

Congress of the United States

Washington, DC 20515

October 20, 2025

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

Dear Secretary Hegseth,

We write with grave concern that America's national security is at risk due to existing loopholes leaving critical taxpayer-funded defense technologies vulnerable to malign foreign influence. These gaps are opportunities for adversarial nations, particularly China, to continue systematically exploiting and stealing taxpayer-funded innovation for military, technological, and strategic gain.

In 2021, a bombshell Pentagon report detailed how the Chinese Communist Party (CCP) had infiltrated key small business research and development programs to steal U.S. taxpayer-funded technology.¹ This alarming study revealed the CCP deployed several tactics targeting American innovators, including recruiting U.S. employees into malign talent recruitment programs, directing investments in U.S.-based startups for the benefit of Chinese firms, and luring U.S. firms to establish Chinese subsidiaries that were subsequently exploited.²

With no formalized vetting required, Congress enacted long-overdue safeguards in the *SBIR and STTR Extension Act of 2022 (P.L. 117-183)* to require agencies to collect disclosures from applicants and evaluate Small Business Innovation Research (SBIR) - Small Business Technology Transfer (STTR) proposals for potential foreign ties.³ Recognizing the need for stronger safeguards, then-Deputy Secretary of Defense Kathleen Hicks issued a risk matrix in 2024 to guide Pentagon services and components in carrying out these reviews.⁴ The then-Office of the Undersecretary of Defense for Research & Engineering (R&E) also established a risk matrix for fundamental research outside of SBIR-STTR in 2023.⁵

¹ 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-content/uploads202205PNSIBStudy-DODSBIR-China-Study-FINAL.pdf>.

² *Id.*

³ *SBIR and STTR Extension Act of 2022*, Pub. L. No. 117-183, 135 Stat. 2180 (2022).

⁴ DEP'T OF DEFENSE, DEPUTY SECRETARY OF DEFENSE, MEMORANDUM FOR SENIOR PENTAGON LEADERSHIP DEFENSE AGENCY AND DOD FIELD ACTIVITY DIRECTORS (May 13, 2024), *available at* https://media.defense.gov/2024/May/23/2003471996/-1/1/1/DUE_DILIGENCE_PROGRAM_OSD003584_24_RES.PDF.

⁵ DEP'T OF DEFENSE, OFFICE OF UNDERSECRETARY OF DEFENSE FOR RESEARCH AND ENGINEERING, INTRODUCTION TO POLICY ON RISK-BASED SECURITY REVIEWS OF FUNDAMENTAL RESEARCH (June 8, 2023), *available at* <https://rt.cto.mil/wp-content/uploads/2025/03/Policy-on-Risk-Based-Security-Reviews-of-Fundamental-Research.pdf>.

Despite these measures, the U.S. House of Representatives Select Committee on Strategic Competition between the United States and the Chinese Communist Party (Select Committee) has produced multiple investigative reports documenting a continued, pervasive exploitation by China's defense research and industrial base entities across the Pentagon's fundamental research, development, and technology ecosystems.⁶ The Select Committee revealed significant shortcomings within the Pentagon's Research & Engineering (R&E) risk matrix that have left taxpayer-funded defense research vulnerable to exploitation by China.⁷

The establishment of a foreign ties due diligence program in the *SBIR and STTR Extension Act of 2022* required agencies to brief Congress every 30 days until implementation was complete.⁸ Through the briefings and oversight work, the Senate Small Business Committee majority confirmed the problem: foreign-ties reviews are riddled with loopholes and produced wildly inconsistent results across the Pentagon.

In some cases, applicants with the exact same background were judged "high-risk" by one component but "low-risk" by another, leading to completely different award decisions.⁹ Even more troubling, the Pentagon's own risk matrix classifies several strong foreign connections, including employee affiliations, prior research ties, or links to sister companies, as merely "low-risk" or "medium-risk," meaning they often escape any mitigation or denial.¹⁰

Out of 522 applications at the Pentagon flagged for having a foreign risk in 2023 and 2024, only 152 applications were denied on the basis of that risk.¹¹ Even worse, some agencies denied 100% of flagged applicants, while others denied less than 1%.¹² These risks spanned from patent and employee analysis flags to flags concerning financial ownership or financial obligations.¹³

This status quo is unacceptable. Our findings indicate that R&E's risk matrices are inadequate and unreliable. The policies contain gaps that permit high-risk collaborations—including with

⁶ STAFF OF SELECT COMM. ON THE CCP, 118TH CONG., INVESTIGATION REPORT - CCP ON THE QUAD: HOW AMERICAN TAXPAYERS AND UNIVERSITIES FUND THE CCP'S ADVANCED MILITARY AND TECHNOLOGICAL RESEARCH (Comm. Print 2024), available at <https://selectcommitteeontheccp.house.gov/media/investigations/investigation-report-ccp-quad-how-american-taxpayers-and-universities-fund>; see also STAFF OF SELECT COMM. ON THE CCP, 119TH CONG., FOX IN THE HENHOUSE, (Comm. Print 2025), available at <https://selectcommitteeontheccp.house.gov/media/investigations/fox-in-the-henhouse>.

⁷ STAFF OF SELECT COMM. ON THE CCP, 119TH CONG., FOX IN THE HENHOUSE, (Comm. Print 2025), available at <https://selectcommitteeontheccp.house.gov/media/investigations/fox-in-the-henhouse>.

⁸ *SBIR and STTR Extension Act of 2022*, Pub. L. No. 117-183, 135 Stat. 2180, Sec. 4 (2022).

⁹ Letter from the Honorable Emil Michael, Undersec. of Def. for Res. and Eng., Dep't of Defense, to Joni K. Ernst, Chair, S. Comm. on Small Business and Entrepreneurship, (Sept. 3, 2025), available at https://www.ernst.senate.gov/imo/media/doc/re_response_to_ernst.pdf.

¹⁰ Dep't of Defense, Deputy Secretary of Defense, Memorandum for Senior Pentagon Leadership Defense Agency and DOD Field Activity Directors (2024), available at https://media.defense.gov/2024/May/23/2003471996/-1/1/1/DUE_DILIGENCE_PROGRAM_OSD003584_24_RES.PDF.

¹¹ 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.).

¹² STAFF OF S. COMM. ON SMALL BUSINESS AND ENTREPRENEURSHIP, CRITICAL AMERICAN TECHNOLOGY VULNERABLE TO CHINA, INVESTIGATION ALERT: URGENT REFORMS NEEDED IN SBIR PROGRAM TO PROTECT NATIONAL SECURITY 9, (May 2025), available at https://www.ernst.senate.gov/imo/media/doc/sbir_report.pdf.

¹³ *Id.*

China's defense institutions—to move forward unchecked. Instead of fully safeguarding U.S. military advantages, these deficiencies have, in practice, enabled China's military modernization and surveillance capabilities—ultimately risking that American innovation could be turned against U.S. service members in future conflicts.

Demonstrating the systemic nature of this problem, the Select Committee identified roughly 1,400 research papers published between June 2023 and June 2025 that acknowledged receiving Pentagon funding while also involving Chinese entities. These publications were tied to more than \$2.5 billion in Pentagon funding spread across hundreds of fundamental research grants.¹⁴ Of the 1,400 publications, over 700 publications were conducted in partnership with entities affiliated with China's defense research and industrial base.¹⁵

- Two 2025 publications on neural mechanisms, co-authored by researchers from Washington University in St. Louis and China's Peng Cheng Laboratory (鹏城实验室), were funded by the Air Force Office of Scientific Research, the National Science Foundation, and the National Institutes of Health. Peng Cheng Laboratory is a Chinese state-directed research institution that operates CloudBrain-II, a high-performance AI supercomputing platform used to support large-scale computational research across disciplines, including cybersecurity and machine learning. The lab has the "Pengcheng Shooting Range", and the "ultra-large-scale multi-field integration of key technologies and systems of the Federal Shooting Range (Pengcheng Network Shooting Range) designed to achieve disruptive technological innovation. References to "shooting range" typically refers to offensive and defensive cyber and information warfare environments.¹⁶
- A 2024 publication on high-strength alloys research funded by the U.S. Office of Naval Research's Additive Manufacturing Alloys for Naval Environments (AMANE) program was co-authored by a researcher from China's Central South University-State Key Laboratory of Powder Metallurgy, identified in Chinese as 粉末冶金国防重点实验室/粉末冶金国家重点实验室. This laboratory carries a defense designation, as reflected by the Chinese characters for "national defense" (国防, Guófáng) in its official name. This lab conducts research on high-temperature alloys for jet turbines (used for fighter jets and missiles), ultra-high temperature carbides for hypersonic vehicles, high-entropy alloys for armor-piercing applications, ballistic impact on various materials, and materials for stealth technology. The research on laser powder bed fusion of high-strength alloys outlined in this publication has direct defense applications across a range of critical systems and technologies, including the production of lightweight, durable components for armor systems, aircraft structures, ground vehicle platforms, and naval applications.¹⁷

While the SBIR and STTR Extension Act of 2022 was a strong start, Congress must finish the job. No more excuses, time to stand up to China.

¹⁴ STAFF OF SELECT COMM. ON THE CCP, 119TH CONG., FOX IN THE HENHOUSE, (Comm. Print 2025), available at <https://selectcommitteeontheccp.house.gov/media/investigations/fox-in-the-henhouse>

¹⁵ *Id.*

¹⁶ *Id.*

¹⁷ *Id.*

The Honorable Pete Hegseth

October 20, 2025

Page 4 of 4

Congress must reform the SBIR-STTR programs to protect sensitive intellectual property from malign foreign influence (as proposed in H.R. 4777, the *INNOVATE Act*) by closing the remaining loopholes that allow America's adversaries to reap the benefits of taxpayer-funded innovation. To fully secure the research powering America's national security, Congress must also pass the *SAFE Research Act* to stop our tax dollars from aiding our adversaries.¹⁸

The Trump Administration has a chance to reverse Biden-era policies and strengthen American research security. Our review has identified recommendations to address shortcomings in Pentagon policy, due diligence, training, and access to critical information.¹⁹ We stand ready to assist and are committed to ensuring 100% of taxpayer dollars for critical technology development serves our warfighters and America's national interest.

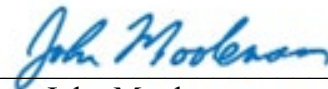
In light of these concerns, please provide responses to the following questions no later than November 3, 2025:

1. Is the Pentagon concerned with the inadequacies in the existing risk matrices? If so, please describe Pentagon plans to amend policy guidance.
2. Does the Pentagon need additional statutory authority to standardize definitions of foreign risk and create minimum eligibility standards to access taxpayer-funded R&D awards?

Sincerely,



Joni K. Ernst
Chair
U.S. Senate Committee on
Small Business & Entrepreneurship



John Moolenaar
Chairman
U.S. House Select Committee on
Strategic Competition between the United
States and the Chinese Communist Party

CC: The Honorable Emil Michael, Under Secretary of War for Research and Engineering,
Department of War

¹⁸ *INNOVATE Act*, H.R. 4777, 119th Cong. (2025), available at <https://www.congress.gov/bill/119th-congress/house-bill/4777>; see also *SAFE Research Act*, 119th Cong. (2025), available at https://amendments-rules.house.gov/amendments/MOOLEN_163_xml250828161843908.pdf?_gl=1*rvsd0r*_ga*MjI3Njg4MzQuMTc0MDA2NDkwMg.*_ga_N4RTJ5D08B*czE3NTc2MTQ1NDkkbzIzJGcxJHxNzU3NjE0NTU1JGo1NCRsMCRoMA.

¹⁹ STAFF OF H. SELECT COMM. ON THE CCP, 119TH CONG., *FOX IN THE HENHOUSE* 52-58, (Comm. Print 2025), available at <https://selectcommitteeontheccp.house.gov/media/investigations/fox-in-the-henhouse>; see also STAFF OF S. COMM. ON SMALL BUSINESS AND ENTREPRENEURSHIP, *CRITICAL AMERICAN TECHNOLOGY VULNERABLE TO CHINA, INVESTIGATION ALERT: URGENT REFORMS NEEDED IN SBIR PROGRAM TO PROTECT NATIONAL SECURITY* 9, (May 2025), available at https://www.ernst.senate.gov/imo/media/doc/sbir_report.pdf.