follow-on funding to facilitate commercialization, and programmatic stability. Most importantly, it must remain embedded within a **strong innovation ecosystem—one that is supported by sustained and substantial investment in our federal R&D agencies and research institutions**. Let us not forget: the future is not waiting. We have the ideas; let's reinforce and keep building.

Thank you, and I look forward to your questions.

---

[11] Forthcoming research at CSIS found that from 2015 through 2023, DOE, NASA, HHS, NSF, and Commerce awarded just 4.5, 2.6, 0.7, 1.6, and 1.9 percent of their total SBIR grant funds to quantum-related projects, respectively. 362 companies received SBIR 862 awards, an average of 2.4 per firm; five firms, representing fewer than 1 percent of the total, received 96 (11.1 percent) of the awards.

[12] Sujai Shivakumar and Julie Heng, "Renewing the United States' Skilled Technical Workforce," CSIS, July 9, 2025, https://www.csis.org/analysis/renewing-united-states-skilled-technical-workforce; Sujai Shivakumar, *Priming the Innovation System: A New Age of U.S. Industrial Policy*, (Washington, DC: CSIS, September 2023), https://www.csis.org/analysis/priming-innovation-system.

Senator HAWLEY. Thank you very much. Dr. Hannas, you're recognized for five minutes for your testimony. The floor is yours.

STATEMENT OF DR. WILLIAM HANNAS, LEAD ANALYST AND RESEARCH PROFESSOR, GEORGETOWN UNIVERSITY'S CENTER FOR SECURITY AND EMERGING TECHNOLOGY, RESTON, VIRGINIA

Dr. HANNAS. Thank you, Chair, Ranking Member Markey, distinguished members of the committee and staff. I'm grateful for the opportunity to testify on this topic.

I'm a founding member of Georgetown University's Center for Security and Emerging Technology, where I track Chinese threats, technology threats posed by China. Prior to that, I was a senior intelligence service officer at CIA, managing the same portfolio. These efforts led to two books on Chinese industrial espionage in 2013 and 2021 into other studies on the topic.

My interest in Chinese foreign tech transfer began as a graduate student preparing a thesis on China's cultural predisposition for holistic thought, which has served China well in practical terms, but hinders progress in basic science that has plagued China's since antiquity. I bring this up to emphasize that China's reliance on foreign ideas has historical roots not easily overcome.

Another factor that drew me to the topic was the discovery that China treats foreign technology acquisition as an academic discipline. Kējì qìngbào, literally "S&T Intelligence", on a par with other scientific fields, replete with degree programs, how-to manuals, academic journals, and career positions supported by legislation and an army, some 100,000 S&T intelligence operatives. That's the term they use.

So, the notion that China's informal transfer of foreign technology is done by opportunistic individuals is pure myth. This is a state-backed soup-to-nuts system that has been running at the central government's direction since the 1950s and is not abating, even as China's indigenous accomplishments grow.

It's impossible to condense volumes of research into five minutes, but here are the basics. China uses three types of transfer practices; legal, illegal, and extra-legal. Illegal transfers run from insider operations, patent infringement, reverse engineering, to the hacking and clandestine exploits we read about in the press. These tech espionage cases are so numerous that the ODNI issues two annual reports, one for China and one for the rest of the world.

Legal transfers done through China's U.S.-based subsidiaries, startup accelerators, targeted hires, direct and indirect investment, mergers and acquisitions, and tech-for-trade agreements are easy to spot, but hard to counter because U.S. participants and oversight officials often confuse legal with "in the U.S. interest."

Finally, there are a dozen categories of extra-legal venues that China uses, including front organizations for deniability, paid short-term visits to state debriefing centers, overseas technical support, guilds, online recruiting, and of course, China's human talent recruitment programs.

In a 2023 book on artificial intelligence, we gave examples of U.S. firms in China including Microsoft, Intel, and IBM, working with China on AI development and credited by the Chinese alumni

of the programs as critical to China's success. In the same book we named 10 types of venues used to effect transfers from foreign academics such as school-to-school "partnerships", co-authorship, and a practice called "using foreigners to draw in foreigners".

These practices threaten U.S. businesses large and small, the lateral especially vulnerable, owing to a scarcity of research funds and investment capital, shrinking talent pools, fewer opportunities to commercialize breakthroughs, inadequate due diligence, and limited venues for redress.

So, what can be done? First, we must appreciate that the reason this is a problem at all is because our lead has shrunk to the point where theft matters. Whereas before we're so far ahead, it didn't matter. Rebuilding U.S. research, entrepreneurship, and productive capacity independently of whatever China is doing or stealing is the only sure way out.

Meanwhile, we propose five common sense measures; Data on China's transfer practices should be gathered and shared with U.S. firms and academic compliance offices. Two, clear guidelines of what is legally permissible should be communicated to foreign actors contemplating research in the United States and the U.S. persons doing research, doing business in China.

Three, members of China's overseas support guilds, talent recruitment programs, lobbying groups, and other united front operatives should register as foreign agents. Four, recipients of U.S. government funding should report contacts with or travel to China to minimize China's ability to benefit from U.S. federal and state level investment. Finally, there are opportunities for U.S. authorities to stand China's transfer apparatus on its head. By seeding these venues with persons disposed to support U.S. interests.

We're past the point where this problem can be ignored. The gap between tech breakthroughs and consequences is measured now in weeks, which puts a premium on keeping what we invent. Thank you for this opportunity to address this issue.

[The prepared statement of Dr. Hannas follows.]

Testimony before the U.S. Senate Committee on Small Business & Entrepreneurship
on
"Innovation in the Crosshairs: Countering China's Industrial Espionage"

William C. Hannas
Research Professor and Lead Analyst
Center for Security and Emerging Technology, Georgetown University
July 23, 2025

Chair Ernst, Ranking Member Markey, distinguished members of the Committee and staff, I am grateful for the opportunity to testify on this topic.

I am a founding member of Georgetown University's Center for Security and Emerging Technology, where I track technology threats posed by China. Prior to that, I was a Senior Intelligence Service officer at CIA managing the same portfolio. These efforts led to two books on Chinese industrial espionage in 2013[1] and 2021[2] and to other studies on the topic.

My interest in Chinese foreign tech transfer began as a graduate student preparing a thesis on China's cultural predisposition for holistic thought, which has served China well in practical terms but hinders progress in basic science—and has plagued China since antiquity. I bring this up to emphasize that China's reliance on foreign ideas has historical roots not easily overcome.

Another factor that drew me to the topic was the discovery that China treats foreign technology acquisition as an academic discipline—科技情报学 or "S&T intelligence study"—on a par with other scientific fields, replete with degree programs, how-to manuals, academic journals, and career positions, supported by legislation and some 100,000 "S&T intelligence operatives."[3]

So, the notion that China's "informal" transfer of foreign technology is done by opportunistic individuals is pure myth. This is a state-backed, soup-to-nuts system that has been running at the central government's direction since the 1950s and is not abating, even as China's indigenous accomplishments grow.[4]

---

[1] William C. Hannas, James Mulvenon, and Anna Puglisi, *Chinese Industrial Espionage*. (New York and London: Routledge, 2013).
[2] William C. Hannas and Didi Kirsten Tatlow, eds. *Beyond Espionage: China's Quest for Foreign Technology* (New York and London: Routledge, 2021).
[3] William C. Hannas and Huey-Meei Chang, "China's STI Operations: Monitoring Foreign Science and Technology through Open Sources," Center for Security and Emerging Technology, January 2021, https://cset.georgetown.edu/publication/chinas-sti-operations/.
[4] Ibid.

It's impossible to condense volumes of research into five minutes but here are the basics: China uses three types of transfer practices: legal, illegal, and extralegal—the last category so named because they occur without supervision and their legality is unknown.

Illegal transfers run from insider operations, patent infringement, and reverse engineering to the hacking and clandestine exploits we read about in the press. China tech espionage cases are so numerous that ODNI issues two annual reports: one on China, and one on the rest of the world. Noteworthy examples include next-generation battery technology, composites for jet engines, and self-driving technology.

Legal transfers done through China-based U.S. subsidiaries, start-up accelerators, targeted hires, direct and indirect investment, mergers and acquisitions, and tech-for-trade agreements are easy to spot but hard to counter because U.S. participants and oversight officials often confuse "legal" with "in the U.S. interest."

Finally, there are a dozen *categories* of "extralegal" venues that China uses, including front organizations for deniability, paid short-term visits to state debriefing centers, overseas technical support guilds, online recruiting and, of course, China's human talent recruitment programs.

In a 2023 book on artificial intelligence[5] we gave examples of U.S. tech firms in China, such as Microsoft, Intel, and IBM, working with China on AI development and credited by alumni of the programs as critical to China's success. In the same book, we named ten *types* of venues used to effect transfers from foreign academics, such as school-to-school "partnerships," co-authorship, and a practice called "using foreigners to draw in foreigners" (以洋引洋).

These practices threaten U.S. businesses large and small. The latter are especially vulnerable owing to a scarcity of research funds and investment capital, shrinking talent pools, fewer opportunities to commercialize breakthroughs, inadequate due diligence, and limited venues for redress. The impact on our proprietary technology, while not quantifiable, is obvious from the importance China attaches to this exploitative enterprise—acknowledged by Chinese scientists, policymakers, and business entrepreneurs.

So, what can be done? First, we must appreciate that the reason this is a problem at all is because our lead has shrunk to the point where theft matters, whereas before we were so far ahead it didn't matter. Rebuilding U.S. research, entrepreneurship and productive capacity—independently of whatever China is doing or stealing—is the only sure way out.

Meanwhile, we propose five commonsense measures.[6] They are:

---

[5] William C. Hannas and Huey-Meei Chang, eds., *Chinese Power and Artificial Intelligence*, (New York and London: Routledge, 2023).

[6] See William C. Hannas and Huey-Meei Chang, "Unwanted Foreign Transfers of U.S. Technology: Proposed Prevention Strategies." Center for Security and Emerging Technology, September 10, 2021, for a more complete list. https://cset.georgetown.edu/article/unwanted-foreign-transfers-of-u-s-technology-proposed-prevention-strategies/.

1. Data on China's transfer practices should be gathered and shared with U.S. firms and academic compliance offices. Persistent, dedicated efforts are needed to track China's activities as they evolve and change to evade the sunlight.

2. Clear guidelines on what is legally permissible should be communicated to foreign actors contemplating research in the United States, and to U.S. persons doing business in China.

3. Members of China's overseas support guilds, talent recruitment programs, lobbying groups, and other United Front operatives should register as foreign agents.

4. Recipients of U.S. government funding should report contacts with or travel to China to minimize China's ability to benefit from U.S. federal and state-level investment.

5. Finally, there are opportunities for U.S. authorities to stand China's transfer apparatus on its head by seeding these venues with persons disposed to support U.S. interests.

We are past the point where this problem can be ignored. The gap between tech breakthroughs and consequences is measured now in weeks, which puts a premium on keeping what we invent.

Thank you for the opportunity to address this important issue.

Wm. C. Hannas
Professor
Georgetown University

CHAIR [presiding]. Thank you very much for your testimony. And we will now go into our question answer period, and each member will have five minutes.

I now recognize myself for five minutes of questions, and Ms. de La Bruyère, let's start with you. I was a proud leader in the creation of a new foreign ties due diligence process for SBIR in 2022. My INNOVATE Act would create a clear and consistent definition of foreign risk to improve agency's analysis of adversarial threats.

Which methods does China most commonly use to exploit technology of innovative startups, and how can we best restrict the flow of those taxpayer dollars to compromised entities?

Ms. DE LA BRUYÈRE. Thank you for that question. I obviously can't answer without first prefacing that China has an immense arsenal and it's adaptive. So, when we put up protections, China tends to find or try to find ways around them. That said, common methods include first investment, including both directly via Chinese companies and funds, and indirectly as, for example, limited partners in U.S. funds.

Second, China uses both customer and supply relationships as well as the information-sharing at those create, and personnel including as have been mentioned; talent programs, talent poaching, and embedding of personnel.

Protecting against this requires top-down measures from Washington, and also, expectations put on companies that are receiving federal funding. From the top down, U.S. restrictions on Chinese investment and presence in the U.S. should be strengthened. For instance, CFIUS should be strengthened to respond to China's indirect investment methods as well as direct directed ones.

But also, federal funding mechanisms like the SBIR program should include due diligence requirements. And those due diligence requirements have to be best-in-class, and they have to be updated for the realities of China's adaptive and indirect ways or means.

It's not enough to say what's first-level ownership or what are direct investments coming into a funded entity. It's also not enough to say just what are its first-tier customers. Due diligence has to look at the indirect investments. It has to look for instance at customer as well as tiered-down suppliers.

And due diligence processes have to be adaptive or proactive so that they're looking at what China's going to be doing next, not what it's already doing. These should be the case. They're largely not in the due diligence approaches and ecosystems that exist. So, that has to change.

And then also from the bottom up, companies that are receiving federal funding should be expected to be doing and refreshing their due diligence throughout their lifespans. So, that should include looking at who they're taking money for and really vetting that for Chinese ties, who they're supplying to, who their customers are, who their partners are.

There should be no entity whether a research university or a two-person startup in a garage that's getting U.S. federal funding that's also partnering with Chinese entities. And that should be fundamental and the penalties should include clawbacks because there has to be an actual risk in there.

CHAIR. No, thank you. And that was very good. A lot of solutions just in that one answer, so I appreciate that. Dr. Hannas, in your testimony you discuss how U.S. oversight officials often confuse legal with "in the U.S. interest."

Can you elaborate further on how to get our federal officials to stop awarding taxpayer-funded grants and contracts to companies that have clear ties to CCP espionage?

Dr. HANNAS. Simply said, but hard to implement. You need data and access to the data. Let me share a war story. Some years ago, I was part of a team reviewing bids of a large U.S. government contract. We had necked down some 200 bidders to a dozen and rank-ordered them.

And by a pure chance, I noticed that one of the one of the companies which was in the top rank was pitching a professor at a U.S. engineering college, whom I remembered as a China talent program member who wrote software for China's bio industry. So, we drew the money line just above that company.

This is not the way to operate. The event should have happened by design, not luck. It's entirely possible for the U.S. government to build detailed lists of persons and venues affiliated with China's technology transfer programs against which grant proposals can be vetted. In fact, we spearheaded a pilot a few years ago that enjoyed some success, but access was restricted. It was limited, which didn't do corporate America much good.

CHAIR. And thank you for that. It's a clear demonstration of why my INNOVATE Act strengthens the denial authority and provides clarity to our program managers that they can't move forward with awards if there are clear threats out there. So, I really do appreciate it. We will go next to a Ranking Member Markey for his questions.

Senator MARKEY. Thank you, Madam Chair. Dr. Shivakumar, as you know, the Small Business Innovation Research and the Small Business Technology Transfer programs will expire in just over two months. And these programs have played an essential role in driving our country's innovation, resulting in at least 70,000 patents in 700 public companies. Since its inception in 1982, the program has resulted in more than 207,000 awards, totaling more than $72 billion, and you are one of the few researchers. Was that extensive analysis of these programs?

So, could you speak, Doctor, to how multiple award winners are important to the growth of certain industries, and could you provide an example of a technology that would not exist without multiple award winners?

Dr. SHIVAKUMAR. Certainly. Well, I was just last month in Colorado looking at the emergence of a quantum innovation cluster in the Mountain West region. There are a number of SBIR companies among those, and they are a limited number.

So, if you think about the need to actually grow our quantum industry, and if you think of the particular solicitations, there are only going to be a limited number of these companies that can respond to any particular solicitation.

So, the idea of those companies will build—well, by nature need to garner multiple awards in order to build scale and to grow the industry in that region. So, it's not just there are concerns about

whether there are, is there is a problem with multiple award winners, people coming you know, gaming the system.

There are cases to be made where multiple award winners are actually important to our national security, if we need to build up our quantum industry, for example. On the other hand, we have program managers at the various agencies who are best positioned to actually monitor any abuse of the program by gaming the system to get multiple awards.

My recommendation is for the Senate or the Congress to sort of manage the program from here, but provide the program managers the resources and the confidence to actually manage their programs. If there are problems, let them document the award. If there are——

Senator MARKEY. Let me ask. Could you speak to the impact of the 2022 due diligence program in protecting our SBIR and STTR program?

Dr. SHIVAKUMAR. So, I think there is obviously an important aspect in protecting our IP, but there's also the consideration that it's a global race now in terms of innovation. There are multiple countries in the world, including China, that have strong innovation systems.

And as you know, the old football saying, you can't win purely on defense. You need a very strong offense, which means that we need to supercharge our innovation system, by making sure that our universities churn out, our research institutions churn out new ideas by making sure that programs like SBIR take those ideas and bring them into businesses, build prototypes, get them ready for the market.

And then to, scale those technologies further up so that we can be competitive internationally while also you know, creating new opportunities for Americans. So, yes, we need to defend, but I think we need to look at both sides of that equation as well. We need to have a strong offense in terms of a very vibrant innovation system.

Senator MARKEY. Yes. And that strong offense would be not cutting the National Institutes of Health, not cutting investment in batteries and solar, and not cutting investment in the National Science Foundation, investing in our young people to compete.

Here's a headline from just last week, "China puts new restrictions on EV battery manufacturing technology." Now that they've made the breakthrough, now that there are companies like BYD, build your dreams, way ahead of Ford and General Motors, and way ahead of Tesla, they're now going to put restrictions on the transfer of any of their battery technology around the world.

Then they invited us in, but their condition was we have to share our technology with them. Now that they're sprinting ahead, they're going to put restrictions on. So, it looks like they were playing us for Uncle Sucker the whole way. And we just have to be realistic about it. But the way to respond is not to cut our research in these critical areas. There's going to be 20 million all electric vehicles sold around the world this year. We only sell 17 million total vehicles in the United States each year. And so, we're seeding the future.

Basically, what China is doing is putting up the walls to protect, not just against us, but anyone else now being able to compete ef-

fectively with them in the marketplace. And we just have to be ruthlessly realistic about that reality. Thank you, Madam Chair.

CHAIR. Okay. Thank you, Ranking Member. And Senator Curtis, you're recognized for five minutes.

Senator CURTIS. Thank you, Madam Chair. I'm really proud to represent Utah. Like some of my colleagues, Utah represents 99 percent small businesses. And this is just a really important committee and topic, it's the lifeblood of our state.

Utah's a major entrepreneurial hub for innovation as well. A lot of our businesses have seen their intellectually property stolen, and Chinese entities frequently copycat their products. They see them on places like TEMU and other things like that. I'm actually convinced that our small businesses have a disproportionate burden here because they don't have compliance officers, they don't have layers of lawyers and accountants.

So, I guess my question for all three of you is, how vulnerable are our startups specifically to this Chinese espionage and are there specific industries that are more at risk? Please.

Ms. DE LA BRUYÈRE. The short answer is highly vulnerable, and not only because of the resource constraints that small businesses face, but also because of the dearth of resource constraints that Chinese entities face. The way Beijing positions in the international commercial ecosystem is to state-led enterprise driven approach, where Chinese agents' companies go out, they have state backing and direction, and that means that they're not bound by market forces. Which lets them reap strategic advantage off of entities that are bound by economic logics, especially those like small businesses that have serious resource constraints.

And ways Beijing does this include, targeting distress companies, companies on the verge of or after bankruptcy, ones that really need to raise investment rounds and will take investment from anyone that's willing to give them money, in short that have strategic value, but aren't necessarily on a commercial trajectory, or one that gives them the freedom to choose between long-term strategic interests for them or the country and Beijing.

And that's a massive difficulty, and you can't solve that without having restrictions on China's role and the role of Chinese entities in the U.S. system.

Senator CURTIS. Thank you.

Dr. HANNAS. So, I made some notes on that point, and yes, indeed, they are especially vulnerable small businesses for a number of reasons. You know, one being the scarcity research funds and investment capital. So, it's not available here, so they look at China, even if they they're not looking at China, shrinking talent pools, plenty of talent available through China's diaspora community. But less and less, within the indigenous American population, fewer opportunities, and commercialized breakthroughs. That's big.

They have discoveries, how do they bring it to market? Not easily done. And it was pointed out, inadequate due diligence. They don't have the wherewithal to determine, who are friendlies and who are not. And finally limited venues for redress. You discover something that you're an agreed party to an agreement, and what do you do about it? Very little you can do about it as a small business. So, yes, they are very vulnerable.

Senator CURTIS. The FBI said that China is "the world's principal infringer of intellectual property," and that it uses laws and regulations to put foreign companies at a disadvantage and its own companies at an advantage.

Earlier this year, I introduced the Combating China's Pilfering of Intellectual Property, CCP IP Act, which holds China accountable for stealing American ideas. This bill would enforce sanctions and visa restrictions on Chinese officials and citizens engaged in intellectual property.

Can any of you walk us through how intellectual property threat, transfers into long-term economic or national security losses for the United States? Go ahead.

Ms. DE LA BRUYÈRE. I think to answer that question, you fundamentally go back to what China's trying to do with intellectual property. Beijing's not just developing cutting edge technology, Beijing is stealing cutting edge technology and then focusing on its application. So, the commercial and the industrial returns that come from that.

And Beijing is like doing that for two primary objectives. One is to control international supply chains. If you control batteries, were mentioned, for instance, the global battery market, you control automobiles, and also you make sure that the U.S. depends on you, which gives you leverage in economic and geopolitical environments.

And second, perhaps most importantly, offensively Beijing's working to build and to scale the global infrastructure for a new technological environment in information technology. For instance, a unified information network that collects all data and transmits all data. And if Beijing is able to do that, and it's directly applying technology to this end, then Beijing can control how markets work, how military work, how people perceive.

Senator CURTIS. Thank you. I'm sadly out of time. Appreciate your expertise, and I yield back.

CHAIR. Senator Shaheen.

Senator SHAHEEN. Thank you, Madam Chair. And thank you to each of our witnesses for your testimony today. I have to say, I agree with the premise that each of you have outlined about the threat that China poses to our innovation and the importance of the SBIR program, and reauthorizing it in ensuring that we continue to innovate.

I just want to point out that last week, the minority on the Foreign Relations Committee issued a report on China that talks about the threat from China and the decisions that have been made in the first six months of this administration, that seed America's leadership in a whole range of issues.

And one of the report's findings highlighted how America's withdrawal from international organizations, seeds influence to China, which in response, has increased its contributions and personnel across a whole range of international bodies. And by proposing a near zeroing out of U.S. contributions to international organizations like the World Intellectual Property Organization, WIPO, the administration risks allowing China to be the dominant voice and international discussions about the future of IP protections, including patents, copyrights, and trademarks.

So, I would ask each of you how America's small businesses benefit from participation in international bodies like the World Intellectual Property Organization. One of my favorite statistics about small businesses, that they create 16 times more patents than large businesses. So, what happens around the IP protections that you all have outlined is critical. So why is it important that the United States participate in those kinds of bodies that provide those protections for our small businesses?

Dr. SHIVAKUMAR. So, you know, there's interesting quote from Chinese leader who said that, the country that controls the standards and patents, controls the world. And they understand that very well, and they have a natural strategy, a 2035 strategy to be a world leader in setting the standards.

If you think about standards, in many respects, they're like language. They set the grammar, they set the vocabulary, the idiom, and the country that sets, you know, is in control of the language, controls the dialogue, controls the thought, controls the innovation in the sphere. So, it's extremely important that the United States, which has long dominated the standard setting environment, the institutions, sort of wake up and reassert itself. It's sort of, we have been in the lead for so long, like the proverbial story or the rabbit and the hare, we have sort of taken a nap.

And so, the relevant agencies need to be prodded, hopefully from here, and to sort of take a leadership and make sure that we are ably represented, that the people who are in these standard setting organizations are trained and that we take a much more active, proactive role in the IP. We have a very strong still in our innovation system research IP. We are an IP machine in many ways, but we need to also have standards you know, part of that equation to make sure that our ideas are dominant, and that we have that advantage of being the standard setters.

Senator SHAHEEN. So, if we don't pay our dues to WIPO the end of this year, we run the risk of not being able to participate again. And what kind of a disadvantage does that put the United States businesses in, if that happens?

Dr. SHIVAKUMAR. Well, if somebody else is writing the rules by which you have to play, that certainly puts you at a disadvantage. So, that's not a situation where you want to be.

Senator SHAHEEN. Thank you. Yes.

Ms. DE LA BRUYÈRE. If I may add, I think one of the underestimated risks of China's approach is that Beijing has co-opted international organizations, including and especially standard setting organizations, intellectual property organizations. And Beijing does so with the benefits of its centralization and scale. That means that even an activated U.S. approach to those organizations doesn't have any hope.

China floods the ITU with members who are paid, they've predecided what standards they're going to form, which means that just by engaging in these standards, in these organizations, the U.S. will be at a disadvantage.

So, the hope that the U.S. can claim is by extracting China from a system that has manipulated and restoring its integrity, such that activities go in a way that follows their actual rules and intent.

Senator SHAHEEN. But if we're not at the table, how are we going to extract China and how are we going to hope to compete, if we're not even there?

Ms. DE LA BRUYÈRE. We need to establish organizations that don't have China in them or find ways like——

Senator SHAHEEN. But again, how do we do that if we're not there to address the rules of those organizations and to establish that ability to make sure that China doesn't participate?

Ms. DE LA BRUYÈRE. You don't have to be part of an organization to launch a new one.

Senator SHAHEEN. Are we in the process of doing that?

Ms. DE LA BRUYÈRE. I think that the most strategically significant move with international organizations the U.S. could make right now, would be to revoke China's permanent normal trade relations status. It's a world trade organization move, not a WIPO——

Senator SHAHEEN. I wouldn't disagree with that at all. I think that that is not a bad move.

Ms. DE LA BRUYÈRE. And then that could have trickle down effects throughout other organizations that Beijing has co-opted.

CHAIR. Very good. Thank you. That'll be our next project. So, thank you. I recognize Senator Young for five minutes.

Senator YOUNG. Thank you, Chair. As chairman of the National Security Council on Emerging Biotechnology, I have dedicated a significant amount of effort on the topic of making sure that we have a vibrant small business sector that can commercialize the many innovations we make in this country.

And one of the key recommendations we have in that report is the urgent need to mobilize the private sector by enhancing the reach and the effectiveness of the Small Business Innovation Research and Small Business Technology Transfer programs. These programs are essential for advancing early-stage innovation and scaling U.S. technologies. They are proven; they have been bipartisan but we think they certainly can be improved.

Mr. Hannas, you've been closely involved with the NSCEB, thank you for your assistance. You helped us shape recommendations. From your perspective, how critical is it that we emphasize and incentivize the commercialization of emerging technologies? Just touch again on that, but as importantly, how much your recommendation to make China's united front operatives register as foreign agents help advance that cause?

Dr. HANNAS. Yes, so the first point. I mean, this is where China excels in commercializing technology. They never set the world on fire in coming up with abstract indigenous theoretical discoveries. But what they do exceptionally well is commercialize what anybody in the world finds. We seem to have exported or lost that ability to commercialize. And there was a time when we could get along okay with royalties from patents, for inventions that we created. But those days are gone, need to commercialize.

And here we might draw a lesson for once from China, something they're doing. I was kind of shocked to discovered a few years ago that they have what are called commercialization centers, which are anything from a storefront with two people in it, two acres wide, and stories tall complexes, that exist solely for the purpose

of commercializing technology, both foreign and indigenous. They don't discriminate.

If it's technology, they'll commercialize getting it to market and or weaponizing it, before anybody else does. I don't know that we have anything like that. And I think we might be able to learn a lesson from that. And your second question, Senator?

Senator YOUNG. If you could very briefly, because I have limited time, but just touch on your recommendation pertaining to making China's united front operatives register as foreign agents.

Dr. HANNAS. Well, clearly, they are. No one's held their feet to the fire to this extent. And again, it goes back to data. We need to understand what groups of people are involved. We already do understand that at a certain level, but we need to get this information into a database where it's scrutinized and made available to other people who can make these analytic judgements, and execute these decisions that we make in determining who are actually China's unpaid actors, China's influence operators. It's not done; it's hit and miss.

Senator YOUNG. You know, it seems to me a sports analogy is applicable here, a good defense is also a good offense, right? In this case, if we cut down on the theft of intellectual property, we leave it to our own market, our own investors, and entrepreneurs. If we up our game with respect to commercialization, to deploy whatever business model they think appropriate, to take advantage of those breakthroughs, creates jobs and prosperity and helps our national security. So, I think the two are very much linked.

Ms. DE LA BRUYÈRE, I'm sorry if I butchered your name. How can we better ensure sustained U.S. leadership in the development and deployment of emerging tech through your proposal to prohibit certain businesses from eligibility for federal procurement, if they run afoul of any of the prescriptions that you suggest; data research, procurement, localization, investment in Chinese entities, how would that work?

Ms. DE LA BRUYÈRE. That starts with defense, right? Part of that is then we're trying to defend our technology from China's access.

Senator YOUNG. Yes.

Ms. DE LA BRUYÈRE. Perhaps more important than that, because fundamentally defensible only works so well against China, is that moves like that, send a message to the private sector, and they tell the private sector that you have to make a choice between the U.S. market and between China. And also, that you can profit from investing in America and investment in the U.S. encountering of China can be a profitable thesis.

The U.S.' greatest strength is our private sector, but that has to be what's activated for the contest against China. We can't just have the government impose restrictions and think that that will work. So moves that force a choice, and make U.S government support contingent on a competitive approach to China, send a signal to the private sector.

Senator YOUNG. Thank you. I'm out of time. Dr. Shivakumar, good to see you. I've enjoyed our work together. Chair.

CHAIR. Yes, thank you, Senator Young. Senator Justice, you're recognized.

Senator JUSTICE. Thank you, Madam Chair, and Ranking Member, and all these wonderful witnesses. And I'm not going to attempt to butcher your last names, there's no way. So, for me, we're going to go with Emily, Doc 1, Doc 2. Okay.

So, let me just start off by making a little bit of a statement, because I've got a lot of white hair. I'm a new kid on the block; I came here for the right reasons and period. I don't want anything. I don't want a thing in the world for me. But with all that being said, I can't for the life of me understand why all the smarts around this table, all the smarts here, all the smarts back there, why we can't just realize where we are.

I mean, we have known forever and a day what China's doing, and we haven't done anything about it. And America believes that no matter what in the world happens, and I'm a believer too, no matter what in the world happens, it's all going to be great. And we can go to Wendy's and get Baby Dog chicken nuggets this afternoon, and we know we can't.

But now, just think about this just for a second, and let me just take you back just in time. Jimmy Carter was the President. We'd given away the Panama Canal, we had interest rates and inflation rates at levels that nobody could ever fathom. We had gasoline lines; we had a hundred hostages in Iran, the Soviet Union was running so strong, it was unbelievable. And to be perfectly honest, a lot of us were afraid. At that point in time, who could have ever dreamed that the Soviet Union could stumble?

And then all of a sudden, we elected Ronald Reagan. And just in a very, very, very short period, almost no time, Ronald Reagan was standing in front of the Berlin Wall saying, Gorbachev, tear down this wall, and the Soviet Union collapsed. Why do we not believe and move with the light speed that we should be moving with, that it could happen to us. And it can.

We're right on the cusp right now of needing energy like you can imagine. Absolutely, we're going to have to decide between homes and industry, if we don't really get moving now. So why in the world does the smarts of this room that is unbelievable, not solve the problem? We've got to solve the problem.

I mean, for God's sakes of living, I mean, if in Madam Chairman's home state, if people are out digging up seeds, and stealing our technology of how we grow these phenomenal crops that yield beyond belief, and I'm a farmer too, you know, what will they not do? What in the world will they not do?

So, all I can say to you is just this, to the small business folks, and my only question would be just this that's already been asked 14 times, how do you protect them? They don't have a host of accountants or lawyers or whatever it may be, or advisors. How do you protect them? And literally, for all of us, a lot of y'all are really young and don't have white hair, but it'll probably happen to you sometime. I was skinny and had brown hair for a long time, and now look.

But anyway, all that being said, absolutely, we have got to solve the problem. We got to solve the problem right now. How do you protect the small businesses? Let's go with Emily, Doc 1, Doc 2, go very quickly. I've only got a minute, and I've said exactly how I feel. But at the end of the day, come on guys, come on. All of us

got to pull the rope together. We have everything at stake. It's not time to be Democrats and Republicans. It's time for all of us to pull this rope together. Emily, please.

Ms. DE LA BRUYÈRE. We remove China from our market, and we incentivize companies not just to develop research but to produce.

Senator JUSTICE. Doc 1.

Dr. SHIVAKUMAR. SBIR is a huge asset that have to accelerate technologies using our small businesses. We need to arm them with the wherewithal, the resources to inoculate themselves and to be aware so that they're not susceptible to this sort of theft.

Senator JUSTICE. Doc 2.

Dr. HANNAS. Level the playing field, so China can't continue to do what it has been doing.

Senator JUSTICE. A hundred percent right. Madam Chair, I'd defer my three, five seconds. Oh, I'm overtime. [Laughter.]

CHAIR. Thank you, Senator Justice. And thanks for bringing up the Chinese theft of seeds in Iowa. That happened in 2013, I believe, and they were sentenced in 2016. But yes, it does happen. They steal our intellectual property and reverse engineer. So, we will next go to Senator Husted for five minutes. Thank you.

Senator HUSTED. Thank you, Madam Chair. Thanks to the witnesses for joining us today. Complicated issue it seems in listening to you, and from the work that I've done in my life, it seems like we've got a situation where our freedom is being used against us. We allow Chinese students to study in our universities, not many times, but sometimes to our detriment, stealing intellectual property, our ideas, outright espionage.

Anytime a small business sells into the Chinese market, I don't know how many times I've talked to a small business, said look, I was selling it. Next thing I know they're selling it. They stole my IP. I have no recourse in their courts. They have recourse though in our courts. We give their businesses the same protections we give our businesses, but yet, that's not reciprocated.

Not to mention some of their advances clearly have also come from stealing technologies from other nations, from other innovations that go there. And I know in talking to small businesses since the tariff issue has come up, that they say —well a lot of times they say, well, I don't necessarily like them, however, it's about time somebody stands up and protects me from what's going on when I try to sell into China, and what they sell into our country and other countries.

I'll ask each of you to comment on what recommendations would you make to the Trump administration as they're looking at the issue of trade with China, and how can we use our trade relationship or the bilateral conversations that are happening, to address some of the issues you've discussed today? Dr. Hannas, we can start with you and go down the line.

Dr. HANNAS. Again, my apologies. I'm not good at solutions. But there is one point that needs to be brought up that is germane I think to your question, and we didn't touch on it enough before. This is not solely a U.S. problem. You know, China does not discriminate among the countries that it exploits. Our book on Chinese industrial espionage, which it was translated in two lan-

guages, guess which two? Japanese and Korean. Because they're suffering the same problems we are.

So, one of the things we can do is align ourselves with our allies who are suffering from the same depredations and come up with a common front against the problem. That would be my major recommendation.

Senator HUSTED. Okay. Thank you.

Dr. SHIVAKUMAR. Challenge system research, a fantastic entrepreneurial culture, but the scale up part of our innovation system infrastructure has eroded over a number of years. We need to rebuild that so that we are the ones who are first and foremost absorbing the IP that's coming out of our research universities faster than anybody else in the world.

Senator HUSTED. And what do you think the barriers are to that? Because we have a lot of capital in this country. What is the barrier, why aren't we scaling it up?

Dr. SHIVAKUMAR. Well, it's a sort of—we have basically hollowed out our manufacturing sector. So as a result, our ecosystem is incomplete. The Chinese have large state-owned enterprises. They have deep pockets. They're able to take ideas and scale them up. And we are kind of weak in that area. So, what we need to do is actually rebuild our innovation system so that it's the most competitive in the world. Go back to when it was.

Senator HUSTED. It's very capital intensive to established.

Dr. SHIVAKUMAR. It's capital intensive. It requires a lot of coordination across. It requires a strong—it's a multifaceted innovation system. It has worker training aspects to it; it has capital markets aspect to it. It has research and development aspects to it. All of these parts of the innovation system have to all work together independently as well as connect with each other.

In fact, one of the advantages of the SBIR program is actually, it takes ideas that may be formed at a university lab, but the venture capitalist doesn't know whether it's a great idea. And so, by creating you know, a two-phase validation of the commercial potential and the technological potential of the technology, it basically flags to venture capitalists, our deep capital markets, that this is an idea that you need to invest in that helps to bring the technology partway across——

Senator HUSTED. Well, our financial systems like sherbets, not speculative well——

Dr. SHIVAKUMAR. Well, the financial system, it's a market. And like any market, it works well when there's lots more information. And this is what SBIR does.

Senator HUSTED. Give chance for our last guest.

Ms. DE LA BRUYÈRE. I'll be sure on the trade front; we need to stop assuming that China's going to play by the rules or will ever compromise. And we should levy significantly higher tariffs on China. We should encourage our allies and partners to do the same, but with a coherent message that says that the international free trade system works. We should all be part of it, but not let China abuse it.

And then we should accept that a message to the American people, that all this will come at a cost in the short term, but that cost

is far more palatable than the long-term cost of not defending against China's manipulation.

Senator HUSTED. So, thank you. And Madam Chair, you know, the three things that I heard from the answer: work with our partners, Japan, Korea, others who are experiencing the same problem, help Made in America work by reestablishing our manufacturing base in this country, and use tariffs against China as a tool to help get this accomplished. Thank you very much.

CHAIR. Yes, thank you. I think this has been a very good hearing and a lot of good suggestions coming from our witnesses as well. So, I am grateful for the recent positive coverage that my INNOVATE Act has gotten from a number of people, including from the CSIS scholars, including provisions to draw in new entrants and focus on SBIR funding on companies that successfully scale innovations to market for private or government end users.

And I ask unanimous consent to enter into the record an article by Phillip Singerman, senior advisor with Renewing American Innovation at CSIS. Not my favorite picture, but we'll have that entered into the record.

CHAIR. So, without objection, so ordered. And Ranking Member Markey, did you have closing comments?

Senator MARKEY. Well, if I may, I just have a couple of more questions. If I may.

CHAIR. Yes, you may. Five minutes.

Senator MARKEY. Thank you. As I mentioned in my opening statement, President Trump has single-handedly decimated our innovation ecosystem. As one professor has noted, over the last few months, an elaborate plan to ensure that China prevails in our global economic competition has taken shape. The plan's chief architects however are not China's leaders. They are U.S. politicians.

And the professor goes on to say, "The Trump administration's cuts to federal agencies are undermining the United States' ability to innovate. Hostile immigration policies are making it harder for U.S. firms, industries, universities, to attract the best ideas and talents. Wild threats of tariffs and restrictions on foreign supply chains are terrifying investors. President Trump has created the perfect storm to destroy our competitive edge."

So, Dr. Shivakumar, how will gutting our innovation ecosystem benefit China?

Dr. SHIVAKUMAR. Well, it'll benefit China by taking us out of the race, clearly. But I think what we need to do is to actually supercharge our innovation system by reinforcing all the things that do work and fixing the things that don't. There are a number of connection points. And you know, our research system is something that we have been investing in for decades now, and it's a legacy system, and it requires reform, but at the same time, we reform it, you don't destroy it. It's an important part facet of our innovation system. It requires care and renovation and resources.

Senator MARKEY. Yeah. So, over the Boston Public Library, it says "The education of its people is the best defense of a nation." And that's been a bipartisan agreement, the Democrats and Republicans have had over generations, that it benefits our national security, it benefits our innovation culture.

And in 1957, President Eisenhower enacted the National Defense Education Act. Sputnik was up in the air giving us an electronic finger from outer space. You are behind, you are behind, we're ahead of you. So, I went to college on a National Defense Student Loan, as did millions of other kids. We got to get in this race, we got to educate people because President Eisenhower recognized that the only way the United States was going to win this space race and protect our national security, was to invest in education, invest in those institutions, provide financial assistance to students.

Now, in 2025, President Trump is doing the exact opposite; taking a sledgehammer to our world-renowned innovation ecosystem, dismantling our education system, and undermining America's competitive edge. And these impacts will be felt for generations to come. As one researcher said, if this continues, we are going to lose a generation of scientists.

So, Dr. Shivakumar, what impact will President Trump's attacks have on American innovation, on National Security, our ability to attract the best and the brightest?

Dr. SHIVAKUMAR. Well, I think you have described what the impacts will be, so I would agree with you. Our innovation system is tightly coupled with our research and development system and if you undermine that research and development part of our ecosystem, you slow down all the other parts of it as well. So, this is going to be a long-lasting negative impact.

In fact, the proposed cuts to NSF and so forth, do take place. But this is what the President has proposed. I think it's for the President to propose, for Congress to dispose. So, I'm hopeful.

Senator MARKEY. So, I've been in Congress for a while. I did not vote for most favored nation status for China. I was always very suspicious of them, especially after I went to China and I could see how they were stealing our intellectual property. When in the year 2000, there was a vote on making it permanent normal trade relations, there's nothing normal about trade relations with China. I voted no each time. But there was a bipartisan consensus, Democrat and Republican Presidents, Democrat and Republican leaders in the House and Senate. I was in the vast minority saying, no, we're going to be handing over our intellectual property.

But they wanted to play, they were smart people thinking big strategic cards. They wanted to play the China card. And we went to ultimately turn over the card, it was a deuce. We didn't get anything in return. They didn't help us strategically; they just helped themselves economically.

And now that they have the lead, they're putting up barriers. They have a battery that can recharge for five minutes and the car goes 400 miles. They cannot allow that to come to the United States for manufacturing, because they are now going to actually finish off this plan, which they had to take advantage of us. And then in turn have us not be able to compete with them on all of these key innovation technologies.

That's why SBIR is so important. That's why all of the investment that we make in innovation and R&D is just so critical. And we are just unfortunately, increasingly, just leaving the playing field. And China, I'm sure is in a state of shock that we're doing

it, not receiving anything in return from the Chinese as a reciprocal concession that is made to us. Okay. I thank you, Madam Chair. I just think this is such an important area for all of us to be able to focus on.

CHAIR. Thank you, Ranking Member Markey. And thank you to our witnesses for your insight today to inform this discussion. Obviously, we all care very, very much about this issue. Our response to China's targeted exploitation of American innovators is of critical importance for America's competitiveness in the years to come.

To maintain our edge, we have to do two things: Ensure taxpayer dollars are invested in the best and the brightest innovators with a plan to scale ideas from lab to market or to our war fighters. That's very important. And number two, eliminate loopholes by which CCP compromised firms gain funding.

And I do want to be very clear here; there is a difference between companies who have won a handful of SBIR awards versus SBIR mills with hundreds of awards, over 40 years in the program. While it is a positive step that we have the foreign ties due diligence program in place, this data has revealed a concerning reality. 6 of the 25 largest recipients of SBIR awards at the Department of Defense have clear links to China. And still received nearly $180 million from the Pentagon in 2023 and 2024. And that was after the implementation of foreign ties due diligence.

Rather than focus on funding on a select, very select, few well connected companies who pursue joint ventures and other business ventures with China, my INNOVATE Act would target funding on firms looking to build and commercialize technology here, for the benefit of Americans. I will continue to shine a light on this issue and work towards reforms. And with that, I will remind you——

Senator MARKEY. If I may——

CHAIR. You had five minutes, Ranking Member Markey. And I would also ask that if anybody would like to take a look at the information, my report is on our Senate Small Business Committee website. You can go to the Republican tab, go under press releases, and you may read it for yourselves.

Senator MARKEY. May I make a unanimous consent request?

CHAIR. Yes.

Senator MARKEY. I make a unanimous request that the independent Government Accountability Office evaluation of the due diligence program that focuses on the Small Business Innovation program and the Small Business Technology Transfer program, that found that all 11 agencies have successfully implemented the due diligence program—and I congratulate you on that—in 2022, continues to be successful. They're working, and they've identified the potential foreign risk, and they've addressed them. And I would just like to put that report in the record.

CHAIR. Without objection.

Senator MARKEY. So that all of that information is made available.

CHAIR. And with that, I want to thank our witnesses for being here with us today. I ask unanimous consent that the record of today's hearing remain open for two weeks for members to submit question, revise and extend their remarks, and submit additional information into the record.

CHAIR. And without objection, so ordered. And again, we want to thank our witnesses for being here today, and obviously an issue of great importance to all of us.

And with that, the Committee on Small Business and Entrepreneurship stands adjourned.

[Whereupon, at 3:55 p.m., the hearing was adjourned.]

United States Senate
COMMITTEE ON SMALL BUSINESS & ENTREPRENEURSHIP
WASHINGTON, DC 20510–6350
TELEPHONE: (202) 224–5175

May 16, 2025

The Honorable Pete B. Hegseth
Secretary
U.S. Department of Defense
1000 Defense Pentagon
Washington, D.C. 20301

Dear Secretary Hegseth,

As Chair of the U.S. Senate Committee on Small Business and Entrepreneurship, I uncovered a troubling pattern among a small group of companies that are the largest recipients of taxpayer dollars through the Department of Defense (DoD)'s Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) programs. A review of the 25 companies in DoD's SBIR-STTR programs with the most awards from fiscal year 2010 to fiscal year 2023 (receiving 7,251 awards amounting to a total of $3.23 billion) showed that six of these firms had concerning ties to the Chinese Communist Party (CCP): Triton Systems, Luna Innovations Inc., Lynntech Inc., TDA Research Inc., Nanosonic Inc., and Kitware Inc.[1] Despite their significant ties to China that jeopardized taxpayer-funded technologies, under the Biden Administration, these six companies still received nearly $180 million in DoD SBIR-STTR awards in 2023 and 2024.[2] This is unacceptable.

Since 2022, I have demanded vetting of all applicants to the SBIR and STTR programs for potential ties to America's foreign adversaries. As a result of my reforms in the *SBIR and STTR Extension Act of 2022* (P.L. 117-183) and subsequent oversight, all 11 agencies in the SBIR and STTR programs have foreign ties due diligence procedures in place as of mid-2023.[3] Nonetheless, I am deeply concerned that sophisticated companies equipped to hire consultants, grant writers, and lobbyists continue to exploit due diligence loopholes to collect hundreds of millions in SBIR-STTR awards that may ultimately benefit China.

I have attached my report detailing these connections between the largest DoD SBIR-STTR recipients and CCP-linked entities. The report also proposes policy reforms necessary to protect critical technologies in the SBIR-STTR programs from our adversaries. I urge you to investigate these six companies on their troubling ties to adversaries and, if necessary, stop all awards to these companies.

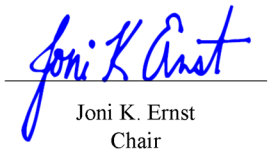
I am grateful for your commitment to spend each taxpayer dollar carefully and in pursuit of America's national security and warfighting capability. We must demand the very best for our men and women in uniform and for all taxpayers. I look forward to working with you on bolstering research security measures in DoD's SBIR and STTR programs. Thank you for your

---

[1] *See* Attachment A, Figure 3: Foreign Adversarial Risks of SBIR Mills.
[2] *See* Attachment A, Figure 5: SBIR Mills and Award Dollars/Count (2023-2024).
[3] SBIR and STTR Extension Act of 2022, Pub. L. No. 117-183, §4(b)(2), 136 Stat. 2182.

prompt attention to this important matter. If you have any questions, please do not hesitate to contact me or my Committee staff at (202) 224-5175.

Sincerely,



Joni K. Ernst
Chair

Outside testimony for the Committee on Small Business and Entrepreneurship

Dr. Patrick Gallagher

Chair Ernst and Ranking Member Markey, thank you for the opportunity to submit my written input to your hearing on Innovation in the Crosshairs: Countering China's Industrial Espionage.

My name is Dr. Patrick Gallagher and I am currently a distinguished professor of physics at the University of Pittsburgh. Previously, I was Undersecretary of Standards and Technology for the U.S. Department of Commerce, and Director of the National Institute of Standards and Technology (Between 2008 and 2014), and then Chancellor of the University of Pittsburgh (between 2014 and 2023). In these roles I enjoyed a front row seat to the ways in which science and engineering discovery fuel our nation's economy and national security advantages.

I am also familiar with the ways in which the innovation system of the United States is being compromised by foreign actors such as China who wish to diminish our strong and long-standing advantages in this area. In 2022, I co-chaired with Sue Gordon, a consensus report of the National Academies of Sciences, Engineering, and Medicine titled, "*Protecting U.S. Technological Advantage*" which explored the challenges of developing effective research security programs in this rapidly changing threat environment. The report focused specifically on the unique challenge posed by China to U.S. leadership in advanced technology development.

I am particularly delighted that the Committee on Small Business has elected to focus on these issues. While there has been much attention recently on the role of scientific discovery and research in advancing technology leadership by the United States, not nearly enough focus has been placed on the essential role of small businesses in our nation's innovation system. New scientific discoveries and engineering advances are an essential ingredient of new technologies. This is why we invest significant public funds in these efforts. But these discoveries and ideas are not sufficient by themselves for it takes enormous effort and ingenuity to turn an idea into a new technology product or services This is why, in terms of dollars spend, the "D" part of R&D is much larger than the "R" part.

In the U.S. this innovation role belongs almost exclusively to our private sector. But vitally, it is our nation's start up community – the small, dynamic, risk-taking businesses that specialize in the newest, riskiest ideas with the most potential for transformative results, that are the real engines of the U.S. innovation system. This was the fundamental insight that led to the Bayh-Dole Act which transferred the ownership of IP from publicly funded research to the private sector inventors. It is also the goal of numerous other federal programs, including the SBIR and STTR programs, which seek to support the earliest stages of these entrepreneurial efforts and

promote their chances of success. While many other countries have high quality research programs, few if any can match the U.S. combination of research leadership combined with the world's most dynamic start up business community.

Viewed in this light, the origin of U.S. technological advantage depends on two things: we must have the latest ideas and we must be the first to develop them into new technologies. Protecting this leadership position then requires two goals:

(1) it must protect the most critical outputs of the research process from theft or misuse (this is the dominant focus of current research security programs); but it must also
(2) promote effective and timely translation of research to be the first to bring new technologies to market.

Failing to achieve either goal diminishes the U.S. leadership position.

Stated more dramatically: a foreign adversary wishing to harm U.S. technology leadership could either seek to steal or copy the key research results, designs and other outputs of research and development – or they could seek to induce us to harm our own system by responding unwisely with cumbersome compliance-based security programs with only a modest security benefit. While the first approach would harm the targeted technology effort, the latter would effectively slow down every small business startup company that faces these requirements.

Properly balancing the need for protection with the need to promote the success of these entrepreneurial firms is the central task we face. This twin challenge is not being discussed adequately by policy makers – and unfortunately it is too easy to "win the battle but lose the war" by focusing only on the research protection aspect. This is why I am so pleased that this Committee is looking at this issue.

Let me offer several thoughts on the challenge of research and development security for entrepreneurial small businesses that I hope are helpful to the Committee's deliberations:

Small is better. The central advantage of the small business (SME) startup community is the speed and efficiency with which they can develop the very newest, and riskiest research results. With small, focused teams formed with a sharp focus on new product development, these SME's move fast while minimizing the financial exposure of taking on the large risks associated with the newest technologies. Big companies, even those with the largest and most advanced R&D programs, cannot match the agility, speed and efficiency of small business start-ups. Since these companies are very small, any new requirement either becomes "collateral duties" for the small number of existing employees or requires them to hire more staff to manage the compliance program. Either approach decreases their productivity and either slows them down or reduces the risks they can take on. While compliance-based programs produce this effect for

companies of all sizes, the results are much more dramatic and existential for these small, and nimble business enterprises.

In adopting any requirements to enhance the security of SME startups, it will be vital that these requirements do not adversely impact the advantages of speed and efficiency that are vital to U.S. technological leadership.

The current government policy approach to security is technology-based, not threat based. This is a blind spot. This was a central finding of the "*Protecting U.S. Technological Advantage*" report. Instead of looking at the objectives and actions of our adversaries, we tend to focus on the technologies themselves when designing security programs (a good example is critical technology lists). While this is part of the problem, it is not the complete picture, and this blind spot is particularly problematic for SME startups. The problem with this approach for small startups is that the technology in question is being developed and is not well defined. In fact, in many cases even the end use of a new technology is still undefined! Applying rigid technology-based controls in a compliance program to the uncertain and fluid environment of a start up is highly problematic and quickly leads to a "just protect everything" approach to setting requirements.

Since the objective of technology innovation is to be first to market, any approach that slows down U.S. small businesses helps foreign adversaries. In other words, the greater threat may be attacking our speed advantage and not stealing the research results and, in those circumstances a more effective response is to accelerate the efforts of U.S. based startup companies, even if we risk some exposure to research loss.

A threat-based response prioritizes minimizing threats to U.S. leadership. This must include protecting the unique advantages of the U.S. SME startups as the world's fastest and most agile new technology developers. This approach suggests that further promoting SME technology development is as important an element as protection research outputs.

SMEs are not big companies. The largest technology firms, with the greatest number of employees, largest markets, and who perform the largest portion of R&D in the world are not subject to some of the compliance and due diligence requirements that have been proposed for small business enterprises. In fact, the largest of these companies are multinational and do research, development, and production in many countries, including in countries where there is considerable geopolitical tension with the U.S. The response of these firms to excessive regulation is to move their R&D programs to lower cost countries. SME startups do not have this option. For them, responding to the costs and liabilities of new regulations would more likely cause them to take on "safer" or less risky efforts – exactly the opposite of what action best promotes U.S. leadership in technology.

Startup companies are not research universities. This is a vital distinction, and one that was highlighted in the "*Protecting U.S. Technological Advantage*" report. Research at U.S. universities is not aimed at commercial technology development and differs in many important ways. By staying away from the unique risks posed by developing technologies, universities are preserving their role, namely, to train research scientists and engineers. In the report, we pointed out that this means that when efforts at universities become too close to commercial development they should be moved out of the main university research environment and into a more restricted environment. For universities, this segregation of environments is important so that they do not have to resort to protecting all environments become some efforts are more sensitive because this would adversely impact the teaching mission.

For startups, particularly those staffed with university-affiliated employees, or who work in close collaboration with universities, this is also a vital distinction. The commercial development they are doing requires a new and unique environment that carries out this development independent from the university. Maintaining this separation of function is a central piece of risk management because it allows the university to pursue its mission without the need for commercial controls on information and participation, and for SME's it allows them to develop new technologies without the need for broad participation and dissemination of results expected by a university. Because SBIR and STTR programs are managed by the same agencies that fund university-based research there may be a tendency to apply the same approach to SMEs that they require for universities. This undercuts the advantages of separating these functions into separate environments.

SBIR and STTR are "security" programs. This is an odd thing to assert, but since they function to support SME's at their most fragile stage of technology development, close to the point of technology transfer, they play a central role in supporting the speed and agility of American technology innovation. From the perspective of protecting U.S. technological advantages from foreign adversaries, ability of these programs to support the rapid translation of research into meaningful technologies is as important to U.S. competitiveness as is protecting the results of research activities. Furthermore, as noted above, to maintain this critical function, it will be important to avoid poorly designed or cumbersome compliance regulations on SME's.

I hope that the Committee on Small Business and Entrepreneurship will take a visible and leading role on these important challenges. I am convinced that focusing only on protecting the research outputs and not on protecting all of our competitive advantages will fail to meet the challenges we face in an increasingly competitive environment. With your unique role you can bring the needed balance to these discussions and in particular ensure that we do not diminish in any way the uniquely American advantage of our entrepreneurial startup community.

Reference:

National Academies of Sciences, Engineering, and Medicine, 2022. *Protecting U.S. Technological Advantage*. Washington, DC: The National Academies Press. https://doi.org/10.17226/26647.

SBIR and the Role of Multiple Awards

Photo: Adam Glanzman/Bloomberg via Getty Images

Blog Post by **Charles Wessner** and **Sujai Shivakumar**
Published July 29, 2025

As the Small Business Innovation Research (SBIR) program reauthorization deadline approaches in September 2025, Congress is debating what form the next phase of this highly successful program should take. While there is bipartisan agreement that SBIR is a critical tool for national innovation and security, some reauthorization proposals would limit or disincentivize "multiple award winners," unintentionally undermining the program's flexibility and effectiveness.

On its face, limiting the number of awards for a particular small business may allow more firms to participate in the SBIR program, thereby broadening the nation's innovation base. But SBIR is already an open program with a remarkable one-third of awardees new to the program each year. Moreover, the share of funding going to multiple award winners is modest, and the number of firms winning high counts of awards is small relative to the program's scale and longevity.

Top-down restrictions and unnecessary administrative burdens, such as those proposed in the INNOVATE Act, would reduce the flexibility and agility of the SBIR program and risk making them less effective as tools to support new technologies and deliver rapid solutions to the mission needs of federal agencies. More fundamentally, rather than seeking to manage the program through legislative restrictions, Congress should encourage agency program managers to weed out firms that do not support SBIR's innovation mission and justify cases where companies receive multiple awards. The program was designed to rely on program managers—and most have proven successful. If they are not, the managers should be changed, not the program.

How Multiple Awards Support Innovation

It is worth asking what we expect out of SBIR award winners. One or two awards do not often generate a thriving company on their own. They may, however, contribute to the creation of intellectual property, measured in patent applications, patents awarded, and patent licensing. The award may attract outside investment from private partners or lead to spinouts of the technology in a new firm focused on developing the results of the award. And there are cases where the firm meets the agency mission need with a low-cost invention or meets a specific analytical need for the awarding agency.

There are multiple reasons why multiple SBIR awards are essential to accelerating innovation:

- ***Building Momentum:*** Technologies do not surge into the market from the head of Zeus: they require iteration, testing, and adaptation. SBIR's structure must allow for reinforcement of initial support as small innovative firms develop, especially for nascent high-tech products that are building momentum toward acquisition or commercialization.
- ***Supporting Small Pools of Expertise in Strategic Fields:*** In strategically important emerging technology areas, such as quantum computing or advanced materials, the pool of innovative companies is typically small and specialized. As a result, multiple awards often concentrate by necessity among the few technically capable firms. Rather than evidence of failure, this reflects the reality of emerging sectors: these firms are often the only ones with the depth of talent and familiarity

with agency missions to meet the research and development (R&D) needs of groundbreaking technologies. SBIR helps grow these pools.

- ***Preventing Premature Abandonment:*** Arbitrarily limiting repeat awards could strand promising technologies in a quasi-developed status, leaving them vulnerable to foreign absorption or emulation. If U.S. firms cannot complete development through domestic support, they may be outpaced or overtaken by foreign competitors, including strategic adversaries. In an era of global technology competition, particularly with China, the cost of under-developing strategic technologies is not theoretical—it is a national security vulnerability.
- ***Extending the Bridge across the Valley of Death:*** Promising projects may require additional SBIR awards simply to reach the threshold for commercial uptake; they have done so in the past, with very powerful results. While SBIR Phases I (Feasibility Study) and II (Prototype Development) are well-established and funded within SBIR, Phase III (Commercialization) often lacks a uniform pathway. Some agencies, like the Department of Defense have robust Phase III programs. Others, like the National Institutes of Health, have follow-on awards. But success in Phase I or II does not guarantee the technology's commercialization. For this reason, the program sometimes needs "an additional arch" in its bridge over the Valley of Death. This can be achieved through more formal initiatives but is probably best handled by encouraging optional follow-on funding at the discretion of program managers. Again, this is a management choice, not a structural issue for Congress.

Support Excellence, Not Arbitrary Headcounts

To fully exploit SBIR's potential in today's hyper-competitive environment, Congress should maintain an open and competitive program and incentivize active agency management, not impose arbitrary caps. The best way to prevent abuse or inefficiency in a program like SBIR is not through rigid legislation, but effective program management. When individual firms receive repeat awards, program managers should be able to justify why. Managers should also be empowered to exclude underperformers or justify continued support where warranted. Legislative caps simply introduce blunt restrictions into a program designed for technical judgment and adaption to changing—and sometimes pressing—national needs.

The key questions are: What are the mission needs? How well does the proposal meet those needs? And how well did the proposing firm do previously? If answers are positive and the quality is high, the award should go forward. If a new firm presents a promising approach, it should win as well. There is no panacea, just multiple low-cost shots on goal. Some will score.

At the end of the day, SBIR's purpose is to identify and support excellence in innovation. The goal is not to just hand out starter grants but to help develop technologies that advance U.S. economic and national security interests. Instead of limiting participation, Congress should expand the program's capacity to support success—wherever it arises—and take meaningful steps to ensure projects can reach the finish line. But above all, the fundamental condition for SBIR success is Congressional support for the R&D budgets that fund it. That is the lifeblood of the program—and the long-term source of American innovation and security.

The authors would like to thank Julie Heng, research associate with Renewing American Innovation, for her contributions to this piece.

Tags

American Innovation, Strategic Capital, and Technology and Innovation

Center for Strategic and International Studies
1616 Rhode Island Avenue, NW
Washington, DC 20036
Tel: 202.887.0200
Fax: 202.775.3199

MEDIA INQUIRIES

Sofia Chavez

Media Relations Manager, External Relations

202.775.7317

SChavez@csis.org

See Media Page for more interview, contact, and citation details.

INNOVATE SBIR: Expanding the Number of Participating Companies and Fostering Commercialization

Photo: Demetrius Freeman/The Washington Post via Getty Images

Blog Post by **Phillip Singerman**
Published July 10, 2025

As the 119th Congress considers reauthorization of Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) legislation, findings from CSIS research and other analyses on SBIR/STTR programs offer valuable suggestions.

Established in 1982, the SBIR Program seeks to advance four objectives: (1) stimulate innovation, (2) increase the use of small businesses in addressing federal R&D needs, (3) foster the participation of socially and economically disadvantaged individuals in innovation and entrepreneurship, and (4) increase private sector commercialization of technologies derived from federally funded R&D. The complementary STTR Program was created in 1992 to facilitate the commercialization of university and federal R&D by small companies. Since their enactments, the programs have been extended and reauthorized several times. In FY2022, federal agencies obligated $4.12

billion for SBIR/STTR, with 91 percent in SBIR awards: $630 million across 2,927 new Phase I awards, and $3.14 billion across 2,344 new Phase II awards.

The SBIR program has been subject to numerous rigorous, independent and comprehensive reviews—most notably by the National Academies of Science, Engineering and Medicine—which have found that the program achieves its legislative goals, including stimulating technological innovation and supporting agency R&D needs through small businesses. However, a recent study prepared by the Congressional Research Service (CRS) identified specific issues for Congress to consider as it analyzes the legislation.

Expanding Participation

According to CRS, some members of Congress and other observers have raised concerns over small businesses that receive multiple SBIR and STTR awards. Indeed, a variety of studies document that in some cases, a very small number of firms receive a disproportionate amount of funding, which can impede the program's broader objectives:

- A Government Accountability Office (GAO) study requested by Congress in the SBIR/STTR Extension Act of 2022 found that from FY2011 to FY 2022, 22 firms received 50 or more Phase II awards each. In other words, these companies accounted for 11 percent of total Phase II awards and 10 percent of total Phase II dollars, despite representing fewer than 1 percent of all Phase II awardees (6,865).
- Small Business Administration (SBA) data show that in FY22, agencies made 3,859 Phase I awards to 2,560 companies; 61 "multiple award winners," who received >15 Phase II awards over five years (2 percent) obtained 548 awards (14 percent). In some agencies, the ratios were greater: at the Department of Defense (DOD), 6 percent companies secured 22 percent of awards, while at the Department of Energy, 8 percent of companies received 17 percent of awards.
- Of SBIR awardees in quantum information science and technology from 2015 through 2023, 362 companies received 575 awards, an average of 1.5 per firm; three firms, representing fewer than 1 percent of the total, received 64 (11 percent) of the awards.

- Similarly, a study cited by the Defense Innovation Board found that over ten years, the top 5 percent of companies with the most Phase I/II awards received 49 percent of all Phase I/II funding, while the top 25 companies (0.53 percent of 4,703) received 18 percent of all Phase I/II funding–over $2.3 billion, averaging $92 million in Phase I/II awards per company.

In response to such concerns, the SBIR/STTR Reauthorization Act of 2011 introduced Transition Rate and Commercialization Rate Benchmarks to track and measure the progress of awardees toward commercialization through the different SBIR phases. Transition rate benchmarks measure the ability of companies to proceed from Phase I to Phase II SBIR awards; by contrast, commercialization rate benchmarks, applied to firms with multiple SBIR awards, measures the degree of sales or investment. The SBIR/STTR Extension Act of 2022 further strengthened the standards for companies with multiple awards. However, the penalties for non-attainment are not proving significant.

To address this problem, the INNOVATE Act of 2025 proposes to cap lifetime company awards to a total of $75 million. Perhaps the most powerful rationale is to limit "SBIR mills"–firms whose business model is writing SBIR proposals–which monopolize available funding, thereby "crowding out" resources that could go to a larger number of qualified companies with promising R&D capabilities.

Crowding out promising firms impedes the ability of SBIR programs to achieve their legislative objectives. The author of this paper has been engaged with SBIR since 1983, and in the author's experience, many high quality SBIR applications are not funded because of the limitation of the funding, not because of the quality of proposals.

The average Phase I selection rate in FY22 was just 15 percent in civilian agencies and 18 percent in DOD agencies. If the proposed INNOVATE Act cap had been in place, $425 million could have been freed up at DOD, enough to fund as many as 1700 Phase I awards ($250,000). Other sums would be available from other agency accounts.

Foster Commercialization

Given current financial constraints, utilizing existing appropriations more efficiently would further the program's objectives. However, expanding the funding available for

young, small innovative firms is by itself not sufficient–helping firms commercialize and maximize the potential of funded research is necessary. Fortunately, agency practices and local government support programs have begun to address this challenge.

For example, the National Institute of Standards and Technology (NIST), an agency with a traditionally small SBIR program, has leveraged new CHIPS & Science Act funds to expand commercialization support. In its 2024 NOFO, building upon earlier efforts to reward commercialization and encourage new firms to participate in the program, NIST's CHIPS R&D Metrology Program offered up to $54 million for 24 awards to support commercialization. NIST used open topics as well as closed ("conventional") topics, increased Phase I and II awards to their maximum levels ($285,500 and $1,910,000 respectively), encouraged Fast Track approvals, tracked Transition Rate Benchmarks and Commercialization Rate Benchmarks, required submission of Commercial Viability and Domestic Production (CVDP), and allowed Technical and Business Assistance (TABA) funding.

TABA, a relatively new program, was authorized by Congress in 2019 to help cover commercialization and business assistance expenses not allowed under regular SBIR funding. Although program specifics vary by agency, generally up to $6,500 may be provided to Phase I winners in addition to the award amount, and up to $50,000 may be allowed as part of a Phase II award. The assistance must be provided by a third-party entity, either chosen by the company, or at its request, by the funding agency. Services include technology assessments, market analysis and strategy, business model development, commercial road mapping, investment readiness assessment, IP, and regulatory affairs support. According to FY22 SBA data, $5.99 million in TABA assistance was provided by civilian agencies, and $23.12 million was provided in award obligations. (Note: DOD uses other authorities, such as the Commercialization Readiness Program (CRP), to accelerate the transition of DOD SBIR/STTR funded technologies to Phase III.)

Montgomery County, MD, the only county-level SBIR matching program, provides $25,000 to Phase I and $50,000 to Phase II awardees, with eligibility limited to small and young companies with few prior SBIR awards. The county has also recently

created a local "TABA-lite" program requiring recipients to spend half their local grant on the reimbursement of third-party expenses attributable to technical, investment, or commercialization assistance.

The INNOVATE Act's "Phase 1A" proposal is another creative provision: it would provide one-time $40,000 awards through a simplified application to companies without prior awards. This would allow agencies to identify and transition first-time applicants into the standard Phase 1 process. The Phase 1A proposal has a similar goal to Phase 0 support programs that local organizations already include as part of their assistance program that encourage new companies to participate the SBIR program and advance commercialization.

According to the State Science and Technology Institute, every state and Puerto Rico offers SBIR programs, which can include financial assistance (through matching grants to awardees), proposal development and mentorship, technical assistance, and networking opportunities. At least 31 organizations offer "Phase 0" awards to help first-time applicants prepare competitive proposals.

An existing federally-funded, state-managed program is the SBA's Federal and State Technology (FAST) Partnership Program, which funds competitive awards of up to $200,000 to provide specialized training, mentoring, and technical assistance. In October 2024, the SBA funded organizations in 48 States and Puerto Rico to provide support, generally in underserved communities, in applying for SBIR awards. For example, the SBIR/STTR Proposal Lab from the Maryland Technology Development Corporation, funded by the FAST Partnership Program, assists first-time applicants to apply for NSF funding.

Recommendations

These findings suggest specific legislative actions and program enhancements to address Congressional concerns, without requiring additional appropriations:

- TABA is a relatively new program with significant potential. Widespread local organizational programs reflect the importance of technical assistance. Agencies should be encouraged to robustly advertise the availability of the program and maximize its usage.

- Similarly, the extensive network of local SBIR support programs should be embraced by federal agencies. Partnerships should be encouraged between agencies and States (and their associations such as SSTI). Local "TABA-lite" local programs should be fostered.
- The Phase 1A concept addresses a definitive need, attested to by the number of local Phase 0 programs. However, implementation of a federal program by agencies with diverse missions and practices is always challenging. Authorizing and carefully monitoring a pilot program is a proven policy tool. (Note: The SBIR program was initially piloted by NSF in the late 1970s.)
- An additional modest vehicle for identifying potential SBIR applicants, developed by NIST, can help connect applicants with alternative support programs. Applicants were given the opportunity to agree (via a checkbox on the cover sheet) to have their contact information publicly disclosed in the event they did not receive funding. Such a requirement would identify "pre-qualified" R&D oriented companies that could benefit from local assistance programs. A variant of the above is to encourage agencies to consider releasing "approved but not funded" (ABNF) lists of companies that would have been funded had there been more funding. This list would also identify "pre-qualified" companies.

Conclusion

The SBIR/STTR programs have delivered tremendous value for more than four decades. Reauthorizing the legislation provides an opportunity to address issues that impede the achievement of Congressional objectives and experiment with new features that could improve the program, namely discourage monopolistic "mills" and expand opportunities for new innovators. The INNOVATE Act provisions described above are a positive contribution to these goals.

Phillip Singerman, PhD, is a senior adviser (non-resident) with Renewing American Innovation at the Center for Strategic and International Studies (CSIS). Previously, he served as NIST's Associate Director for Innovation and Industry Service and the U.S. Assistant Secretary of Commerce for Economic Development. Singerman has been engaged with the SBIR program since 1983 as the funder of companies that participate in the SBIR program, as the manager of federal and state-sponsored support

programs, as the executive responsible for SBIR programs at NIST, and as an NSF SBIR panel reviewer.

Tags

American Innovation, Strategic Capital, Technology and Innovation, and Technology

---

Center for Strategic and International Studies
1616 Rhode Island Avenue, NW
Washington, DC 20036
Tel: 202.887.0200
Fax: 202.775.3199

MEDIA INQUIRIES

Sofia Chavez

Media Relations Manager, External Relations

202.775.7317

SChavez@csis.org

See Media Page for more interview, contact, and citation details.

U.S. SENATE COMMITTEE ON
SMALL BUSINESS AND ENTREPRENEURSHIP

SBCGOP
SENATOR JONI ERNST
CHAIR

CRITICAL AMERICAN TECHNOLOGY VULNERABLE TO CHINA

INVESTIGATION ALERT: URGENT REFORMS NEEDED IN SBIR PROGRAM TO PROTECT NATIONAL SECURITY

May 2025

Key Takeaways

Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) Programs

The SBIR-STTR programs serve a key role in ensuring that the United States maintains technological supremacy. The programs award more than $4 billion annually to small businesses seeking to develop and commercialize critical technologies.

Foreign Adversaries Exploit SBIR-STTR Programs Necessitating Due Diligence

A bombshell 2021 Department of Defense (DoD) report revealed that foreign adversaries, particularly the Chinese Communist Party (CCP), had infiltrated the SBIR-STTR programs for years to steal U.S. taxpayer-funded research and technology.

Through the *SBIR and STTR Extension Act of 2022*, Senator Joni Ernst (R-Iowa) created a foreign influence due diligence process to screen– **for the first time**– SBIR-STTR applicants for ties to adversaries and better protect taxpayer-funded innovations. This new provision required each participating agency to fully assess the security risks presented by each small business applying for funding.

Inadequate Due Diligence and Enforcement

Senator Ernst's establishment of a foreign ties due diligence program took an important first step by revealing that most applicants with a flagged foreign risk **still** received funding. Out of **835** applications flagged for a foreign risk, only **303** were denied for that risk.

This data obtained through Senate Committee on Small Business and Entrepreneurship Chair Ernst's oversight efforts revealed that federal agencies lack a standard process in evaluating foreign risks, leaving loopholes for China and others to exploit.

SBIR Mills Pose a Significant Risk

Most concerning—a small number of companies, known as SBIR mills, exploit the program by receiving the lion's share of funding, while maintaining troubling ties to foreign adversaries.

Ernst's new due diligence process uncovered that **six** of the **25** largest recipients of SBIR-STTR funding at the Department of Defense (DoD) have clear links to countries like **China**, yet still received nearly **$180 million** in DoD awards in 2023 and 2024.

Chair Ernst's INNOVATE Act Strengthens Protections

Chair Ernst is closing the loopholes being exploited by foreign adversaries and ensuring taxpayer-funded research remains secure through her *Investing in National Next-Generation Opportunities for Venture Acceleration and Technological Excellence (INNOVATE) Act.*

The legislation takes a three-pronged approach, 1) improving the definition of "foreign risk," to ensure that it is strong, clear, and applied consistently across all agencies; 2) requiring mandatory denials for companies with reviews that show adversarial ties; and, 3) strengthening clawback provisions, so that any company that does violate the law and expose taxpayer-funded research to any foreign adversary must pay the funding back in full.

Driving American Innovation: The SBIR and STTR Programs

Originally the Small Business Innovation Research (SBIR) program was created by Congress to provide small businesses with early-stage funding to advance research toward commercialization of their technological innovations for the benefit of government and private sector customers.[1] Eleven federal government agencies direct a dedicated percentage of their research budget to the program, ensuring that small businesses play a key role in fostering innovation. Five federal agencies carry out a complementary STTR program where small businesses work with outside research institutions to develop their technologies. In Fiscal Year (FY) 2024, the SBIR-STTR programs provided over $4.7 billion in funding to small businesses building emerging technologies.

Since their inceptions, SBIR in 1982, and STTR in 1992, these programs have provided seed funding to thousands of small businesses seeking to commercialize emerging research in critical technology areas and contributed to the growth of multiple success stories.[2]

Chinese Infiltration in the SBIR-STTR Programs

In 2021, the DoD issued a groundbreaking report detailing how the CCP gained access to DoD-funded SBIR-STTR research for malign purposes.[3] Their investigation showed that the CCP employed a number of tactics to steal SBIR-funded research and technologies. For example, in addition to recruiting U.S. employees at SBIR-backed firms, CCP agents bought U.S.-based SBIR startups and transitioned them over to Chinese firms or

convinced the U.S. firm to establish China-based subsidiaries that were subsequently "investigated" by the CCP. They also regularly overtook SBIR-backed U.S. firms through venture capital funding or arranged business partnerships with Chinese-tied firms to sell their products abroad.

Concerningly, the DoD report further detailed how China has leveraged the SBIR-STTR programs to identify DoD technology development priorities. It concluded that, in all their company case studies, China, not America, was the ultimate beneficiary of these U.S. government research investments. The report recommended that a due diligence process in the SBIR-STTR program be established to assess national security risks before further taxpayer funds go into the wrong hands.[4]

Senator Ernst Establishes Due Diligence Requirement

The 2021 DoD report and subsequent reporting by the Wall Street Journal led Senator Joni Ernst (R-Iowa) to create a first of its kind foreign due diligence program in the *SBIR and STTR Extension Act of 2022.* The legislation identified concerning financial, ownership, and academic interests between SBIR-STTR applicants and foreign countries of concern (Russia, Iran, China, and North Korea).[5] As a result of Senator Ernst's reforms, SBIR-STTR applicants are now required to submit a foreign ties disclosure form as part of their application.[6]

Over the past two and a half years, federal agencies administering the program have developed processes to implement the due diligence program, identify concerning relationships with these adversarial foreign countries as required by statute, and determine which risks warrant a denial of award. By mid-2023, all agencies with an SBIR program established an operational due diligence process to evaluate adversarial foreign ties.[7] **For the first time, agencies are evaluating foreign risk before SBIR awards are granted to small businesses and collecting data to understand adversarial threats to the program.**

Inconsistent Standards Create Problems

The 2022 due diligence program was a major step forward because it produced a treasure trove of data, enabling Congress and federal agencies to analyze the scope of adversaries' attempts to steal SBIR innovations.

In a November 2024 response to a letter from then-Ranking Member Ernst, each agency with an SBIR or STTR program, except the Department of Energy, provided data on their

due diligence programs including the number of applications flagged for a foreign risk, the nature of that foreign risk, and the number of applications denied on the basis of a foreign risk.[8] This data is displayed below in Figure 1 and Figure 2.

Figure 1: SBIR-STTR Foreign Risk Flags and Denials in Fiscal Year (FY) 23 and FY24[9]

Federal Agency	Number of Flagged Applications	Number of Denied Applications for a Foreign Risk
National Science Foundation	6	2
National Institutes of Health	144	144
Department of Homeland Security*	1	1
Department of Transportation	0	0
National Institute of Standards and Technology	1	0
National Aeronautics and Space Administration	125	1**
Department of Education*	22	0
Department of Defense	522	152
Environmental Protection Agency	0	0
National Oceanic and Atmospheric Administration	5	0**
United States Department of Agriculture*	9	3
Department of Energy***	N/A	N/A

*Some agencies reported flagged "applicants" or "companies" in lieu of applications.
** Of applications flagged for concerning adversarial ties, NASA denied 107 applications and NOAA denied 3 applications due to lack of technical merit - not on the basis of their foreign ties.
*** As of April 2025, the Department of Energy did not provide requested data to the Senate Committee on Small Business and Entrepreneurship.

Figure 2: Nature of SBIR-STTR Foreign Risk Flags in FY23 and FY24[10]

Federal Agency	Number of Cyber-security Flags	Number of Patent Analysis Flags	Number of Employee Analysis Flags	Number of Foreign Ownership Flags	Flags in a Different Category
National Science Foundation	0	0	6*	6*	0
National Institutes of Health	19	7	98	22	134 (Financial Ties and Obligations)
Department of Homeland Security	1	0	0	0	0
Department of Transportation	0	0	0	0	0
National Institute of Standards and Tech.	0	0	1	0	0
National Aeronautics and Space Administration	0	1	105	5	25 (Business Arrangements and Funding)
Department of Education	0	1	19	2	2 (Supply Chain)
Department of Defense	0	79	386	178	63 (Financial Obligations)
Environmental Protection Agency	0	0	0	0	0
National Oceanic and Atmospheric Administration	0	0	5	0	0
United States Department of Agriculture	0	2	7	2	0
Department of Energy**	N/A	N/A	N/A	N/A	N/A

*National Science Foundation said their six flagged applications were a combination of employee and ownership flags.

**As of April 2025, the Department of Energy did not provide requested data to the Senate Committee on Small Business and Entrepreneurship.

Based on 11 Congressional briefings that further outlined due diligence implementation, it became evident that there were inconsistencies in how agencies identify foreign ties risks and determine when an applicant should be denied.[11] Some agencies seem willing to approve an applicant with a significant foreign ties risk when agency officials are determined to fund a certain technological capability, no matter the consequences.[12]

Further, existing loopholes allow certain adversarial relationships with SBIR-STTR awardees to avoid detection by current processes, and the extensive ties of certain SBIR mills and their spinoffs with Chinese researchers and institutions place significant amounts of taxpayer-funded intellectual property at risk. To counter American adversaries, reforms are needed to strengthen the foreign ties due diligence program.

Unfortunately, **the conclusion of the sustained Congressional oversight of this issue is that further reforms are needed to fully protect the SBIR-STTR research and technologies from U.S. adversaries, particularly China.**

SBIR Mills and Foreign Ties Concerns

The data gathered from the 2022 due diligence protocols also expose an extra national security weakness in the SBIR-STTR programs, the threat from SBIR mills—firms that specialize in writing SBIR grant applications and are adept at winning the most grants. A review of the 25 companies in DoD's SBIR-STTR program with the most awards from 2010-2023 (receiving 7,251 awards amounting to a total of $3.23 billion, all of which are considered SBIR mills) showed many of these firms had troubling ties with foreign adversaries.[13] This evaluation, displayed below in Figures 3, 4, and 5, revealed that at least **six** out of the top **25** SBIR mills had problematic relationships with foreign adversaries yet continued to receive awards even after implementation of due diligence requirements. **In 2023 and 2024, these firms received 297 awards amounting to a total of $178,420,926.**[14]

Given that these firms were evaluated under due diligence protocols dozens of times, once for each award they received since 2022, the continued dominance of these SBIR mills calls into question the consistency of due diligence standards. **This also raises concerns that hundreds of millions of taxpayer dollars have been knowingly exposed to adversarial risks.**

Figure 3: Foreign Adversarial Risks of SBIR Mills

SBIR Mill	Type of Risk	Concerning Foreign Affiliations with Adversaries
Luna Innovations Inc.	Joint Venture	Luna Innovations has a Guangdong, China based "designated agent and technical service center" operating as a joint venture with Jietong Technology Service Co., for its products in the Asia-Pacific region.[15]
Triton Systems	Spinoff	The long-time CEO of Triton Systems, Ross Haghighat, had recent ties to a Chinese government sponsored investment firm. In 2020, Ross Haghighat was appointed to the board of CITIC Capital Acquisition Corp, a special purpose acquisition company (SPAC) sponsored by CITIC Capital Holdings Limited, a branch of the Chinese state-owned CITIC Group.[16] FRX Polymers Inc., a spinoff of Triton Systems, received a $22 million investment from Chinese investment firm CITIC Capital.[17] In 2019, FRX Polymers started a joint venture with a Chinese company to produce flame retardants.[18] Triton Systems received multiple SBIR awards to produce flame retardants, including awards used to develop technology at FRX Polymer.[19] The Navy SBIR-STTR program touts the FRX Polymer spinoff as a success story for the program.[20] Mr. Haghighat was Chairman of the Board at FRX Polymers.[21] A separate spinoff of Triton Systems, Aduro Biotech, merged with the biotech company Chinook Therapeutics in 2020.[22] In 2021, the company launched a joint venture with the Chinese biotech company Pivotal bioVenture Partners.[23] Ross Haghighat, was an independent director at both Aduro Biotech and Chinook Therapeutics.[24]
Lynntech	Personnel	A research scientist at Lynntech was recruited into a Chinese state-sponsored talent program.[25] At the university he was recruited to, Zhengzhou University, he conducted research in similar scientific areas as did under SBIR-STTR awards at Lynntech.[26]

TDA Research	Joint Research	TDA Research has done joint research with Sinopec, a state-owned Chinese oil company, for several years.[27]
Kitware	Personnel	On its company blog, Kitware lists as customers of its technology Nanjing University of Aeronautics and Northwestern Polytechnical University - two universities that are part of China's Seven Sons of National Defense, a grouping of public universities affiliated with the Ministry of Industry and Information Technology of China.[28] An employee of Kitware did joint research with academics at the University of Chinese Academy of Sciences, a state-backed Chinese research institution.[29]
Nanosonic Inc	Joint Research	STTR funding awarded to Nanosonic was used by Chinese researchers who also received funding from state-backed Chinese research institutions.[30]

Figure 4: SBIR Mills and Award Dollars/Count (FY 2010-FY 2023) [31]

Company	Total SBIR-STTR Award Dollars	Award Count
Luna Innovations Inc.	$206,311,172	493
Triton Systems	$222,025,095	509
Lynntech Inc.	$175,425, 516	474
TDA Research, Inc.	$173,297,272	419
Kitware Inc.	$98,707,634	172
Nanosonic Inc.	$102,396,710	277

Figure 5: SBIR Mills and Award Dollars/Count (2023-2024)[32]

Company	Total SBIR-STTR Award Dollars	Award Count
Luna Innovations Inc.	$6,850,417	8
Triton Systems	$60,404,276	104
Lynntech Inc.	$31,960,426	61
TDA Research, Inc.	$38,119,898	62
Kitware Inc.	$28,393,474	28
Nanosonic Inc.	$12,692,435	34

Note: Foreign ties due diligence programs were operational at participating agencies by mid-2023

It is vital to safeguard taxpayer-funded research from being exploited by adversarial interests. Furthermore, SBIR mills are profiting to the tune of hundreds of millions of tax dollars and crowding out truly small start-ups, as they develop business relationships that enable CCP agents to have access to U.S. technological innovations. Congress must ensure that the SBIR-STTR programs serve a competitive set of small businesses and maintain strong research security protocols that safeguard American emerging technologies from exploitation.

Based on these findings, Senator Ernst's *INNOVATE Act* builds upon her previous work and takes important steps to ensure taxpayer-funded research remains secure:

1. Establishes a clear and consistent definition of "foreign risk" as a consistent baseline for due diligence review across all participating agencies: a foreign affiliation, technology licensing agreement, joint venture, contractual or financial obligation (pending or otherwise), investment agreement, research relationship (including co-authorship), or business relationship between a small business (including subsidiaries, spinoffs, and affiliates) submitting a SBIR or STTR proposal, its owner, or other key personnel and individuals or entities in a foreign country of concern within the last 10 years.[33]

2. Creates clear eligibility rules around foreign ties for SBIR-STTR applicants: requires a denial of awards for companies connected to adversarial entities on government sanctions lists, among other egregious adversarial ties.[34] Strengthens agencies' ability to deny awards to companies that pose a risk to national security at the discretion of the agency leadership.[35]

3. Codifies collaboration between participating agencies and the intelligence community and/or relevant inspectors general on due diligence reviews.[36]

4. Imposes a maximum $75 million cap on lifetime SBIR-STTR Phase I and Phase II awards.[37]

5. Strengthens agencies' ability to claw back SBIR and STTR awards when national security is at risk.[38]

Endnotes

[1] S. Comm. on Small Business, S. 881 - Small Business Innovation Research Act of 1981, S. Rep. No. 97-194, at 7, (Sep. 25, 1981) [hereinafter 1981 Comm. Report].

[2] Marcy E. Gallo, Cong. Rsch. Serv. (R43695), Small Business Research Programs: SBIR and STTR, (Oct. 21, 2022), *available at* https://crsreports.congress.gov/product/pdf/R/R43695.

[3] PROTECTING THE NATIONAL SECURITY INNOVATION BASE STUDY GROUP AND OSE/FACTOR 8 PROGRAM, SURVEY OF PRC STATE-SPONSORED TECHNOLOGY TRANSFERS AFFECTING SBIR PROGRAMS: A DOD CASE STUDY, (Apr. 2021), *available at* https://cdn01.dailycaller.com/wp-content/uploads/2023/10/%E2%80%8Esbtc.orgwp-contentuploads202205PNSIBStudy-DODSBIR-China-Study-FINAL.pdf.

[4] *Id at 4.*

[5] Kate O'Keefe, *Pentagon's China Warning Prompts Calls to Vet U.S. Funding of Startups,* WALL ST. J., (MAY 8, 2022), *available at* https://www.wsj.com/articles/pentagons-china-warning-prompts-calls-to-vet-u-s-funding-of-startups-11652014803.

[6] SBIR and STTR Extension Act of 2022, Pub. L. No. 117-183, 136 Stat. 2180.

[7] SBIR and STTR Extension Act of 2022, Pub. L. No. 117-183, §4(b)(2), 136 Stat. 2182.

[8] *See* Figure 1 and Figure 2; Letter from Joni K. Ernst, S. Comm. on Small Business and Entrepreneurship, to Alejandro Mayorkas, Secretary, DHS, (Nov. 5, 2024), *available at* https://www.ernst.senate.gov/imo/media/doc/ernst_letter_re_sbir_due_diligence_data_compiled.pdf; Letter from Joni K. Ernst, Ranking Member, S. Comm. on Small Business and Entrepreneurship, to Lloyd Austin, Secretary, DoD, (Nov. 5, 2024), *available at* https://www.ernst.senate.gov/imo/media/doc/ernst_letter_re_sbir_due_diligence_data_compiled.pdf; Letter from Joni K. Ernst, Ranking Member, S. Comm. on Small Business and Entrepreneurship, to Pete Buttigieg, Secretary, DOT, (Nov. 5, 2024), *available at* https://www.ernst.senate.gov/imo/media/doc/ernst_letter_re_sbir_due_diligence_data_compiled.pdf; Letter from Joni K. Ernst, Ranking Member, S. Comm. on Small Business and Entrepreneurship, to Miguel Cardona, Secretary, Dept. of Ed., (Nov. 5, 2024), *available at* https://www.ernst.senate.gov/imo/media/doc/ernst_letter_re_sbir_due_diligence_data_compiled.pdf; Letter from Joni K. Ernst, Ranking Member, S. Comm. on Small Business and Entrepreneurship, to Michael Regan, Adm'r, EPA, (Nov. 5, 2024), *available at* https://www.ernst.senate.gov/imo/media/doc/ernst_letter_re_sbir_due_diligence_data_compiled.pdf; Letter from Joni K. Ernst, Ranking Member, S. Comm. on Small Business and Entrepreneurship, to Bill Nelson, Adm'r, NASA, (Nov. 5, 2024), *available at* https://www.ernst.senate.gov/imo/media/doc/ernst_letter_re_sbir_due_diligence_data_compiled.pdf; Letter from Joni K. Ernst, Ranking Member, S. Comm. on Small Business and Entrepreneurship, to Monica Bertagnolli, Director, NIH, (Nov. 5, 2024), *available at* https://www.ernst.senate.gov/imo/media/doc/ernst_letter_re_sbir_due_diligence_data_compiled.pdf; Letter from Joni K. Ernst, Ranking Member, S. Comm. on Small Business and Entrepreneurship, to Laurie Locascio, Director, NIST, (Nov. 5, 2024), *available at*

https://www.ernst.senate.gov/imo/media/doc/ernst_letter_re_sbir_due_diligence_data_compiled.pdf; Letter from Joni K. Ernst, Ranking Member, S. Comm. on Small Business and Entrepreneurship, to Richard Spinrad, Adm'r, NOAA, (Nov. 5, 2024), *available at* https://www.ernst.senate.gov/imo/media/doc/ernst_letter_re_sbir_due_diligence_data_compiled.pdf; Letter from Joni K. Ernst, Ranking Member, S. Comm. on Small Business and Entrepreneurship, to Sethuraman Panchanathan, Director, NSF, (Nov. 5, 2024), *available at* https://www.ernst.senate.gov/imo/media/doc/ernst_letter_re_sbir_due_diligence_data_compiled.pdf; Letter from Joni K. Ernst, Ranking Member, S. Comm. on Small Business and Entrepreneurship, to Thomas Vilsack, Secretary, USDA, (Nov. 5, 2024), *available at* https://www.ernst.senate.gov/imo/media/doc/ernst_letter_re_sbir_due_diligence_data_compiled.pdf; Letter from Joni K. Ernst, Ranking Member, S. Comm. on Small Business and Entrepreneurship, to Jennifer Granholm, Secretary, DOE, (Nov. 5, 2024), *available at* https://www.ernst.senate.gov/imo/media/doc/ernst_letter_re_sbir_due_diligence_data_compiled.pdf.

[9] Letter from Thomas Vilsack, Secretary, USDA, to Joni K. Ernst, Ranking Member, S. Comm. on Small Business and Entrepreneurship, (Dec. 13, 2024) (on file with Comm.); Letter from Sethuraman Panchanathan, Director, NSF, to Joni K. Ernst, Ranking Member, S. Comm. on Small Business and Entrepreneurship, (Dec. 6, 2024) (on file with Comm.); Letter from Dmitri Kusnezov, Under Secretary, DHS, to Joni K. Ernst, Ranking Member, S. Comm. on Small Business and Entrepreneurship, (Dec. 6, 2024) ((on file with Comm.); Letter from Michael Lauer, Deputy Director for Extramural Research, NIH, to Joni K. Ernst, Ranking Member, S. Comm. on Small Business and Entrepreneurship, (Dec. 4, 2024) (on file with Comm staff); Letter from Maureen Gwinn, Acting Assistant Administrator for Research and Development, EPA, to Joni K. Ernst, Ranking Member, S. Comm. on Small Business and Entrepreneurship, (Dec. 19, 2024) (on file with Comm.); Letter from Robert Hampshire, Chief Science Officer, DOT, to Joni K. Ernst, Ranking Member, S. Comm. on Small Business and Entrepreneurship, (Nov. 20, 2024) (on file with Comm.); Letter from Laurie Locascio, Director, NIST, to Joni K. Ernst, Ranking Member, S. Comm. on Small Business and Entrepreneurship, (Nov. 21, 2024) (on file with Comm.); Letter from Alicia Brown, Associate Administrator for Legislative and Intergovernmental Affairs, NASA, to Joni K. Ernst, Ranking Member, S. Comm. on Small Business and Entrepreneurship, (Nov. 20, 2024) (on file with Comm.); Letter from Matthew Soldner, Acting Director, Institute for Education Sciences, Dept. of Education, to Joni K. Ernst, Ranking Member, S. Comm. on Small Business and Entrepreneurship, (Dec. 9, 2024) (on file with Comm.);

Letter from Heidi Shyu, Under Secretary for Research and Engineering, DoD, to Joni K. Ernst, Ranking Member, S. Comm. on Small Business and Entrepreneurship, (Dec. 16, 2024) (on file with Comm.); Letter from Kaitlyn Montan, Director of Legislative and Intergovernmental Affairs, NOAA, to Joni K. Ernst, Chair, S. Comm. on Small Business and Entrepreneurship, (Jan. 14, 2025) (on file with Comm.).

[10] *Id.*

[11] USDA, NASA, DoD, Dept. of Ed, NSF, EPA, NIST, NIH, NOAA, DOE, DHS, and DOT Briefings on SBIR-STTR Due Diligence Implementation to S. Comm. on Small Business and Entrepreneurship Staff, H. Comm. on Small Business Staff, and H. Comm. on Science, Space, and Technology Staff, (July 11-12, 2024).

[12] *Id.*

[13] SBA, *SBIR.gov Portfolio Award Data, available at* https://www.sbir.gov/awards.

[14] SBA, *SBIR.gov Portfolio Award Data, available at* https://www.sbir.gov/awards. Award dollar total from SBIR.gov database (FY 2024 data incomplete as the database is continually updated throughout the year. As a result, data for FY24 is not expected to be complete until March 2025.)

[15]GTL Technology & Service, *available at* http://www.gtlsvc.com/about.html, (last accessed Mar. 7, 2025).

[16] *CITIC Capital Acquisition Corp. Appoints Ross Haghighat to the Board,* MARKETSCREENER, (May 7, 2020), *available at* https://www.marketscreener.com/quote/stock/CITC-CAPI-105997940/news/CITIC-Capital-Acquisition-Corp-Appoints-Ross-Haghighat-to-the-Board-33878787/.

[17] Frank Esposito, *$22 million investment to help FRX grow in China,* PLASTICSNEWS, (Sept. 9, 2016), *available at* https://www.plasticsnews.com/article/20160909/NEWS/160909798/22-million-investment-to-help-frx-grow-in-china.

[18] Press Release, FRX Innovations, FRX Polymers and China's Yoo-Point Jointly Develop Water-Based Emulsions Containing Nofia Non-Halogenated Flame Retardants, (Apr. 29, 2019), *available at* https://web.archive.org/web/20240524172434/https://www.frx-innovations.com/news/frx-polymers%C2%AE-and-china's-yoo-point-jointly-develop-water-based-emulsions-containing-nofia%C2%AE-non-halogenated-flame-retardants.

[19] NOVEL LOW COST FIRE RESISTANT COMPOSITE FOR VARTM, *SBIR.gov Portfolio Award Data, available at* https://www.sbir.gov/awards/119181; SBA, SBIR.GOV PORTFOLIO AWARD DATA, *High Temperature Multifunctional Foam Core Materials, available at* https://www.sbir.gov/awards/119178; SBA, SBIR.GOV PORTFOLIO AWARD DATA *Enabling Hull Structural Innovations for High Speed Lighters, available at* https://www.sbir.gov/awards/119309.

[20] U.S. NAVY, OFFICE OF NAVAL RESEARCH, Navy SBIR/STTR Success: Fire Retardant Blast Mitigation for Sea Vessels, Triton Systems, *available at* https://www.navysbir.com/success/docs/Triton_Systems-N02-207.pdf

[21] WSJ MARKETS, *FRX Innovations Inc.*, (Accessed Mar. 5, 2025), *available at* https://www.wsj.com/market-data/quotes/FRXIF/company-people/executive-profile/78471647.

[22] Press Release, *Chinook Therapeutics Closes Merger with Aduro Biotech and Completes $115 Million Private Placement Financing*, GlobalNewsWire, (Oct. 5, 2009), *available at* https://www.globenewswire.com/news-release/2020/10/05/2103580/0/en/Chinook-Therapeutics-Closes-Merger-with-Aduro-Biotech-and-Completes-115-Million-Private-Placement-Financing.html.

[23] Ben Adams, *Chinook launches a new biotech with major VCs in China to double down on kidney disease R&D*, Fierce Biotech, (Nov. 30, 2021), *available at* https://www.fiercebiotech.com/biotech/chinook-launches-a-new-biotech-major-vcs-china-to-double-down-kidney-disease-r-d.

[24] WSJ MARKETS, *FRX Innovations Inc.*, (Accessed Mar. 5, 2025), *available at* https://www.wsj.com/market-data/quotes/FRXIF/company-people/executive-profile/78471647.

[25] PROTECTING THE NATIONAL SECURITY INNOVATION BASE STUDY GROUP AND OSE/FACTOR 8 PROGRAM, SURVEY OF PRC STATE-SPONSORED TECHNOLOGY TRANSFERS AFFECTING SBIR PROGRAMS: A DOD CASE STUDY, (Apr. 2021), *available at* https://cdn01.dailycaller.com/wp-content/uploads/2023/10/%E2%80%8Fsbtc.orgwp-contentuploads202205PNSIBStudy-DODSBIR-China-Study-FINAL.pdf.

[26] *Id.*

[27] Gokhan Alptekin, Pilot Testing of a Highly Efficiency Pre-combustion Sorbent-based Carbon Capture System, OSTI.GOV, (Dec. 26, 2022), *available at* https://www.osti.gov/biblio/1906977; National Carbon Capture Center (@NCarbonCaptureC), X, (Apr. 18, 2017, 12:06 PM EST), *available at* https://x.com/NCarbonCaptureC/status/854365567482040322;

NATIONAL PETROLEUM COUNCIL, MEETING THE DUAL CHALLENGE: A ROADMAP TO AT-SCALE DEPLOYMENT OF CARBON CAPTURE, USE, AND STORAGE APPENDIX F EMERGING CO2 CAPTURE TECHNOLOGIES PAGES F-12 F-16 (Dec. 12, 2019), *available at* https://www.energy.gov/sites/default/files/2021-06/2019%20-%20Meeting%20the%20Dual%20Challenge%20Vol%20III%20Appendix%20F.pdf.

[28] Press Release, Kitware, ITK/VTK Get Popular in China, (Oct 9, 2012), *available at* https://www.kitware.com/itkvtk-get-popular-in-china/.

[29] Yongsheng Yu et al, *Unbiased Multi-Modality Guidance for Image Inpainting*, ARXIV (Aug. 25, 2022), *available at* https://arxiv.org/pdf/2208.11844.

[30] Qingbo Wei et al, *Highly stable and efficient perovskite solar cells produced via high-boiling point solvents and additive engineering synergistically*, SPRINGER NATURE, (Apr. 14, 2020), *available at* https://link.springer.com/article/10.1007/s11426-019-9727-8; See "This work was supported by the National University Research Fund (GK261001009), the National Natural Science Foundation of China (61604090, 21663030), the Shaanxi Provincial Science and Technology Plan Project (2020JM-546), the Doctoral research initial funding from Yan'an University (YDBK2017-14), and the Natural Science Foundation of Yan'an University (YDQ2018-15). D. Y. acknowledged the financial support from Air Force Office of Scientific Research (FA9550-18-1-0233) and STTR Program (Nanosonic)."

[31] SBA, *SBIR.gov Portfolio Award Data, available at* https://www.sbir.gov/awards.

[32] SBA, *SBIR.gov Portfolio Award Data, available at* https://www.sbir.gov/awards (denoting award dollar total from SBIR.gov database but that FY 2024 data is incomplete as the database is continually updated throughout the year. As a result, data for FY24 is not expected to be complete until March 2025.)

[33] INNOVATE Act, S. 853, 119th Cong., § 401 (2025).

[34] *Id.* at § 402; See U.S. DEP'T OF HOMELAND SEC., *Uyghur Forced Labor Prevention Act Entity List*, *available at* https://www.dhs.gov/uflpa-entity-list; OFF. OF FOREIGN ASSETS CONTROL, U.S. DEP'T OF THE TREASURY, *Non-SDN Chinese Military-Industrial Complex Companies List*, *available at* https://home.treasury.gov/policy-issues/financial-sanctions/consolidated-sanctions-list/ns-cmic-list ; John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232 § 889, 132 Stat. 1636; William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283 § 1260H, 134 Stat. 3388, *available at* https://media.defense.gov/2025/Jan/07/2003625471/-1/-1/1/ENTITIES-IDENTIFIED-AS-CHINESE-MILITARY-COMPANIES-OPERATING-IN-THE-UNITED-STATES.PDF;

BUREAU OF INDUS. & SEC., U.S. DEP'T OF COM., Military End User List, 15 C.F.R. pt. 744, Supp. No. 7, *available at* https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-744/appendix-Supplement%20No.%207%20to%20Part%20744; BUREAU OF INDUS. & SEC., U.S. DEP'T OF COM., Entity List, 15 C.F.R. pt. 744, Supp. No. 4. *available at* https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-744/appendix-Supplement%20No.%204%20to%20Part%20744; FED. COMMC'NS COMM'N, *Covered Communications Equipment and Services List*, *available at* https://www.fcc.gov/supplychain/coveredlist; U.S. CUSTOMS & BORDER PROT., *Withhold Release Orders and Findings List*, *available at* https://www.cbp.gov/trade/forced-labor/withhold-release-orders-and-findings.

[35] INNOVATE Act, S. 853, 119th Cong., § 402 (2025).

[36] *Id.*

[37] *Id.* at § 201.

[38] *Id.* at § 404.

Senate Committee on Small Business and Entrepreneurship Hearing
July 23, 2025
Follow-Up Questions for the Record

Questions for de La Bruyère

Questions from:

Chair Ernst

Examining Chinese Shell Companies

QUESTION 1:

Ms. de la Bruyère, how well do current U.S. defense and economic security frameworks track opaque structures such as Chinese shell companies, particularly where partial foreign ownership hides behind U.S. corporate registrations in high-stakes sectors?

Existing US defense and economic security frameworks do not adequately track opaque structures such as Chinese shell companies – or Chinese indirect, partial, and second-order investment and ownership. For instance, US due diligence efforts, and third-party suppliers thereof, tend to focus on surface level, direct Chinese threat vectors and to be reactive rather than anticipatory. The US needs to flip the script. We need due diligence frameworks and approaches that a) account for the indirect and opaque nature of China's threat and b) are anticipatory, to keep pace with the adaptive nature of Beijing's offensive. This is a standard that any entity that vets recipients of federal funding should be held to. There is also an opportunity here for the US government, including the intelligence community, to share open source information to facilitate risk identification, assessment, and prevention on the part of both private sector and government entities.

Adversarial Influence in Government Supply Chains

QUESTION 2:

Ms. de la Bruyère, the federal government contracts with more than 100,000 businesses annually who provide critical goods and services across our government ecosystem. What are the potential ramifications of failing to secure our government supply chains from foreign adversarial influence?

Failure to secure government supply chains from foreign adversarial influence threatens US national and economic security – as well as our ability to compete for next generation technologies and industry. Supply chain dependence on foreign adversaries grants those adversaries influence over the United States; the ability to pressure, coercive, and, ultimately, disrupt or deny. Foreign adversaries can also use their presence in the United States and US government supply chains to access critical information, infrastructure, and technology.

Moreover, at the most fundamental level, industrial capacity today is a necessary condition for technological innovation tomorrow. Those who control supply chains determine the direction in which they, and the sectors that depend on them, evolve. Those who produce in today's critical industries will be able to identify – and capture – their next generation innovations.
In other words, a weak industrial base undermines US competitive positioning in the here and now. It also relinquishes America's future competitiveness.

Questions from:

Senator Scott

QUESTION 1:

Given the documented inconsistencies in agency implementation of foreign ties due diligence in the SBIR-STTR programs, what steps should Congress take to ensure uniform and robust application of national security protections across all participating agencies?

In order to ensure uniform and robust application of national security protections across all agencies participating in the SBIR-STTR programs, Congress should provide clear standards and best practices for robust due diligence of foreign ties. And – not only in the SBIR and STTR programs but across federal funding initiatives – Congress should incentivize agencies to implement those best practices, including by penalizing those that they fail to do so: An agency that does not vet against national security concerns should see budgetary and programmatic implications.

Such an approach would lean on agencies to do the work for which they are responsible and qualified. And it would avoid creating new bureaucratic entities or processes that risk over-complicating government systems and retarding the very innovation that the SBIR and STTR programs are intended to support.

QUESTION 2:

How can we ensure that additional due diligence requirements do not substantially increase the administrative burden put on small businesses during the SBIR application process?

Businesses should know their vendors, customers, and investors. This is not an undue responsibility – especially for businesses supporting the US government.
At the same time, information sharing on the part of government entities can facilitate – and enhance – the implementation of due diligence requirements. The intelligence community, for instance, could be tasked with sharing open-source information on adversarial supply chains, corporate networks, and technology ecosystems with businesses. This would improve companies' access to relevant data while also disseminating best practices with respect to vetting and risk assessment.

QUESTION 3:

If implemented, how might the INNOVATE Act affect interagency coordination on SBIR awards, particularly in identifying and mitigating risk across agencies?

The INNOVATE Act provides a framework and standard for assessing adversarial risk to be leveraged across agencies involved in the SBIR/STTR program. And that framework could – and should – ultimately inform due diligence and risk assessment across federal government programs not just the SBIR/STTR programs. The US government needs this. Washington needs to adopt a unified, coordinated approach both to competing with and defending against China.

Questions from:

Senator Cantwell

Tech NATO

Much of the attention on China has been with the goal of denying Chinese access to American innovation. In some cases we may need to do that, and do it with our allies, as Ms. De La Bruyère has written. But China is also developing very competitive advanced technologies – for example, their progress with DeepSeek. And China is pushing for its technology to be adopted by countries across the globe. We must accelerate our investment in research and innovation and increase cooperation with allies to stay competitive in the global race for emerging technology.

QUESTION 1:

I have been advocating for a technology alliance, something like a Tech NATO, where governments with aligned interests adopt technologies from trusted vendors in areas such as artificial intelligence and quantum computing. Those technologies would adhere to certain standards – for instance, no government back doors. Do you support the concept of an alliance with like-minded countries, or Tech NATO, to establish and set the rules of the road and create new markets for trusted vendors?

I certainly support the concept of an alliance with like-minded countries to establish and set the technological and industrial rules of the road and create new markets for trusted vendors. And in any such effort to coordinate across allies and partners, there should be guardrails to ensure that the standard for trusted technologies is sufficiently high, insulated from adversarial co-option, and enforced – as well as that allies and partners are appropriately defending against second-order risks (e.g., Chinese indirect investment).

To that end, alliances of this sort should be framed around meeting a best-in-class standard for technological competition and defense – not sinking to the level of the lowest common denominator. The United States can use partnerships like this, as well as trade agreements, bilateral tech partnerships, and access to the US market, to incentivize allies and partners to adopt more robust competitive stances, and corresponding protections, against foreign

adversaries. Participation could, for instance, be contingent on implementing trade restrictions against and ending tech partnerships with China.

Questions from:

Senator Booker

National Security

As global competition intensifies and national security concerns grow, Chinese investment in U.S. companies, particularly those in sensitive or emerging technology sectors, has come under increasing scrutiny. At the same time, small American businesses, often the drivers of innovation, face mounting challenges in protecting their intellectual property and maintaining technological security in a rapidly evolving international landscape.

QUESTION 1:

What are the risks associated with Chinese investment in U.S. companies, especially in sensitive or emerging technology sectors?

Chinese investment – direct and indirect – in US companies grants the PRC access to American technology, information, and profits. Investment also grants China influence over those companies, with it the ability to shape their development trajectories, business models, and partnerships. And Chinese investment seeds an overarching dependence on the PRC that prevents both the investment targets themselves and their larger ecosystems from competing with America's strategic adversary.

QUESTION 2:

How has Congress responded to the threats facing small businesses, particularly regarding IP protection, foreign investment, and technology security? What further action is recommended or necessary?

Thus far, while Congress has correctly diagnosed the threats that foreign adversaries pose to small businesses, the response has been tactical where it should be strategic. Robust standards for due diligence in federal funding programs, export controls and other technology protections, and identification of high-risk Chinese actors are all important. But they amount to a scalpel at a gun fight. To protect US small businesses – and US national and economic security, more generally – Congress has to take real, strategic action to remove the People's Republic of China from the American market.

Such a strategic push should start from Congressional re-consideration and ultimate revocation of China's permanent normal trade relations status. Corresponding efforts should include restrictions on direct and indirect investment; joint ventures, including minority stakes, and tech licensing; access to federal funding; and construction and deployment of information systems, components, and software that could give the PRC access to US information and data. These

restrictions should adopt definitions of Chinese entities that Beijing cannot circumvent through shell companies or localization — for example, the US Commerce Department's definition of a "person owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary" — and presumptions of denial.

At the same time, Congress should ensure that American, ally, and partner companies free from foreign adversary exposure have the opportunity to thrive in the United States. Congress can do so by providing energy and other infrastructure necessary for production, a functional regulatory environment, and a free and fair market defended from Chinese distortion.

CSET CENTER *for* SECURITY *and* EMERGING TECHNOLOGY

Questions for the Record from Chair Joni Ernst
and Senators Tim Scott, Maria Cantwell, and Cory Booker
for Dr. William Hannas
"Innovation in the Crosshairs: Countering China's Industrial Espionage"

William C. Hannas
Research Professor
Georgetown University

September 29, 2025

The Honorable Joni Ernst
Chair, Committee on Small Business & Entrepreneurship
United States Senate

Dear Chair Ernst and Esteemed Committee Members:

Thank you for the opportunity to respond to your follow-up questions regarding testimony I provided to your Committee July 23, 2025 on "Innovation in the Crosshairs: Countering China's Industrial Espionage." My replies follow.

(Senator Ernst)

Question 1: *Dr. Hannas, from your perspective, what targeted federal policy tools—such as investment incentives, enhanced trade enforcement, or procurement reform—could help level the playing field for small manufacturers facing subsidized foreign competition?*

Using trade disincentives and global forums to penalize unfair competitors may be a lost cause, as evidenced in the USTR's failed remedies in the Eastman Kodak vs. Fuji Film debacle of the 1990s. Better to "fight poison with poison" (以毒攻毒) by adapting China's highly successful practice of state-subsidized "commercialization centers" that support aspiring small businesses and entrepreneurs that have promising technology.

These centers are brick-and-mortar facilities ranging from small buildings to acres-wide and stories-tall complexes, spread over China and numbering some 900 (last time we counted). They are managed jointly by local government and business associations and become eligible for state support on fulfilling certification criteria. Their aim is to create a hospitable environment for individuals and small businesses—low taxes, free use of equipment, no-cost utilities, deferred or interest-free loans, and zero-to-little rent—that facilitates transitioning ideas into products. We detail the evolution of this system in our book "Chinese Industrial Espionage" (2013).

The centers are one of many tools China uses to support smaller businesses trying to market innovative technology. When a new class of technology becomes identified, guidelines are issued by state-level bodies[1] explaining in broad terms how it should be developed. Decisions are not made *ex cathedra* but reflect the views of scientists and their institutions that emerged previously in public statements and published research. While basic science gets some attention, the guidelines tend to promote concrete applications. These state edicts, in turn, inform the type of support provided by municipal governments, which take up the gauntlet at the local level.[2]

Finally, China's national and local governments sponsor websites aimed at matching people, who have technology to offer, with Chinese firms seeking technologies for commercial and military projects. While we do not often recommend PRC practices, these state-backed efforts to support business enterprise at the grassroots level may be worth emulating.

(Senator Scott)

Question 1*: Given the documented inconsistencies in agency implementation of foreign ties due diligence in the SBIR-STTR programs, what steps should Congress take to ensure uniform and robust application of national security protections across all participating agencies?*

If large American corporations can fall prey to China's myriad techniques to extract proprietary technology, what hope do smaller businesses have?

ODNI's National Counterintelligence and Security Center made early and promising strides in drawing attention to the problem, but it lacks the infrastructure (and budget) to grapple with this matter on the scale needed. NSF's SECURE program, while a step in the right direction, is focused more on academic research security, less on smaller businesses.

We recommend establishing a national center within or accountable to the U.S. federal government—but *outside* existing Title 50 organizations—to (1) collect data on China's tech acquisition venues, practices, and personnel and (2) use this data to serve as a national resource for the U.S. government, businesses and universities by responding to queries (supporting due diligence), and *pushing out* information as a public service.

Detailed data on China's foreign technology acquisition infrastructure was at one time gathered within the USIC but never transitioned from government archive to the public domain due to security and legal concerns, even though the information was derived entirely from open sources. We state this not as criticism but as evidence that the ability to build and run such a facility is well within our national grasp, albeit something we have not taken seriously.

Question 2*: How can we ensure that additional due diligence requirements do not substantially increase the administrative burden put on small businesses during the SBIR application process?*

---

[1] Typically, China's State Council or the China Natural Science Foundation.

[2] For example, Beijing Municipal Science and Technology Commission, "Beijing Embodied Intelligent Technology Innovation and Industry Cultivation Action Plan (2025-2027)" (北京具身智能科技创新与产业培育行动计划（2025-2027 年）的通知) https://www.beijing.gov.cn/zhengce/zhengcefagui/202503/t20250304_4024579.html.

See above. These services should be provided free of charge to legitimate U.S. consumers.

***Question 3**: If implemented, how might the INNOVATE Act affect interagency coordination on SBIR awards, particularly in identifying and mitigating risk across agencies?*

The proposed national information clearinghouse—the basis for which can be inferred from or specifically called out within the INNOVATE ACT—would support coordination between USG entities exercising oversight while addressing the needs of national enterprises.

Due diligence must be conducted not only by technology providers but also by USG contract managers. We cannot assume all U.S. persons and organizations are naïve in their dealings with China, or that the short-term interests of U.S. manufacturers and exporters necessarily align with longer term U.S. national interests. CFIUS manages only a fraction of these cases and lacks the data to make well-informed judgments.

***Question 4**: The Committee report found several SBIR recipients with known links to China still received awards. Are agencies currently equipped with the right tools and intelligence-sharing procedures to effectively identify and address these risks?*

It's all hit-or-miss. We take seriously military defense of the United States. This threat is just as serious and demands appropriate national attention and resourcing, something it currently lacks.

The problem is partly lack of commitment and partly institutional. The USIC is not disposed to share with the public information derived from classified sources. This problem is compounded by the tendency of Title 50 organizations to focus on the classified genres they are budgeted to exploit, which do not include open sources except as an "enabler" of classified research, and not something pursued for its intrinsic value. Efforts to address this imbalance quickly fizzle out as the agencies revert to what they do best—obtaining the adversary's secrets.

Open sources, however, are where most of the information on China's technology transfer practices is found, including the identities and affiliations of bad actors. It is also *shareable* with businesses. The optimum solution is a mix of open and classified sources, but locating the former task within agencies chartered to pursue the latter is doomed to fail—as it has in the past.

Hence our recommendation for an independent national open source analysis center tasked to monitor foreign technology developments and alert the USG and private enterprises to foreign attempts to appropriate technology.

(Senator Cantwell)

***Question 1**: I have been advocating for a technology alliance, something like a Tech NATO, where governments with aligned interests adopt technologies from trusted vendors in areas such as artificial intelligence and quantum computing. Those technologies would adhere to certain standards – for instance, no government back doors. Do you support the concept of an alliance*

with like-minded countries, or Tech NATO, to establish and set the rules of the road and create new markets for trusted vendors?

We're aligned here. My GU team interacts with private and government-sponsored think tanks in Great Britain, Germany and Japan—i.e., the "other" major technology innovators—and we hear similar calls for a coordinated approach in technology planning in the active sense that you describe and reactive sense of blocking unwanted accesses by China—the open, covert, and "extralegal" practices we've written about. Our proposal for a national open source analysis center aimed at detecting foreign (Chinese) technical advances and mitigating unwanted tech acquisitions by monitoring tech transfer networks assume collaboration with allies.

We have seen multiple instances in which the United States has been able to deny China (easy) access to technology only to witness China turning to U.S. allies to source the same capabilities. So, while we agree some sort of U.S.-led technical alliance among advanced democratic nations would be productive, it must be done with the help of a data-driven shared "watchboard" to elucidate in a timely fashion the threats we commonly face.

Question 2: *You have written about the risks that China is acquiring and stealing foreign technology. You also said in your testimony that the only sure way out is to rebuild U.S. research, entrepreneurship, and productive capacity. Can you expand on that?*

Mitigation is a zero-sum game. At best you are holding the line, buying time. We need to recover our lead in S&T as the only sure guarantor of national security. Here are some ways:

(1) Restore and expand national and local government funding for hardcore science, both basic research and applications-oriented. Hardly a week goes by in which my team does not see some famous U.S. or allied country scientist pulling up roots and moving to China. It's not just the lure of better compensation; nowadays it's a matter of survival for many scientists.

(2) Make science and technology careers more prestigious and aspirational in society and our education system. We need to restore the notion—even expectation—that STEM degrees are the rule, not the exception, and the raison d'être for higher education.

(3) Finally, I mentioned above China's subsidizing of technical startups through "innovation centers" and "commercialization centers," which we should also look into seriously.

In sum, you don't get S&T overlordship for free. It doesn't "emerge" on its own by maintaining the proverbial open-and-free society.

(Senator Booker)

Question 1*: 1 What more can Congress do to support small businesses and entrepreneurs who are dealing with IP theft? How do small, medium, and large enterprises differ in their ability to protect intellectual property (IP) and defend against cyber or corporate espionage threats?*

This question overlaps with others and I am glad the Committee is giving it the attention it deserves. Our proposed national "clearinghouse" meant to track foreign tech appropriation and provide alerts to American companies would be particularly helpful to smaller firms that lack the resources and savvy to protect their intellectual assets.

***Question 2**: How is artificial intelligence (AI) impacting the capabilities of both small businesses and of Chinese influence operations? Does it empower innovation or expose them to new risks such as IP theft or cyber vulnerabilities?*

We testified earlier to a House committee about the unholy relationship between AI and foreign tech appropriation. AI-enabled cyber exploits are a growing feature of China's illegal transfer efforts directed against U.S. high tech generally and AI technology in particular. The purloined AI technology in turn helps China's AI progress. I (and many others) question whether smaller U.S. companies have adequate knowledge and resources to defend against professional state-sponsored attacks.

***Question 3**: How does U.S. support for AI startups compare to China's approach? As AI ecosystems evolve, does the structure of support and regulation in each country give one a competitive edge, and should this matter to U.S. policy and business strategy?*

Large tech firms in the U.S. are the major beneficiaries of government AI support, whereas in China it seems to be more even-handed, spreading their support to smaller startups with the expectation that a couple of these might become the next generation of leading tech companies. There is an inherent dilemma here that we're not sure how to solve, namely, we all have a big stake in AI safety but restrictions in one country—the United States—meant to slow progress toward artificial general intelligence (AGI) gives an advantage to other countries—China—less encumbered by "western-style" safety protocols.

Although China has publicly declared its commitment to safe AI development, the Chinese term for "safety" (安全, ānquán) also denotes "security" in the sense of "national security" (国家安全), that is, the two are a single concept. Much of what we have seen suggests the latter concern is the dominant motivation.

Also, there is a myth circulating in the western press that China is more concerned with building AI applications than with winning an AGI race. The truth is China's AI decision-makers on all levels—scientists and policymakers—*see no contradiction between the two goals* and believe strongly that embodying AI in physical applications will expedite their realization of AGI, which is an articulated state-sponsored goal.

Please feel free to call on my team if we may be of further assistance.

Respectfully yours,

William C. Hannas
wh451@georgetown.edu

○