AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

ASSESSING THE THREAT TO U.S. FUNDED RESEARCH

HEARING

BEFORE THE

SUBCOMMITTEE ON INVESTIGATIONS AND OVERSIGHT

OF THE

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

OF THE

HOUSE OF REPRESENTATIVES

ONE HUNDRED NINETEENTH CONGRESS

FIRST SESSION

MARCH 5, 2025

Serial No. 119–4

Printed for the use of the Committee on Science, Space, and Technology

Available via the World Wide Web: http://science.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE

58–978PDF WASHINGTON : 2026

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

HON. BRIAN BABIN, Texas, *Chairman*

RANDY WEBER, Texas
JIM BAIRD, Indiana
DANIEL WEBSTER, Florida
JAY OBERNOLTE, California
CHUCK FLEISCHMANN, Tennessee
DARRELL ISSA, California
CLAUDIA TENNEY, New York
SCOTT FRANKLIN, Florida
MAX MILLER, Ohio
RICH MCCORMICK, Georgia
MIKE COLLINS, Georgia
VINCE FONG, California
DAVID ROUZER, North Carolina
KEITH SELF, Texas
PAT HARRIGAN, North Carolina
SHERI BIGGS, South Carolina
JEFF HURD, Colorado
MIKE HARIDOPOLOS, Florida
MIKE KENNEDY, Utah
NICK BEGICH, Alaska
VACANT

ZOE LOFGREN, California, *Ranking Member*
SUZANNE BONAMICI, Oregon
HALEY STEVENS, Michigan
DEBORAH ROSS, North Carolina
ANDREA SALINAS, Oregon
VALERIE FOUSHEE, North Carolina
EMILIA SYKES, Ohio
MAXWELL FROST, Florida
GABE AMO, Rhode Island
SUHAS SUBRAMANYAM, Virginia
LUZ RIVAS, California
SYLVESTER TURNER, Texas
SARAH MCBRIDE, Delaware
LAURA GILLEN, New York
GEORGE WHITESIDES, California,
Vice Ranking Member
LAURA FRIEDMAN, California
APRIL MCCLAIN DELANEY, Maryland
JOSH RILEY, New York

SUBCOMMITTEE ON INVESTIGATIONS AND OVERSIGHT

HON. RICH MCCORMICK, Georgia, *Chairman*

DANIEL WEBSTER, Florida
DARRELL ISSA, California
PAT HARRIGAN, North Carolina
NICK BEGICH, Alaska

EMILIA SYKES, Ohio,
Ranking Member
SUZANNE BONAMICI, Oregon
LUZ RIVAS, California

C O N T E N T S

March 5, 2025

Page

Hearing Charter 2

Opening Statements

Statement by Representative Rich McCormick, Chairman, Subcommittee on Investigations and Oversight, Committee on Science, Space, and Technology, U.S. House of Representatives 10
Written Statement 11

Statement by Representative Emilia Sykes, Ranking Member, Subcommittee on Investigations and Oversight, Committee on Science, Space, and Technology, U.S. House of Representatives 12
Written Statement 13

Statement by Representative Brian Babin, Chairman, Committee on Science, Space, and Technology, U.S. House of Representatives 14
Written Statement 16

Statement by Representative Zoe Lofgren, Ranking Member, Committee on Science, Space, and Technology, U.S. House of Representatives 17
Written Statement 18

Witnesses:

Mr. John F. Sargent Jr., Retired, Specialist in Science and Technology Policy, Congressional Research Service
Oral Statement 19
Written Statement 22

Mr. Jeffery Stoff, President, Center for Research Security & Integrity
Oral Statement 40
Written Statement 42

Dr. Maria Zuber, E.A. Griswold Professor of Geophysics and Presidential Advisor for Science and Technology Policy, MIT
Oral Statement 84
Written Statement 86

Discussion 95

Appendix I: Answers to Post-Hearing Questions

Mr. John F. Sargent Jr., Retired, Specialist in Science and Technology Policy, Congressional Research Service 112

Mr. Jeffery Stoff, President, Center for Research Security & Integrity 132

Dr. Maria Zuber, E.A. Griswold Professor of Geophysics and Presidential Advisor for Science and Technology Policy, MIT 139

Appendix II: Additional Material for the Record

Article submitted by Representative Emilia Sykes, Ranking Member, Subcommittee on Investigations and Oversight, Committee on Science, Space, and Technology, U.S. House of Representatives
"Exclusive: US intel shows Russia and China are attempting to recruit disgruntled federal employees, sources say," Natasha Bertrand, Katie Bo Lillis and Zachary Cohen, CNN 148

ASSESSING THE THREAT TO U.S. FUNDED RESEARCH

WEDNESDAY, MARCH 5, 2025

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON INVESTIGATIONS AND OVERSIGHT,
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY,
Washington, D.C.

The Subcommittee met, pursuant to notice, at 10 a.m., in room 2318 of the Rayburn House Office Building, Hon. Rich McCormick [Chairman of the Subcommittee] presiding.

COMMITTEE ON
SCIENCE, SPACE
AND TECHNOLOGY
CHAIRMAN BRIAN BABIN

SUBCOMMITTEE ON INVESTIGATIONS & OVERSIGHT

HEARING CHARTER

Assessing the Threat to U.S. Funded Research

Wednesday, March 5, 2025
10:00 a.m.
2318 Rayburn House Office Building

Purpose
The hearing will assess the current threat to the U.S. research enterprise posed by malign foreign actors. This includes the risk to federal, state, non-governmental institutions, and academia. The hearing will explore trends and tactics used to steal, exploit, and undermine U.S. science, research, development, and deployment.

Witnesses:
- **John F. Sargent Jr.,** Retired, Specialist in Science and Technology Policy, Congressional Research Service
- **Jeffrey Stoff,** Founder and President, Center for Research Security & Integrity
- **Dr. Maria Zuber,** E.A. Griswold Professor of Geophysics and Presidential Advisor for Science and Technology Policy, MIT

Background:

The scientific community generally views the free and open exchange of information as vital to the process of scientific inquiry.[1] Since Vannevar Bush's *Science: The Endless Frontier (1945)*, the United States has built our national research strategy around these ideals. Unfortunately, foreign threat actors have abused this openness, stealing scientific innovation through illicit means. Various efforts of foreign governments—most notably the Chinese Communist Party (CCP)—have aimed to influence and exploit the openness of the U.S. research ecosystem. The acquisition of U.S. advances in science and technology, intellectual property, and talent by foreign adversaries like the CCP undermines our global economic competitiveness. Balancing transparency, openness, and collaboration with the protection intellectual property and critical technologies remains a challenge.

CCP Research Collection Tactics:

Three beginning and necessary key points:

(1) The CCP is the most prolific user of these tactics, but other countries do as well;

(2) The tactics being used by all of these nations are varied, constantly changing, and are not limited to criminal activity or traditional espionage.[2] The CCP specifically is using an "all of nation" approach that is outlined in multiple CCP government documents.[3] Through this "all of nation" approach the CCP has implemented laws requiring all government entities, companies, organizations, and citizens to "pick[] flowers in foreign lands to make honey in China;"[4] and

(3) The research being acquired is not limited to any one sector and most targets are considered fundamental research that is not classified or otherwise being conducted in secure facilities. [5]

Though the gathering tactics vary and are always changing, historically the CCP has used programs such as the Thousand Talents Plan (TTP) to "recruit[] science and technology professors, researchers, students, and others—regardless of citizenship or national origin—to apply for talent plans."[6] Researchers, professors, and other individuals with expertise in or access to research and technology, which China lacks access to or is behind competitively are preferred. Researchers and other "[p]articipants enter into a contract with a Chinese university, researcher, or company—often affiliated with the Chinese government—that usually requires them to: subject themselves to Chinese laws; share new technology developments or breakthroughs only with China (they can't

---

[1] Significant portions of this charter were taken from a CRS brief: Emily G. Blevins, Marcy E. Gallo, Congressional Research Services, *Research Security Policies: An Overview*, IF12589, Dec. 4, 2024, at https://crs.gov/Reports/IF12589?source=search

[2] *Id.*

[3] *Id.*

[4] Presidential Memorandum on U.S. Government Supported Research and Development National Security Policy, President Donald Trump, Jan. 14, 2021, available at https://trumpwhitehouse.archives.gov/presidential-actions/presidential-memorandum-united-states-government-supported-research-development-national-security-policy/ (referenced as "NSPM-33"); *see also* *Foreign Threats to Taxpayer-Funded Research: Oversight Opportunities and Policy Solutions* hearing before the S. Comm. on Fin. 116th Cong. June 5, 2019 (statement for Charirman Chuck Grassley) https://www.finance.senate.gov/imo/media/doc/Grassley%20NIH%20Opening%20Statement_v7.pdf.

[5] Nicholas Eftimiades, *Chinese Intelligence Operations*, 1st Ed., Taylor and Francis, 2017.

[6] Fed. Bureau of Investigation, *The China Threat*, Counterintelligence News, last viewed Feb. 25, 2025, available at https://www.fbi.gov/investigate/counterintelligence/the-china-threat/chinese-talent-plans.

share this information with their U.S employer or host without special authorization from China); and recruit other experts into the program—often their own colleagues."[7] U.S. researchers are barred from being a part of these types of programs and accepting foreign funds, *if* they are also accepting funds from the US government.[8] When a researcher is found to have accepted funds from both the U.S. and other countries of concern, the U.S. can, and has, barred the offending researcher from accepting any further U.S. funds.[9] Though a seemingly logical response from the U.S. government, this can have negative consequences – giving U.S. researchers reason to go abroad and get funded by foreign adversaries such as the CCP. Some researchers in this position have been approached by the CCP and offered significant packages to move their operations to China.[10]

Some talent recruitment plans are less blatant than the TTP was or otherwise simply look less nefarious. These programs can also go beyond just a single researcher and target entire organizations or universities. Recently, U.C. Berkley was caught participating in just such a program and openly partnered with CCP affiliated universities.[11] "In exchange for monetary contributions, U.C. Berkeley officials offered exclusive tours of cutting-edge semiconductor research facilities to Chinese delegations. These delegations included Chinese researchers as well as multiple senior Chinese government officials. This is especially troubling given that there are no divisions between China's government and its business and academic community, and the CCP has publicly disclosed that its plan to surpass the U.S. in science and technology involves stealing the results of our research, whether through foreign talent programs, forced acquisition, or other illicit means."[12] In addition to receiving support from the Chinese government, U.C. Berkeley explored additional funding opportunities with dozens of Chinese companies, including Huawei, ZTE and DJI, all of which were later sanctioned by the U.S. government.[13]

The U.S. Response[14]

Congress and the executive branch have initiated actions intended to preserve the benefits of an open research environment while securing it from external threats by foreign governments.[15] In 2019, the National Defense Authorization Act (NDAA) for Fiscal Year 2020[16] directed federal agencies, among other things, to develop descriptions of known and potential threats to federally funded research and development (R&D) and to the integrity of the U.S. scientific enterprise. In

---

[7] *Id.*
[8] *Id.*
[9] *Id.*
[10] *Id.*
[11] Press Release, H. Comm. on Sci., Space, and Tech. Science, Committee Leaders Want Answers on UC Berkeley's Failure to Disclose Gifts from the Chinese Government (Jun. 1, 2023), https://science.house.gov/2023/6/science-committee-leaders-want-answers-on-uc-berkeley-s-failure-to-disclose-gifts-from-the-chinese-government; *see generally* The Select Committee on the CCP, *How American Taxpayers and Universities Fund the CCP's Advanced Military and Technological Research*, Congressional Report, Sept. 23, 2024, available at CCP on the Quad: How American Taxpayers and Universities Fund the CCP's Advanced Military and Technological Research | Select Committee on the CCP (referenced as "Select Committee Report").
[12] *Id.*
[13] *Id.*
[14] *See generally*, https://www.aau.edu/sites/default/files/AAU-Files/Key-Issues/Science-Security/Actions-Taken-Research-Security.pdf.
[15] CRS, *Supra* note 1.
[16] P. L. 116-283.

January 2021, President Trump issued National Security Presidential Memorandum 33 (NSPM-33).[17] Following this action, in January 2022, the Biden Administration issued guidance to federal agencies on the implementation of NSPM-33.[18]

This charter summarizes key developments in five selected research security policy areas: disclosure requirements; foreign talent recruitment programs; research security training and program requirements; information sharing and risk assessment; and university biases and enforcement deficiencies.

Disclosure Requirements

Congress and the executive branch have worked to strengthen existing policies and institute new requirements for applicants for federal R&D funding, specifically, what must be disclosed regarding foreign support. While these disclosure requirements are a good start, given the extent of the issues with illicit activities by the CCP and other threat actors, there is more that must be done.

In January 2021, with the enactment of the NDAA for FY2021,[19] Congress directed federal agencies to require applications for federal R&D funding to include a disclosure of all current and pending research support. It also made universities accountable for ensuring faculty are aware of these disclosure requirements and they are accurate. Congress also tasked the Office of Science and Technology Policy (OSTP) with the responsibility of ensuring that disclosure requirements are consistent across federal agencies.

Under NSPM-33, section 4(b)(vi) listed specific information agencies must require funding applicants to disclose and reaffirmed the need for agency coordination.[20] The 2022 NSPM-33 implementation guidance elaborated that funding applicants should disclose "all resources made available, or expected to be made available, in support of the individual's [R&D] efforts."[21] This would include both domestic and foreign support, both monetary and in kind. In November 2023, the National Science Foundation (NSF) released the Biographical Sketch Common Form and the Current and Pending (Other) Support Common Form to assist in the collection of these required disclosures.[22] In February 2024, an additional change was implemented. OSTP directed all federal agencies with annual extramural research expenditures over $100 million to require grant and cooperative agreement applications to include the forms.[23]

---

[17] NSPM-33, President Donald Trump, Jan. 14, 2021, available at https://trumpwhitehouse.archives.gov/presidential-actions/presidential-memorandum-united-states-government-supported-research-development-national-security-policy/

[18] NATIONAL SCIENCE AND TECHNOLOGY COUNCIL, GUIDANCE FOR IMPLEMENTING NATIONAL SECURITY PRESIDENTIAL MEMORANDUM 33 (NSPM-33) ON NATIONAL SECURITY STRATEGY FOR U.S. GOVERNMENT-SUPPORTED RESEARCH AND DEVELOPMENT, SUBCOMMITTEE ON RESEARCH SECURITY AND JOINT COMMITTEE ON RESEARCH ENVIRONMENT, JANUARY 2022. (referenced as "NSPM-33 Guidance").

[19] P.L. 116-283.

[20] NSPM-33, President Donald Trump, Jan. 14, 2021, available at https://trumpwhitehouse.archives.gov/presidential-actions/presidential-memorandum-united-states-government-supported-research-development-national-security-policy/

[21] *Id.*

[22] Off. Management and Budget (OMB), Biographical Sketch Common Form, Nov. 1, 2023, at https://www.doi.gov/sites/default/files/documents/2024-07/biographical-sketch-common-form-doi-omb-3145-0279.pdf

[23] CRS, *Supra* note 1.

The FY21 NDAA directed agencies to require covered individuals, as defined in NSPM-33 implementation guidance, to update their disclosure information during the term of the award, as determined by the agency.[24] Yet the NSPM-33 implementation guidance form defers to individual agency policies on the frequency and timing of the post-award disclosure requirements.[25]

Counter Foreign Talent Recruitment Programs

Not only has the executive branch and Congress required disclosure of foreign support, but they have also issued specific policies governing both federal employee and grantee participation in foreign talent recruitment programs. The CHIPS and Science Act[26] directs agencies to establish policies: (1) to require covered individuals such as principal investigators to disclose if they are party to a foreign talent recruitment program contract; and (2) to the extent practicable, require federal R&D funding recipients including universities to prohibit covered individuals from participating in malign foreign talent recruitment programs and from working on projects supported by federal R&D awards. This statute also prohibits all personnel of federal research agencies from participating in foreign talent recruitment programs.

Section 10632 of the CHIPS and Science Act specified that, not later than August 9, 2024, federal research agencies should establish policies requiring an R&D award proposal to include: (1) certification from covered individuals that they are not a party to a malign foreign talent recruitment program, as part of the initial submission and annually throughout the award; and (2) certification from an institution of higher education or other organization applying for the award that each covered individual employed by the entity has been made aware of and is in compliance with the malign foreign talent recruitment program disclosure requirements.

Within this process, each individual identified as a senior or key person on a federally funded research project must complete the Biographical Sketch Common Form.[27] This form currently requires applicants to certify that "at the time of submission" they are not involved in a malign foreign talent recruitment program.[28]

In February 2024, OSTP issued uniform guidance to inform agency implementation of statutory prohibitions on foreign talent recruitment program participation in compliance with CHIPS requirements. The guidance indicates that although statutory prohibitions pertain to current and/or ongoing program participation, agencies may "apply mitigation and management measures to address past participation."[29]

---

[24] P.L 116-283.
[25] NSPM-33, President Donald Trump, Jan. 14, 2021, available at https://trumpwhitehouse.archives.gov/presidential-actions/presidential-memorandum-united-states-government-supported-research-development-national-security-policy/
[26] P.L. 117-167.
[27] OMB, *Supra* note 22.
[28] *Id.*
[29] CRS, *Supra* note 1.

Research Security Training and Program Requirements

To ensure compliance and implementation of these research security policies, the executive branch and Congress developed research security training and program requirements. For example, research institutions receiving more than $50 million per year in federal science and engineering support were required under NSPM-33 to certify that they have established and operate a research security program with the parent agency.[27] The required research security programs were to include "elements of cyber security, foreign travel security, insider threat awareness and identification, and, as appropriate, export control training."

Additionally, the CHIPS and Science Act directs agencies to require specified individuals applying for R&D awards to complete research security training annually.[30] OSTP was directed to coordinate with relevant research agencies to develop research security training modules and to issue guidelines for institutions in developing research security training programs. In January 2024, NSF released four interactive online research security training modules to be used by U.S. researchers and institutions.[31]

OSTP released guidance in 2024 for federal agencies detailing methods of implementation of the research security program requirements established by NSPM-33 and the CHIPS and Science Act.[32] The guidance established "as a standardized requirement" that federal agencies require covered institutions to certify that their research security programs include specific elements related to the four categories listed in NSPM-33.[33] The guidance also directed federal agencies to clearly communicate program requirements with covered institutions and to ensure access to training, materials, and other resources needed to fulfill such requirements.

The OSTP guidance also established implementation deadlines. In implementing the new, standardized research security program requirements, each agency is required to submit a plan detailing how it will update its policies to reflect the new guidance and requirements, which were due by January 9, 2025. It also directs agencies to require covered institutions to implement research security programs no later than 18 months after the date that they submitted their plan to OSTP.

Information Sharing and Risk Assessment

Along with the training and program requirement, NSPM-33 directed agencies to share information about individuals and institutions that violate disclosure policies to improve identification and response to research security threats. Similarly, NSF announced the establishment of the Safeguarding the Entire Community of the U.S. Research Ecosystem (SECURE) Center to "serve as a clearinghouse for information to empower the research

---

[30] P.L. 117-167.

[31] National Science Foundation, Research Security Training, modules, last viewed Feb. 25, 2025, available at www.nsf.gov/research-security/training.

[32] Off. Science and Technology Policy, *COGR Overview of OSTP Guidelines for Research Security Programs at Covered Institutions*, Feb. 25, 2025, at https://www.cogr.edu/sites/default/files/Overview%20of%20OSTP%20Guidelines%20for%20Research%20Security%20Programs%20at%20Covered%20Institution%20clean%20copy%20july%2012%202024%20REVISED.pdf

[33] *Id*.

community to identify and mitigate foreign interference that poses risks to the U.S. research enterprise." Congress has also directed individual agencies to develop risk assessment tools and frameworks to manage and mitigate security risks.

Issues within Academia

While it is not entirely the fault of U.S. academia, China's efforts to exploit, influence, and corrupt our research ecosystem have been enabled and amplified in some part by the willing participation of universities. While the federal government has not been a party without fault, numerous universities have been disturbingly complicit in the syphoning of our research through various forms. Some of which include lack of awareness, negligence in taking responsibility for identifying and mitigating issues, willful violations of integrity, and the disregard of grant rules and conditions that have been implemented to ensure fairness and reasonable allocation of federal resources. Through NSPM-33 many universities have implemented changes and put programs in place to fortify research security, but initial implementation lacked specific guidance. OSTP eventually released additional guidance at the end of last year to inform implementation. But more must be done to address the threat.

Department of Energy, NASA, and other Agencies[34]

The Department of Energy (DOE), NASA, and other agencies within the Committee's jurisdiction have implemented congressional directives as well as NSPM-33, but threats to federally funded research continues to advance. In the National Defense Authorization Act FY2024, Congress further directed DOE to restrict access to foreign individuals from countries of risk to protect research activities at the National Laboratories. Despite these newly enacted measures, hostile actors have evolved their tactics to gain access to DOE researchers, government-funded technologies, and federal dollars through contracts and grants.[35] The CCP is also investing billions of dollars in key emerging technology areas in hopes to supplant the leadership of United States research and development. Their hope is over the next few decades to have world leading science facilities that will attract researchers from around the world to China.[36]

Enforcement

Generally, enforcement mechanisms do not come into effect until there has been proof of illicit activity. Many cases of breaches in research security have been prosecuted through other crimes such as securities fraud, wire fraud, or espionage. Yet many cases where research is most vulnerable is through these "gray" activities. Through the partnerships mentioned above between researchers and universities, the CCP steals important information. The best mechanism for enforcement is through the False Claims Act (FCA).[37] The FCA has an extremely broad

---

[34] *See generally*, https://science.house.gov/2025/2/from-transformative-science-to-technological-breakthroughs-doe-s-national-laboratories.

[35] "Strategic Environment." National Security Agency, 3 May 2016, www.nsa.gov/About/Strategic-Environment/.

[36] 6 Atkinson, Robert D. "China Is Rapidly Becoming a Leading Innovator in Advanced Industries." Information Technology and Innovation Foundation | ITIF, 16 Sept. 2024, itif.org/publications/2024/09/16/china-is-rapidlybecoming-a-leading-innovator-in-advanced-industries/.

[37] Robert Metzger, *Software and Supply Chain Assurance Forum, Regulated Cybersecurity: Where We Are. The Consequences of Non-Compliance,* Homeland Security, National Defense, Commerce and Standards, General Services, June 1, 2023, at

jurisdiction that applies to anyone who, "knowingly presents, or causes to be presented, a false or fraudulent claim approval"; or for payment or "knowingly makes, uses, or causes to be made or used, a false record or statement false or fraudulent claim."[38] These cases can be brought by the government or through whistleblowers under *qui tam* suits.[39] But even this framework does not encompass the struggle to enforce consequences for research security noncompliance.

https://csrc.nist.gov/csrc/media/Presentations/2023/regulated-cybersecurity-the-consequences-of-non-co/images-media/RMetzger-ssca-forum-060123.pdf

[38] *Id.*

[39] *Id; see* generally https://kkc.com/product/rules-for-whistleblowers/.

Chairman MCCORMICK. The Subcommittee on Investigations and Oversight will come to order. Without objection, the Chair is authorized to declare recess in the Subcommittee at any time. I'd like to now recognize myself for 5 minutes for opening remarks.

And first of all, I'd like to thank you all, my guests, for coming here today on my first chair. It's exciting to have here some delightful experts in our oversight, and it's also an honor to have my Ranking Member Sykes here with me today.

I want to lay out our objectives and how we're going to run our Committees from here on out. In reference to former Chair Gallagher in a Subcommittee I was a part of, we'll start on time, we'll stay on time, and we'll not use acronyms to the best of our abilities because most people don't understand acronyms, even the people that use them, I've found, in the military.

I even practiced this too, so this is great.

All right. Our country is in a unique position to collect talent from all over the world. I think this is one of our greatest strengths for the last several decades, and it's made us this amazing hodgepodge of talent, and it's really accelerated our country and technologies and our ability to lead the rest of the world to collect ideas from all over the world and to accelerate that process through our educational system.

It has also made us a target. When you look at the people who are immigrating here to do education, we have about a million students here every year. A large portion of them are from countries that are our peers and our rivals and that take that technology back to their countries, and we have to be careful of that or we'll lose our position.

In case you haven't been keeping up with our educational system, it's ranked, I think, 40th in the world right now. It's not a good position to be, even when you're in the lead. You can't just steal talent and stay in front of everybody else. And when you're giving your information to other countries willingly—and I think there's something to be gained from collaboration. I think that's a good thing, but you have to be careful. You have to be smart if you're running a business or a country.

I think when we have the unique and changing ways, especially in advanced technologies, AI (artificial intelligence), quantum, and everything else that we're teaching our children in schools now, we have to be very, very quick to put guardrails on that to make sure that we stay in the leading edge of technologies and that we continue to be competitive and actually lead the rest of the world.

One of the things I realized that the CCP (Chinese Communist Party) has done is they refer to our fruits as their honey. They literally say they're coming up and suckling at that nectar if you will, absorbing that pretty much at cost. They don't have to invest in it. They just get to take it back to their country and benefit from it. That doesn't necessarily benefit the United States, though. When you have foreign companies and professors and other people coming here to pick the flowers in foreign lands to make honey in China, that doesn't well—bode well for us. And we need to make sure that this is not only a quote, but realize that this is the mantra of the CCP right now.

I think we need to continue to slow the leaks, make sure we protect our technologies, and provide opportunities for our homegrown students who will remain in America and be the future of our technologies when we talk about developing our oversight for this—for these technologies.

Starting with what is firmly within our control, we should review Federal regulations that are seen both as too burdensome and also those that are too lenient, work with researchers and research institutions to implement new methods to ensure accountability is enhanced and improved as we go forward. And we also need to ensure that grant awards have contractual mechanisms to certify that background checks on staff are done.

And one thing that maybe you don't realize, when I was an associate professor at Georgia Tech and Morehouse, we had foreign instructors. We had foreign students, matter of fact, a large portion of them, and there's a financial advantage to that. But I was also used as an investigator or to help investigate from the FBI (Federal Bureau of Investigation) a foreign national instructor who was then arrested because they were stealing secrets. This is a real thing, and this—and that was a couple decades ago. It hasn't gotten better. It's gotten worse, and we need to be careful.

Our Nation's premier research institutes have been an all-you-can-eat buffet for other countries right now, and especially our adversaries. We cannot let this metaphorical buffet continue, or we risk ceding our dominance in innovation in scientific research. I look forward to the witnesses' testimony today informing our Committee on the steps we can take to reverse these current vulnerabilities and enlighten us on what we can do better.

[The prepared statement of Chairman McCormick follows:]

Our country is unique in that we attract the most brilliant minds around the world to study and learn here. This quality raises the bar domestically and has allowed us as a nation to be leaders of innovation. Unfortunately, this has also made us a target. Countries that do not play fair and want to thwart our intellectual property laws and other domestic protections are finding unique and ever-changing ways to acquire our innovations. This not only unfairly inflates the profitability of these foreign companies, but it also discourages and stifles progress at home.

America's innovation is threatened by carelessness and the prying eyes of our adversaries. The Chinese Communist Party (CCP) has made it clear they are taking an "all of country" approach to acquire sensitive information as early as possible and as quickly as possible. They have referred to the fruits of our innovation as "honey" and told the entirety of their country: researchers, professors, grad students, companies, and school children alike that they should "pick flowers in foreign lands to make honey in China." This is not only a quote, but a mantra by the CCP to their academic and commercial base.

The age of this quote and the number of times Congress has had hearings like this should underscore the fact that research security is not a new issue. For the last 20 years we as government have taken the issue seriously, especially as it applies to the CCP. U.S. taxpayers should not be subsidizing Chinese research and development, ever. Congress and the executive branch have made efforts, both legislative and administrative, to slow the leaks and combat the problem.

Despite research security being directly tied to our national security and advancement, our efforts seem to have achieved limited success.

We can look at the following opportunities for improvement:

- Starting with ourselves, we should review federal regulations that are both too "burdensome" and "lenient" at the same time.
- Researchers and research institutions are not diligent enough with mitigating threats of research security, we need new methods to ensure this accountability is enhanced and iterated on.
- Grant awards need to be paired with contractual mechanisms to ensure oversight is conducted and appropriate enforcement actions are taken on violators.

Our goal here today is to learn about the state of play and determine how we can adjust and do better. I fear that our nation's premier research institutions have been all-you-can-eat buffets which our adversaries are using to consume untold numbers of innovative ideas. If this issue is not taken seriously here, we risk ceding our dominance in innovation and scientific research.

In today's hearing, I look forward to the witnesses' testimony informing the Committee on what steps we need to take next to reverse the current vulnerabilities.

Chairman MCCORMICK. With that, I yield to the Ranking Member.

Mrs. SYKES. Thank you, Chair McCormick, and congratulations on your chairmanship of this Subcommittee. Your practice rounds served you well. I also look forward to working with you and the entire Subcommittee for ensuring that we have robust and productive meetings in order to help serve the science community for our country.

Before I start my remarks, I do want to take the time to express my condolences for the loss of one of the Members of our full Committee, Sylvester Turner, who passed away last night. He represented the State of Texas and was formerly the Mayor of Houston. And my husband and I have known him for some time, and I can't even begin to express the sadness that we feel, not only for the city of Houston, for his family, but for this country who has lost a great man, a great patron, and a great American. So if you have a moment to send up a prayer or thoughts of words of comfort for him and his family and his community, on behalf of the Democrats in this Committee. And hopefully, I speak for the full Committee in expressing my condolences.

For years, this Committee has led the way in promoting sensible and responsible research security policy. America did not become the world leader in science because we cowered from our adversaries. We became the world leader because we created a welcoming research environment that set the standard of how global science is conducted. And while we are proud of these values, we are also aware that adversarial governments, including the People's Republic of China (PRC), often take advantage of our system and exploit its openness. But our response should not be to let our opponents fundamentally change our American scientific culture, and in turn, make it difficult for our researchers to address our most pressing national challenges.

As a proud Representative of Ohio's 13th Congressional District in northeast Ohio, I know what's at stake. Ohio's 13th is home to a tech hub that received $51 million in *CHIPS and Science* investment to leverage Akron's national leadership in polymer science and sustainable polymers. From sustainable tires to cutting-edge polymers, the next generation of rubber and plastic products will happen in my district.

This opportunity was not, however, created in a vacuum. It was made possible by fundamental researchers around the world working together on chemistry and engineering. Researchers at the University of Akron worked on these fundamental chemistry problems within a global science community, and we have benefited from international partnerships, and we welcome the best minds from around the world to allow our Nation and our expertise to grow.

Of course, we recognize that there are valid research security concerns, and this Committee has worked in a bipartisan way to

address these issues, including through the landmark *CHIPS and Science Act* that was passed in a bipartisan way, and we will continue to fight to maintain the *CHIPS and Science Act.* I know we heard some contrary conversation yesterday at the address from the President.

Among its many actions, *CHIPS and Science* authorized the National Science Foundation (NSF) to maintain a research security office that works closely with law enforcement intelligence communities to address many of these concerns from a Federal agency perspective. This office, in conjunction with efforts from other SST (Science, Space, and Technology) agencies in the White House Office of Science and Technology Policy (OSTP), has created research security training modules, created frameworks to assess grant proposals for national security risks, and issued commonsense disclosure forms for use across grantmaking agencies.

Since the Committee began looking at this issue in 2018, universities have also stepped up to the plate, examining their own research enterprise and identifying ways to make it more secure. MIT (Massachusetts Institute of Technology), for example, compiled a report in 2022 that investigates how our premier research institutions can promote research security while preserving open scientific research, open intellectual exchange, and the free flow of ideas and people. I look forward to hearing about Dr. Zuber's experience co-chairing the National Academies' roundtable where academies, industry, law enforcement, and intelligence community worked to come to a common understanding of research, security threats, and best practices.

It is my hope that this Committee continues to be a productive place to hold these very important conversations, particularly as we are witnessing attacks to the very core of our Federal research enterprise. Just as we must be clear-eyed about the threat posed by foreign adversaries, I hope my colleagues on both sides of the aisle don't shy away from speaking out when their own government weakens the United States' standing on the international stage. If we do not maintain American leadership in science and technology (S&T), we will lose what is worth protecting in the first place. And if we don't lead, someone else will follow. I would prefer the United States leads.

Thank you very much, Mr. Chair. Thank you to the Committee Members, to the staff for what I know will be a productive Congress. Thank you to our witnesses for being here. And, Mr. Chair, I yield back.

[The prepared statement of Mrs. Sykes follows:]

Thank you, Chairman McCormick—and congratulations on your Chairmanship of this Subcommittee. Also, thank you to our witnesses for appearing today. For years, this committee has led the way in promoting sensible and responsible research security policy.

America did not become the world leader in science because we cowered from our adversaries, we became the world leader because we created a welcoming research environment that set the standard of how global science is conducted. While we are proud of these values, we are also aware that adversarial governments, including the People's Republic of China, often take advantage of our system and exploit its openness. But our response should not be to let our opponents fundamentally change our American scientific culture, and in turn, make it difficult for our researchers to address our most pressing national challenges.

As a proud representative of Ohio's 13th District, I know what's at stake. Ohio's 13th is home to a Tech Hub that received $51 million in *CHIPS & Science* investment to leverage Akron's national leadership in polymer science. From sustainable tires to cutting-edge polymers, the next generation of rubber and plastics production will happen in my district. This opportunity was not created in a vacuum. It was made possible by fundamental researchers around the world working together on chemistry and engineering. Researchers at the University of Akron worked on these fundamental chemistry problems within a global science community. We have benefited from international partnerships, and we welcome the best minds from around the world to grow our national expertise.

Of course, we recognize that there are valid research security concerns, and this committee has worked in a bipartisan way to address these issues, including through the landmark *CHIPS and Science Act.* Among its many actions, *CHIPS and Science* authorized the National Science Foundation to maintain a Research Security Office that works closely with law enforcement and intelligence communities to address many of these concerns from a federal agency perspective.

This office, in conjunction with efforts from other SST agencies and the White House Office of Science and Technology Policy, has created research security training modules, created frameworks to assess grant proposals for national security risks, and issued common disclosure forms for use across grant-making agencies.

Since the Committee began looking at this issue in 2018, universities have also stepped up to the plate, examining their own research enterprise and identifying ways to make it more secure. MIT, for example, compiled a report in 2022 that investigates how our premier research institutions can promote research security while preserving open scientific research, open intellectual exchange, and the free flow of ideas and people.

I look forward to hearing about Dr. Zuber's experience co-chairing the National Academies roundtable, where academics, industry, law enforcement, and the intelligence community worked to come to a common understanding of research security threats and best practices. It is my hope that this Committee continues to be a productive place to hold these important conversations, particularly as we are witnessing attacks to the very core of our federal research enterprise.

Just as we must be clear-eyed about the threat posed by foreign adversaries, I hope that my colleagues on both sides of the aisle don't shy away from speaking out when our own government weakens U.S. standing on the international stage. If we do not maintain American leadership in science and technology, we will lose what is worth protecting in the first place.

Thank you, I yield back.

Chairman MCCORMICK. Thank you, Ranking Member Sykes. It's a pleasure. And with that, I recognize Chair Babin. And thank you for joining us today this morning, sir, for your opening remarks.

Chairman BABIN. Thank you, Mr. Chairman, really appreciate it. And the first thing I want to say is—excuse me. Man, I'm sorry. I want to thank Ranking Member Sykes for that news, very sad. I want to express my condolences at the loss of former Mayor and our fellow Member of this Committee of Sylvester Turner. I'm absolutely shocked. I knew he had been having some health problems, but I did not know that we were going to lose him at this early date like this. I just want to say how sorry I am about it. I've worked with him for several years now and really appreciated his service as Mayor of Houston. He was a go-to guy, and he was nice. He was always a gentleman. I just want to say how much I appreciated his service. I'm sorry for his family and just shocked that we've lost him. And anyway, thank you for telling us about that.

I want to thank our witnesses as well for being here and joining us to discuss a very serious, relevant topic, the security threats to our Federal research enterprise. America's leadership in science and technology was built on the foundation of Federal investment in basic research. These investments have enhanced our national security, strengthened our economy, and improved the lives of our citizens. Our unique research ecosystem, which combines Federal,

academic, and private R&D (research and development) efforts, drives America's advancement in science and technology. However, for this system to work, we need a degree of open science that facilitates collaboration and transparency. The challenge is ensuring this openness does not compromise our research security.

Although the United States has greatly profited from international scientific collaboration and the contributions of foreign-born scientists, other countries, both friend and foe, are also benefiting from U.S. investments. And while our goal is to ensure that all federally funded scientists adhere to the U.S. principles of scientific fairness and integrity, regardless of race or citizenship status, it is important to recognize that not all nations share these values.

As this Committee is well aware, the Chinese Communist Party, or CCP, is determined to surpass the United States as the global leader in science and technology by 2050 and by any means necessary, including espionage, theft, or forced acquisition. And I think history has borne that out, that they're willing to do whatever it takes.

The theft of our basic research poses a significant risk to our global competitiveness, handing our cutting-edge innovations to adversaries and undermining both our economy and our ability to lead in discovery. This is no idle threat, and it creates a serious strategic challenge. The CCP has been explicit about its efforts to steal our research results to further its technological progress.

A 2023 survey by the Center for Strategic International Studies (CSIS) found 224 reported instances of Chinese espionage directed at the United States, and more than 1,200 lawsuits were filed by U.S. companies against Chinese entities for intellectual property (IP) theft since 2000. In fact, even the Chinese consulate was closed in Houston, Texas, where my district is, from Houston over to Louisiana. It was closed back during the first Trump Administration for some of these very reasons. For the instances of espionage where the actor and intent were known, 49 percent of incidents directly involved Chinese military or government employees, 46 percent involved cyber espionage, 29 percent sought to acquire military technology, and 54 percent targeted commercial technologies.

This Committee has passed multiple bills to protect American research. Some of this legislation directed the Office of Science and Technology Policy to coordinate efforts and standardize requirements across all Federal science agencies to provide a strong framework for research security. However, the previous Administration failed to execute this framework within the directed timeline, missing deadlines by over a year in some cases, and provided little to no coordination and no community engagement.

The government needs clear and uniform guidance for our agencies and researchers, and I'm confident that this second Trump Administration will continue the good work of its previous term and reopen communication channels. Effective communication between law enforcement agencies and universities is paramount to securing our research enterprise. Universities need to know when researchers are targeted by nefarious actors, and law enforcement should be aware of the participants and conflicts of interest within our academic research ecosystem.

This collaboration should also extend to our technology transfer systems. Startups are an important part of our S&T enterprise and present a vulnerability that our global competitors are exploiting. While universities can track licenses derived from on-campus research, they lack transparency about the startup's investors. For instance, a foreign entity could access sensitive research through early investment in a startup before the technology license is even granted, thereby avoiding a review by the Federal Committee on Foreign Investment in the United States, or CFIUS. Clearly, this is a complex task that requires thoughtful consideration, but I believe that we are up to this challenge.

I look forward to hearing from our witnesses today and how we can assess and monitor these threats to our scientific research enterprise. And, Mr. Chairman, I'd like to yield back.

[The prepared statement of Chairman Babin follows:]

I want to thank our witnesses for joining us today to discuss a very serious and relevant topic: the security threats to our federal research enterprise.

America's leadership in science and technology was built on the foundation of federal investment in basic research. These investments have enhanced our national security, strengthened our economy, and improved the lives of our citizens.

Our unique research ecosystem, which combines federal, academic, and private R&D efforts, drives America's advancement in science and technology.

However, for this system to work, we need a degree of open science that facilitates collaboration and transparency. The challenge is ensuring this openness does not compromise our research security.

Although the U.S. has greatly profited from international scientific collaboration and the contributions of foreign-born scientists, other countries—both friend and foe—are also benefiting from U.S. investments.

While our goal is to ensure that all federally funded scientists adhere to U.S. principles of scientific fairness and integrity, regardless of race or citizenship status, it is important to recognize that not all nations share these values.

As this Committee is well aware, the Chinese Communist Party (CCP) is determined to surpass the U.S. as the global leader in science and technology by 2050 by any means necessary, including espionage, theft, or forced acquisition.

The theft of our basic research poses a significant risk to our global competitiveness, handing our cutting-edge innovations to adversaries and undermining both our economy and our ability to lead in discovery.

This is no idle threat and creates a serious strategic challenge. The CCP has been explicit about its efforts to steal our research results to further its technological progress.

A 2023 survey by the Center for Strategic and International Studies found 224 reported instances of Chinese espionage directed at the U.S., and more than 1,200 lawsuits were filed by U.S. companies against Chinese entities for intellectual property theft since 2000.

For the instances of espionage where the actor and intent were known, 49% of incidents directly involved Chinese military or government employees, 46% involved cyber espionage, 29% sought to acquire military technology and 54% targeted commercial technologies.

This Committee has passed multiple bills to protect American research.

Some of this legislation directed the Office of Science and Technology Policy to coordinate efforts and standardize requirements across all federal science agencies to provide a strong framework for research security.

However, the previous Administration failed to execute this framework within the directed timeline—missing deadlines by over a year in some cases—and provided little to no coordination and community engagement.

The government needs clear and uniform guidance for our agencies and researchers. I am confident this second Trump Administration will continue the good work of its previous term and reopen communication channels.

Effective communication between law enforcement agencies and universities is paramount to securing our research enterprise.

Universities need to know when researchers are targeted by nefarious actors, and law enforcement should be aware of the participants and conflicts of interest within our academic research ecosystem.

This collaboration should also extend to our technology transfer systems. Startups are an important part of our S&T enterprise and present a vulnerability that our global competitors are exploiting.

While universities can track licenses derived from on-campus research, they lack transparency about the startup's investors.

For instance, a foreign entity could access sensitive research through early investment in a startup before the technology license is granted, thereby avoiding a review by the federal Committee on Foreign Investment in the United States.

Clearly, this is a complex task that requires thoughtful consideration, but I believe we are up to the challenge.

I look forward to hearing from our witnesses today on how we can assess and monitor the threats to our scientific research enterprise.

Chairman MCCORMICK. Thank you, Mr. Chair. And right now, I'd like to recognize Representative Lofgren for her opening statement.

Ms. LOFGREN. Thank you, Chairman McCormick and Ranking Member Sykes. I really do hope that research security will remain a bipartisan and productive topic for this Committee. We have an impressive legacy of legislation and oversight on research security for years. On both sides of the aisle, we have maintained a deep understanding of and respect for, which the Chairman has just mentioned, the spirit of openness that animates fundamental research. Republicans and Democrats alike have taken threats to research security seriously, while understanding that in order to be the world leader in science and discovery, we must welcome international collaboration while guarding against espionage.

One year ago, we sat in this hearing room and discussed the progress that had been made on research security. Honestly, it's difficult to have that same conversation today without acknowledging how different our scientific enterprise looks. The past 6 weeks have seen a widespread attack on Federal science. Science agencies froze their awards at the order of President Trump and Elon Musk, and recipients of these prestigious grants were worried not only about continuing their work, but honestly, about paying their bills. They now only have certainty for as long as the temporary restraining orders last.

Scientists across the Federal Government were fired in sweeping terminations of probationary employees. And it's worth noting that, you know, probationary employees are people who received a merit-based promotion and were in a probationary status for the promotion, so we have singled out the most meritorious scientists for termination. And the Administration is demanding that more be fired. This will impede agencies' ability to disburse congressionally authorized grant money, among other crucial functions. The rug has really been pulled out from under our Federal scientific enterprise, which had been the envy of the world. Now, it will be naïve to think that this won't affect our ability to attract and retain talent, both American and foreign-born.

This Committee has a lot to be proud of when it comes to commonsense research legislation. *CHIPS and Science* bolstered our research security resources, our agencies' resources. It catalyzed cross-governmental harmonization of research security policies. More needs to be done. Unfortunately, even the progress that has been made will be undercut due to recent decisions.

CHIPS and Science established a research security office within NSF. This office was seriously impacted by the probationary firings and the resignations amidst the hostile environment Elon Musk

and DOGE (Department of Government Efficiency) has created. *CHIPS and Science* also mandated that NSF run the SECURE (Safeguarding the Entire Community of the U.S. Research Ecosystem) Center to support and empower research institutions to mitigate foreign interference. That center lacks a permanent Director, and NSF can't hire one while the hiring freeze is in place. Now, while probationary employees are being hired back this week because of the court decisions, there's no guarantee that the agency will get through the coming firings without again compromising the research security office.

NSF is a pretty efficient agency. Only about 5 percent of its budget is spent on agency operations and awards management. By firing NSF employees and coercing others to resign, this Administration harms our ability to distribute grant money to meritorious cutting-edge research, and it's kneecapping our research security capabilities. We might consider the title of this hearing "The most pressing threat to U.S.-funded research is coming from inside the house."

For years now when we sat for these hearings, Democrats and Republicans celebrated the fact that the United States was the chosen home of world-class talent. We took pride in the fact that nearly 80 percent of foreign-born STEM (science, technology, engineering, and mathematics) Ph.D. recipients chose to remain in the United States. If the destabilization of our research ecosystem continues, we will tarnish our reputation, and we will invite brain drain.

I firmly support the bipartisan work that the Science Committee has done to bolster research security. I hope we can all stand up for that work and insist that existing laws are enforced, and where there are remaining vulnerabilities, I hope we can work together the way we have for years to find commonsense solutions that respect the openness of science first articulated at the Presidential level by Ronald Reagan in 1985. I fear that unless Republicans and Democrats alike stand against the destruction of our scientific enterprise, we will cede our leadership to China in ways that no research security policies can prevent.

With that, Mr. Chairman, I yield back.

[The prepared statement of Ms. Lofgren follows:]

Thank you, Chairman McCormick and Ranking Member Sykes. I really do hope that research security remains a bipartisan and productive topic for this Committee. We have an impressive legacy of legislation and oversight on research security. For years, on both sides of the aisle, we have maintained a deep understanding of, and respect for, the spirit of openness that animates fundamental research. Republicans and Democrats alike have taken threats to research security seriously, while understanding that in order to be the world leader in science and discovery, we must welcome international collaboration.

One year ago, we sat in this hearing room and discussed the progress that had been made across the federal government on research security. It is difficult to have that same conversation without acknowledging how different our scientific enterprise looks today. The past six weeks have seen a widespread attack on federal science. Science agencies froze their awards at the order of President Trump and Elon Musk, and recipients of these prestigious grants were worried not only about continuing their work, but about paying their bills.

They now only have certainty for as long as the temporary restraining order lasts. Scientists across the federal government were fired in sweeping terminations of probationary employees, and the Administration is demanding more workforce cuts, which will seriously impede agencies' ability to disburse Congressionally authorized grant money, among other crucial functions. The rug has been pulled out from

under our federal scientific enterprise, which hasbeen the envy of the world. It would be naïve to think that this will not affect our ability to attract and retain talent, both American- and foreign-born.

This Committee has a lot to be proud of when it comes to common sense research securitylegislation. *CHIPS & Science* bolstered our research agencies' resources and catalyzed cross-governmental harmonization of research security policies. Unfortunately, the progress will backslide due to recent decisions. *CHIPS & Science* established a research security office within NSF, and this office was seriously impacted by the probationary firings and the resignations amidst the hostile environment Elon Musk and DOGE has created. *CHIPS & Science* also mandated that NSF run the SECURE Center to support and empower research institutions to mitigate foreign interference. That Center lacks a permanent director, and NSF cannot hire one while the hiring freeze is in place. While probationary employees are being hired back this week, there is absolutely no guarantee that the agency will get through the forthcoming RIFs without again compromising the research security office. NSF is an incredibly efficient agency—only 5% of its budget is spent on agency operations and awards management.

By firing NSF employees and coercing others to resign, this administration is gutting our ability to distribute grant money to meritorious, cutting-edge research and kneecapping our research security capabilities.

I think that we should reconsider the title of this hearing. The most pressing "threat to U.S. funded research" is coming from inside the house. For years now, when we sat for these hearings, Democrats and Republicans celebrated the fact that the United States was the chosen home of world-class talent. We took pride in the fact that nearly 80% of foreign-born STEM PhD recipients chose to remain in the U.S. If the destabilization of our research ecosystem continues, we are actively tarnishing our reputation and inviting brain drain.

I firmly support the bipartisan work that the Science Committee has done to bolster research security. I hope we can all stand up for that work and insist that existing laws are enforced. Where there are remaining vulnerabilities, I hope we can work together the way we have for years to find common-sense solutions that respect the openness of science first articulated at the presidential level by Ronald Reagan in 1985. I fear that unless Republicans and Democrats alike stand against the destruction of our scientific enterprise, we are ceding our leadership to China in ways that no research security policies can prevent.

I yield back.

Chairman MCCORMICK. Thank you, Ranking Member Lofgren. I appreciate your remarks today.

With that, Mr. John Sargent, who is not new to the halls of Congress, has only recently retired from Congressional Research Service, where he provided Members of Congress and their staffs with research briefings and expert insight on the litany of science and technology issues and policies. In addition to being a long-term expert on our niche issues here in SST, Mr. Sargent earned a degree in systems engineering from University of Virginia.

With that, I yield for your comments.

TESTIMONY OF MR. JOHN F. SARGENT JR., RETIRED, SPECIALIST IN SCIENCE AND TECHNOLOGY POLICY, CONGRESSIONAL RESEARCH SERVICE

Mr. SARGENT. Thank you. Chairman McCormick, Ranking Member Sykes, and distinguished Members of the Subcommittee, thank you for the opportunity to testify today on this issue, which is of vital importance to U.S. national and economic security.

Let's get right down to it. China is not our friend. I wish they were, but they're not. China is an ascendant economic and military power that seeks global tech leadership in emerging, enabling, and critical technologies. China has also become an aspiring hegemonistic power. China first seeks regional domination in East Asia and, from there, world dominance, economically and mili-

tarily. The path to their aspirations depends on technological preeminence.

To realize this future, China is doing three things in particular. They are building a world-class military and drawing up battle plans against the United States, Taiwan, and their regional neighbors. They have adopted a comprehensive whole-of-nations strategy to acquire foreign technology and are making massive investments to develop new technologies indigenously. And they have adopted a civil military fusion strategy to deploy this technology in both their commercial industries and their military industrial base. More than ever, the future of national economic and military power will be built on technological leadership.

Speaking broadly, we have it and they don't. That makes American companies, laboratories, and universities China's primary targets for the acquisition of leading-edge technology. And China uses a wide range of—excuse me—tools to get it, illegal and legal, among them, espionage, theft of U.S. intellectual property, forced technology transfers from U.S. companies, talent recruitment programs, and sending students to study STEM in the United States, some acting as spies.

The Soviets sought military superiority, the Japanese economic superiority. China seeks both. China is not only a potential military adversary like the Soviet Union during the cold war, it's an economic juggernaut, second in GDP (gross domestic product) only to the United States, and larger than Japan, Germany, and the United Kingdom combined. And unlike our relationship with the Soviets, we are actively engaged in trade with China, further complicating the relationship and our ability to limit their access to U.S. technology.

We have a myriad of academic relationships with China as well, many on the cutting edge of research and development, and we are educating hundreds of thousands of the best and brightest minds from China at American universities, many in our top graduate science and engineering programs. Much has been done over the past 8 years to better protect U.S. universities and their research from nefarious actors, and yet here we are again, still trying to tamp down the seemingly ceaseless efforts of China and other adversaries to acquire U.S. scientific knowledge.

Too often, government efforts have met resistance from the academic community, which in large measure would prefer to go about its business with no restrictions. I believe this attitude is detrimental to U.S. national security. It should be a core patriotic duty of every U.S. university to support, protect, and defend the country that provides them with a home, physical security, civil liberties, and protection of their IP, as well as billions of dollars in research and development funding and billions more for the education of their students.

America needs its academic community as a full partner in the protection of our country and its investments in academic research. We need a sea change in the way researchers understand their obligations to the country. They need to bring an attitude toward making this work for America, not just a check-the-block exercise to be met with minimal compliance. We need the academic community to work with the Federal Government to further develop and

strengthen research security protocols, and we need to more fulsomely implement what is already in place.

Similarly, we need to better protect private research. For this, we need U.S. industry to step up as well, especially given the growing magnitude of the private sector's investment in R&D and its work on the bleeding edge of dual-use technologies. In addition, we should consider whether new regimes are needed altogether.

Perhaps most importantly, with respect to research funding, the U.S. Government should start with the rebuttable presumption that science and technology cooperation with China is not in the national interest of the United States. We should be asking first whether any proposed research with China is absolutely indispensable to U.S. national security, the U.S. economy, or U.S. public health and the environment; second, whether China is the only partner in the role with whom we can do such proposed research; and third, whether the proposed research advances U.S. national security, economic, or public health interests more than it does China's. And every decision we make needs to be informed by the answer to whether our men and women in uniform will face these U.S.-funded technologies on the battlefield. In the immortal words of Thomas Jefferson, "Eternal vigilance is the price of liberty."

Thank you, Mr. Chairman.

[The prepared statement of Mr. Sargent follows:]

TESTIMONY OF JOHN F. SARGENT, JR.

RETIRED ANALYST, CONGRESSIONAL RESEARCH SERVICE AND DEPARTMENT OF COMMERCE

BEFORE THE INVESTIGATIONS AND OVERSIGHT SUBCOMMITTEE

UNITED STATES HOUSE COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

Assessing the Threat to U.S. Funded Research

MARCH 5, 2025

Chairman McCormick, Ranking Member Sykes, and distinguished members of the subcommittee. Thank you for the opportunity to testify today on this issue which is vital to the national security and economic interests of our great country.

INTRODUCTION

My name is John Sargent, I recently retired from the Congressional Research Service (CRS), where I spent 15 years working for, and on behalf of, this august body as a Specialist in Science and Technology Policy. In this capacity, my work focused on federal, national, and international R&D and research security, as well as policy analysis related to Department of Defense (DOD) Research Development Test & Evaluation (RDT&E), the National Institute of Standards and Technology (NIST), and the White House Office of Science and Technology Policy. I was also the lead CRS analyst on nanotechnology, manufacturing technology, and the science and engineering (S&E) workforce.

I previously worked in the executive branch for the Commerce Department's Technology Administration, including the Under Secretary for Technology and the Office of Technology Policy, doing analytical work on issues affecting U.S. scientific and technological innovation, leadership, and competitiveness, including research and development (R&D) and S&E workforce. I also served as Director of the Secretariat for the Clinton Administration's Partnership for a New Generation of Vehicles, a multi-agency initiative with the U.S. auto industry, universities, and national laboratories. I earned my Bachelor of Science degree in systems engineering from the University of Virginia's School of Engineering and Applied Sciences.

A few opening thoughts. First, my testimony today is mine and mine alone. I do not speak for my former agencies or colleagues. My remarks, however, are based on my knowledge of science and technology policy and experience as gained through my work at those agencies.

Second, let me be clear: I am an unabashed supporter of the United States of America. You could say that I am America First, last, and always. It's in my family's blood. My father, John Francis Sargent, was a colonel in the U.S. Army Artillery and Air Defense Artillery. During World War II (WWII), he received an Army commission and was part of the forces that occupied Japan after its surrender, he then served in the Virginia Army National Guard

and went on to serve in Germany during the Korean War, and later in the Army Reserve. He also worked as a civilian engineer alongside my maternal grandfather (Rudolph J. Lambert, a draftsman) in the Newport News Shipbuilding and Drydock Company building U.S. warships. Years later, he became a civilian DOD marine engineer designing landing craft and hovercraft for U.S. Army logistics operations. My father-in-law, Robert L. Meares, served with a joint U.S. Army Air Corps-Royal Air Force unit in North Africa doing photo reconnaissance during WWII and survived being shot down. My paternal grandfather, John Samuel Sargent, was an enlisted cavalryman who served in Teddy Roosevelt's Rough Riders, as well as in Europe during WWI, rising to the rank of major. I, too, served in the U.S. Army during the Cold War. I was branched Army Corps of Engineers and later served as a command public affairs officer. My family takes our national security very seriously.

TECHNOLOGICAL LEADERSHIP IS CENTRAL TO NATIONAL ECONOMIC AND MILITARY STRENGTH

Following WWII, the United States emerged as a global leader in science and technology, building on the sophisticated infrastructure put in place to win that war—including our newly minted national laboratories that, among other things, developed and built the first nuclear weapons—and made a substantial investment in research and development and educating a new generation of scientists and engineers, following in large measure a vision set out by presidential science advisor Vannevar Bush at the request of President Roosevelt. For decades, the U.S. technological enterprise stood virtually alone at the top, followed by several European nations, before being joined by Japan in its rise to industrial prominence in the 1970s.

For perspective, in 1960, the United States accounted for approximately 69% of global R&D, most of which was funded by the federal government. Over time, other nations recognized the vital importance of science and technology and boosted their R&D spending. In 2022, the United States accounted for 30.3% of global R&D, China for 26.6%, and Japan for 6.6%.[1] China's growth in R&D expenditures has been the fastest, growing by 2,367% between 2000 and 2022, By comparison, U.S. R&D grew by 244%.

Technological progress is the key to economic growth. As the 1994 Economic Report of the President states correctly that "Time after time, epoch after epoch, and country after country, technological advance has produced higher wages and living standards…This is exactly what we expect to happen again in the 21st century." And my oh my, the 21st century has arrived—on steroids.

A panoply of emerging and enabling technologies—for example, artificial intelligence (AI), quantum computing, nanotechnology, biotechnology, robotics and autonomous systems—driven by massive global investments in R&D (over $3 trillion in 2022) hold the

[1] Author's analysis of Organisation for Economic Co-operation and Development (OECD), Gross Domestic Expenditure on R&D (GERD) data, Main Science and Technology Indicators (MSTI database), https://data-explorer.oecd.org.

potential for revolutionary advances in commercial and military technology, as well as the standard of living, job creation, public health, and quality of life. Leadership in these and other fields is likely to play a decisive role in countries' global economic leadership and military strength in the 21st century.

Not surprisingly, with so much on the line, the world is witness to extraordinary growth in R&D investments, and U.S. adversaries are looking to acquire scientific and technological knowledge by any available means.

LAYING A FOUNDATION FOR UNDERSTANDING U.S. R&D FUNDING AND PERFORMANCE

The United States funds more research and development annually than any other country in the world, an estimated $940.0 billion in 2023. This includes $709.2 billion in private expenditures (75.5% of the total), $172.3 billion in federal government expenditures (18.3%), $29.0 billion in higher education expenditures (3.1%), with the balance provided by non-federal governments and non-profit organizations. These investments—much of which are in dual-use, leading-edge fields (having commercial and military applications)—are the targets for China.

With its funding, the U.S. government supports a broad range of scientific and engineering R&D. Its purposes include addressing national defense, health, safety, the environment, and energy security; advancing knowledge generally; developing the U.S. scientific and engineering workforce; strengthening the capacity of U.S. institutions and firms to conduct cutting-edge scientific research and to develop innovative technologies; and enhancing the global competitiveness of U.S. institutions and firms. Most of the R&D funded by the federal government is performed in support of the unique missions of individual funding agencies.

R&D is characterized in terms of basic research, applied research, and development (federal R&D is divided further into experimental development and non-experimental development). Basic and applied research are sometimes collectively referred to as research. In contrast to most development work, such research is generally non-proprietary and often published openly, though it can lead to important proprietary research and patents.

> **Basic Research.** Basic research is defined as experimental or theoretical work undertaken primarily to acquire new knowledge of the underlying foundations of phenomena and observable facts.
>
> **Applied Research.** Applied research is defined as original investigation undertaken in order to acquire new knowledge. Applied research is, however, directed primarily towards a specific practical aim or objective.
>
> **Experimental Development.** Experimental development is defined as creative and systematic work, drawing on knowledge gained from research and practical

> experience, which is directed at producing new products or processes, or improving existing products or processes. Like research, experimental development will result in gaining additional knowledge.[2]

Development means "the translation of research findings or other knowledge into a plan or design for a new product or process or for a significant improvement to an existing product or process whether intended for sale or use."[3] Non-experimental development is all development work except that which fits the definition of experiment development (above). The Department of Defense (DOD) and the National Aeronautics and Space Administration (NASA) are the primary funders of non-experimental development.

U.S. R&D can be analyzed by who provides the funding (funders) and who performs the work with the funds (performers).

Funders. U.S. investments in R&D are made primarily by private industry and the federal government, and to a lesser degree by U.S. universities, non-profit organizations, and non-federal governments. In 2022, the private sector spent $672.9 billion (76.0%), the federal government spent $159.8 billion (18.0%), and universities spent ($25.5 billion).

Performers. Federal research funding ($97.4 billion in 2022) is performed primarily by universities (45.1%) and federal laboratories (21.8%), and federally-funded R&D centers (FFRDCs, 16.0%). Research performed by universities is generally unclassified and is frequently published in research journals and, therefore, publicly accessible.

Frequently, academic research is conducted solely at a university that receives a grant. The researchers who conduct this work can include professors; other university employees; and undergraduate, graduate, and post-graduate students. Many of these students are U.S. citizens, but a substantial number are from foreign countries, by some estimates as many as 70-80% in certain disciplines (e.g., computer science, petroleum engineering).[4] China is the largest source of foreign science and engineering students.

The Center for Security and Emerging Technology (CSET) estimates that approximately 16% of all science, technology, engineering, and mathematics (STEM) graduate students in the United States are Chinese nationals. According to the CSET report, the number varies by discipline: 33% in mathematics and statistics, 19% in engineering, 14% in physical sciences, 14% in computer science, 10% in agricultural sciences, and 7% in biological

---

[2] Executive Office of the President, Office of Management and Budget, Circular No. A-11, "Preparation, Submission, and Execution of the Budget."
[3] "Definitions of Research and Development: An Annotated Compilation of Official Sources," National Science Foundation, March 2018, https://wayback.archive-it.org/5902/20240829040334/https://www.nsf.gov/statistics/randdef/rd-definitions.pdf.
[4] See, for example, "More International Students Enroll in U.S. Grad STEM Programs: The Numbers and Their Impact," Educational Testing Services, website, https://www.ets.org/grad-school-journey/international-students-stem-programs.html#:~:text=In%20industries%20such%20as%20computer,rates%20as%20high%20as%2081%25.

sciences.[5] A 2018 Defense Innovation Unit Experimental (DUIx) report estimated that the percentage of Chinese nationals in graduate STEM programs is as high as 25%.[6]

Frequently, U.S. academic researchers conduct their research with academics at other universities. Sometimes they establish centers that focus on a specific scientific or engineering field, some of these in conjunction with external partners including other universities, private companies, nonprofit organizations. Research can also be conducted with university and other partners outside the United States, including China. Several U.S. universities have established R&D centers with Chinese universities to conduct joint efforts.

THE PEOPLE'S REPUBLIC OF CHINA IS NOT OUR FRIEND

With respect to the topic of today's hearing: **THE PEOPLE'S REPUBLIC OF CHINA (CHINA) IS NOT OUR FRIEND**, no matter how much we would like them to be. They could be (and one day, I hope they will be), but they have chosen, and continue to choose, not to be. Among the things to keep in mind with respect to how to view the U.S. relationship with China:

- China's *People's Liberation Army* plans for war against U.S. forces and capabilities.
- There is no separation between commercial and defense companies in China. If a U.S. company engages in what it sees as a purely commercial activity with a Chinese entity, any insights and knowledge gained by the Chinese entity will be shared throughout the Chinese commercial and military complex. This policy is China's Military-Civilian Fusion (MCF) strategy. Under MCF, China is systematically reorganizing its science and technology enterprise to ensure new technology and innovations, whether developed indigenously or from external sources, simultaneously advance its economic and military development.
- China is building military capabilities explicitly needed to defeat U.S. forces in battle.
- China engages in trade in illicit goods and use of forced labor, creating low-priced goods that undercut American products in the global marketplace.
- China conducts cyber-attacks on U.S. government, private sector, and critical infrastructure.[7]

---

[5] *Estimating the Number of Chinese STEM Students in the United States,* Center for Security and Emerging Technology, Georgetown University, https://cset.georgetown.edu/publication/estimating-the-number-of-chinese-stem-students-in-the-united-states/

[6] Michael Brown and Pavneet Singh, *China's Technology Transfer Strategy: How Chinese Investments in Emerging Technology Enable a Strategic Competitor to Access the Crown Jewels of U.S. Innovation*, DIUx, January 2018, https://admin.govexec.com/media/diux_chinatechnologytransferstudy_jan_2018_(1).pdf. DIUx is now DIU having dropped the "x" as the organization was no longer considered experimental.

[7] "China remains the most active and persistent cyber threat to U.S. Government, private-sector, and critical infrastructure networks. If Beijing believed that a major conflict with the United States were imminent, it would consider aggressive cyber operations against U.S. critical infrastructure and military assets. Such a strike would be designed to deter U.S. military action by impeding U.S. decisionmaking, inducing societal panic, and interfering

- China has been complicit in the overdose deaths of hundreds of thousands of Americans and the destruction of the lives of many more. The government of China has subsidized and otherwise incentivized PRC chemical companies to export fentanyl and related precursor chemicals used to produce synthetic opiodssold illicitly in the United States.[8] China (along with Mexico and India) is the primary source country for fentanyl and fentanyl-related substances trafficked directly into the United States.[9] Opiate-related fatal overdoses in the United States from 2020-2024 are estimate at over 350,000, far in excess of total U.S. war deaths since WWII (including in Vietnam and Korea).
- China steals intellectual property from U.S. companies, universities, federal agencies, and federal laboratories. China conducts widespread espionage and talent recruitment against U.S. targets, including academic institution, corporations, and even federal laboratories and their staffs. According to a 2022 report by Strider Technologies, a provider of strategic intelligence, between 1987 and 2021, at least 162 scientists who worked at Los Alamos National Laboratory, one of America's leading nuclear weapons laboratories, returned to China to support their R&D enterprise. These scientists and engineers have since conducted research for China on sensitive technologies such as hypersonics, deep earth penetrating vehicles, unmanned aerial vehicles, jet engines and submarine noise reduction. One even held a Q clearance, allowing access to Top Secret restricted data and national security information.[10]

China also does not share American values on human rights, engaging in

> widespread coercive population control methods [including forced abortion, forced sterilization, and involuntary implantation of birth control], forced labor, arbitrary detention in internment camps [including detention of more than one million Uyghurs, ethnic Kazakhs, ethnic Kyrgyz, and members of other Muslim minority groups], torture, physical and sexual abuse, mass surveillance, family separation, and repression of cultural and religious expression.[11]

So why do we choose to not only allow, but to facilitate, and in some cases even fund scientific and technological development in China through U.S. academic institutions, U.S. corporations, and even federal laboratories and federal scientists?

---

with the deployment of U.S. forces." Office of the Director of National Intelligence, 2024 Annual Threat Assessment, https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors/china.

[8] "Imposing Duties to Address the Synthetic Opioid Supply Chain in the People's Republic of China," Executive Order, The White House, February 1, 2025.

[9] U.S. Drug Enforcement Agency, *Fentanyl Flow into the United States*, DEA-DCT-DIR-008-20, January 2020, https://www.dea.gov/sites/default/files/2020-03/DEA_GOV_DIR-008-20%20Fentanyl%20Flow%20in%20the%20United%20States_0.pdf.

[10] The Los Alamos Club, Strider Technologies, Inc., 2022, https://content.striderintel.com/wp-content/uploads/2022/09/Strider-Los-Alamos-Report.pdf.

[11] U.S. Department of State, "The Chinese Communist Party's Human Rights Abuses in Xinjiang," website, https://2017-2021.state.gov/ccpabuses/.

Congress and the President need to make this clear to the American people and to the world. And our policies—including, and maybe especially, our science and technology policies—need to reflect this view. The U.S. government often uses diplomatic and obfuscatory terms like "countries of concern" and "strategic competitor" to describe our relationship with China, but these terms do not convey the seriousness with which we need to take China and our China-focused policies. Perhaps something more akin to Cold War II adversary would be more appropriate. I know that I am not alone in this view. I suspect that some members of this subcommittee share this perspective. As U.S. Director of National Intelligence, now-CIA Director, John Ratcliffe warned in 2021, "[China] poses the greatest threat to America today, and the greatest threat to democracy and freedom world-wide since World War II."[12] Let me put an exclamation point on this—this period would include the U.S. Cold War with Soviets. Take that in: a threat greater than the Soviets posed during the Cold War! The Senate's bipartisan confirmation of Director Ratcliffe suggests that his views are in the mainstream.

Accordingly, I believe we are approaching S&T cooperation with China from the ayong direction. **We should start with the rebuttable presumption that S&T cooperation with China is not in the U.S. national interest. Instead of the default position of looking only for reasons why a proposed R&D project might be harmful to U.S. interest, we should assume that it will be. Instead we should start by asking (1) whether any proposed research with China is absolutely essential and indispensable to U.S. national security, the U.S. economy, or U.S. public health; (2) whether China is the only partner in the world with whom we can do such proposed research with effectively; and (3) whether the proposed research advances U.S. national security, economic, or public health interests more than it does China's.**

This approach is certainly true for federally-funded research but may also be appropriate to apply to private sector research funding and activities as well.

CHINA'S GOALS

Let's be clear—China is an ascendant economic and military power that seeks global leadership in emerging, enabling, and critical technologies. They see the United States as both their economic and military competition, while also a major trading partner and source of technology and innovation. More than ever, the future of national economic and military power will be built on technological leadership. Speaking broadly: We have it, they don't.

China seeks to build an indigenous technological and innovative capacity equal to or exceeding that of the United States and it is investing heavily to build that capacity. China's R&D investments have soared since the turn of the millennium (rising from $32.9 billion

[12] John Ratcliffe, *China Is National Security Threat No.1*, Wall St. J. (Dec. 3, 2020).

(PPP) to $811.9 billion in 2022, an increase of 2,367%).[13] And they have many exceptional scientists and engineers, many of them trained in the United States, and who have experience from working in leading U.S. corporations and startups. But until China can achieve self-sufficiency, they will seek to acquire it from the United States and other advanced countries.

In fact, China has built a complex set of laws, directives, and policies to achieve this self-sufficiency. Collectively, these constitute not just a WHOLE OF GOVERNMENT approach, but rather they are pursuing a WHOLE OF COUNTRY approach to acquiring it.

This approach involves their national and provincial government agencies and institutions, their corporations, their academic institutions, their charitable and cultural foundations, their non-governmental organizations (NGOs), and their people, both in China and their expats living in the United States and elsewhere. China seeks to achieve technological leadership by any means necessary. This is a massive and centrally enforced effort. And China considers it a patriotic duty of their citizens to acquire advanced technology and send it home.

China is very explicit in articulating its national goals, frequently publishing its national plans, including Five-Year Plans, like the Soviet Union did before them. For example:

- The 13th Five Year Plan of the PRC
    - Achieve a leading position in semiconductors, chip materials, robotics, aviation equipment, quantum computing, and satellites
    - Increase R&D spending to 2.5% of GDP
    - Create a $4.4 billion investment fund for startups and new technology
- The 14th Five-Year Plan of the PRC
    - Focus on indigenous innovation, reduce reliance on foreign inputs
    - Upgrade human capital, including improving the use of English to "facilitate the absorption of benefits deriving from technology transfer and innovation."
    - 10-year action plan for basic research
    - Increase R&D by at least 7% a year
    - Focus areas include aerospace, biotech, neuroscience, AI, quantum computing, and semiconductors
- Made in China 2025
    - Align state and private efforts to make China the pre-eminent manufacturing power by 2049
    - Improve integration of information technology

[13] Author's analysis of Organisation for Economic Co-operation and Development (OECD), Gross Domestic Expenditure on R&D (GERD) data, Main Science and Technology Indicators (MSTI database), https://data-explorer.oecd.org. China's growth is the fastest of any country tracked and published by the OECD. During this period, China's R&D has grown from 12.3% the size of the U.S. investment in R&D to 87.9%. In 1991, the first year of OECD published data for China's GERD, China accounted for less than 6% of the level of U.S. R&D.

    - Priority sectors identified as advanced IT, automated machines tools and robotics, aerospace and aeronautical engineering, maritime equipment and high tech shipping, and biopharma and advanced medical products
- China's Mega Projects
    - Manhattan Project-style efforts to meet dual-use needs; projects include fusion, manned spaceflight, chemical production, offshore oil, two-way connection between 5G devices and satellites, and intelligent computing.
- China's State Council established a roadmap to make China the world leader in AI by 2030.

HOW DID WE GET HERE? A BRIEF HISTORY OF U.S.-CHINA SCIENCE AND TECHNOLOGY COOPERATIVE

Let's take a stroll down memory lane to understand how we got here.

In 1972, during the Cold War and in the midst of the Vietnam War, when China was essentially the largest third world country, President Richard Nixon made an unprecedented trip to China to open diplomatic and cultural relations. At that time, China had no industrial or technological base, or military strength to speak of. The relationship was sought as a hedge against the Soviet Union (Russia). According to historian Ken Hughes, the effort sought to "play China against the Soviet Union, the Soviet Union against China, and both against North Vietnam."[14] With trade liberalization providing access to inexpensive goods and labor, it also put downward pressure on U.S. inflation.

In the 1980s, under President Ronald Reagan, the issue arose of how to prevent foreign government interference and exploitation of U.S. S&T, especially with respect to the Soviet Union. In 1985, President Reagan issued National Security Decision Directive (NSDD)-189. This directive states:

> *It is the policy of this Administration that, to the maximum extent possible, the products of fundamental research remain unrestricted. It is also the policy of this Administration that, where the national security requires control, the mechanism for control of information generated during federally-funded fundamental research in science, technology and engineering at colleges, universities and laboratories is classification. Each federal government agency is responsible for: a) determining whether classification is appropriate prior to the award of a research grant, contract, or cooperative agreement and, if so, controlling the research results through standard classification procedures; b) periodically reviewing all research grants, contracts, or cooperative agreements for potential classification. No restrictions may be placed upon the conduct or reporting of federally-funded*

[14] Ken Hughes, "Nixon on China," University of Virginia Miller Center, https://millercenter.org/the-presidency/educational-resources/nixon-china.

> *fundamental research that has not received national security classification, except as provided in applicable U.S. Statutes.*[15]

Economic, cultural, and scientific cooperation presented no significant threat to the United States. Eventually, China's large, cheap labor pool and potential consumer market proved a magnet to U.S. and other western countries. U.S. companies flocked there in the hopes of serving and benefitting from the Chinese market.

Trade accelerated with the accession of China into the World Trade Organization in 2001, after President Bill Clinton gained congressional approval for the *United States–China Relations Act of 2000*. It was expected (hoped!) that China would play by the established international norms of trade, but China chooses instead to play by its own rules.

> *China has a long record of violating, disregarding and evading existing WTO rules. China has also sought to frustrate WTO oversight and accountability mechanisms, such as through its poor record of adhering to its WTO transparency obligations. In addition, and more critically, after more than two decades of WTO membership, China still embraces a state-led, non-market approach to the economy and trade, despite other WTO Members' expectations–and China's own representations – that China would transform its economy and pursue the open, market- oriented approach endorsed by the WTO.*[16]

With few exceptions, American companies found themselves in a Charlie Brown-and-Lucy situation with the Chinese pulling the football out at the last moment, time and time again, foiling our corporations' desires to sell into their market. China seeks to extract trade, technology, and other concessions in exchange for access to their labor, markets, and minerals. China's goal was, and remains today, to establish national champions (Chinese-owned/controlled companies) in key industries that can compete with the best in the world. China seeks to do this through technology substitution, relying temporarily (which in their framework can mean decades) on U.S. and other western countries' technology for leading manufacturing and services, while building a national capability that can eventually replace it (i.e., substituting China's indigenous technology—both home-grown and stolen—for U.S. and other western countries' technology). For examples, China currently relies on U.S. and other countries' semiconductor manufacturing capabilities. It seeks to replace this capability with its own companies and technology to produce high-end chips crucial for its technological advancements, especially in areas like artificial intelligence and military applications. This has become more essential due to the tightening of U.S. export controls limiting China's access to advanced semiconductor.

Shortly after the United States and China established diplomatic relations in 1979, President Jimmy Carter and China's Chairman Deng Xiaoping signed the U.S.-China

---

[15] NSDD-189 states that " 'Fundamental research' means basic and applied research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community, as distinguished from proprietary research and from industrial development, design, production, and product utilization, the results of which ordinarily are restricted for proprietary or national security reasons."

[16] *2023 Report to Congress on China's WTO Compliance,* U.S. Trade Representative, 2023.

Science and Technology Cooperation Agreement (STA), the first major agreement between the two governments. The STA was a part of the U.S. strategy at the time to counter the influence of the Soviet Union by building ties with China. During the 1980s and 1990s, U.S. strategy vis-a-vis China shifted toward enhancing S&T ties as part of a broader U.S. effort to integrate China into the global system and influence its development trajectory and behavior.

President Barack Obama expanded S&T ties with China to address global challenges in areas such as health, energy, and climate change. Many U.S. universities have engaged in extensive research and development activities across a wide range of scientific and engineering fields, including critical emerging technologies such as AI, nanotechnology, biotechnology hypersonic weapons, fourth generation nuclear weapons technology, and semiconductor technology.[17]

Under President Donald Trump, the United States' posture toward China increasingly emphasized protecting and advancing U.S. interests in the context of China as a strategic competitor. STA proponents and critics both say that the STA does not reflect this U.S. policy shift or U.S. concerns about PRC S&T practices and industrial policies. Some say the most recent STA did not address China's growing technological capabilities and restrictive and potentially risky operating environment for cross-border research.[18]

The Biden Administration renewed this agreement last year with minor changes. There is still no database of activities under this authority that would allow for congressional oversight, public and legal scrutiny, and accountability.

LEGAL AND ILLEGAL WAYS CHINA USES TO ACQUIRE U.S. TECHNOLOGY

China engages in both legal and illegal efforts to acquire U.S. and other foreign technology. Much of the public anger and outrage is focused on China's **illegal** acquisition of U.S. and western intellectual property, and rightfully so. For example, in 2019 the FBI reported that the United States loses between $225 billion and $600 billion annually due to Chinese IP theft (including counterfeit goods, pirated software, and theft of trade secrets), or about 1%-5% of U.S. GDP.[19] A survey of chief financial officers found that one in five corporations report China having stolen IP within the previous year.[20] China also requires U.S. companies to transfer technology to Chinese corporate or governmental entities (i.e., forced technology transfer). This can occur, for example, when China requires U.S. companies operating in China to form joint ventures with local companies, or when China

[17] "*CCP on the Quad: How American Taxpayers and Universities Fund the CCP's Advanced Military and Technological Research*," Majority Staff Report, The Select Committee on the CCP, U.S. House of Representatives, September 2024.
[18] "*In Focus: U.S.-China Science and Technology Cooperation Agreement*," Congressional Research Service, Emily Blevins, updated December 5, 2024.
[19] *China: The Risk to Corporate America,* Federal Bureau of Investigation, 2019.
[20] Eric Rosenbaum, *1 in 5 Corporations Say China Has Stolen Their IP Within the Last Year: CNBC CFO Survey*, CNBC, 2019.

requires U.S. companies to share technology with local firms to get approvals from state regulators.

Nevertheless, of equal or great concern is the myriad of **legal** ways in which China acquires U.S. technology. These include:[21]

- Sending Chinese students to study STEM in the United States and other western countries (The Center for Security and Emerging Technology estimates that approximately 16% of all STEM graduate students in the United States are Chinese nationals. According to the CSET report, the number varies by discipline: 33% in mathematics and statistics, 19% in engineering, 14% in physical sciences, 14% in computer science, 10% in agricultural sciences, and 7% in biological sciences).[22] A 2018 Defense Innovation Unit Experimental (DUIx) report estimated that the percentage of Chinese nationals in graduate STEM programs is as high as 25%.[23]
- Sponsorship of, and acquisition of intellectual property rights in, U.S. academic R&D.
- Access to information (i.e., information that's available to the public without special permission, including published research results, scientific publications, news media, public data, and information from social media).
- Foreign direct investment by Chinese firms in U.S. firms ($28.0 billion in 2023, down from a high of $38.8 billion in 2019.[24]), including acquisition of U.S. companies, giving them access to companies' IP.
- Investment by Chinese companies in U.S. venture-backed deals.
- Private equity investments.
- Investments through special purpose vehicles (designed to obscure the source of capital).
- U.S.-based associations sponsored by the Chinese government to recruit talent.
- Acquisition of technical and business expertise from U.S. firms.

---

[21] These mechanisms have been discussed by a number of analysts, but the author would like to recognize the DIUx for identifying many of them in its report, *China's Technology Transfer Strategy: How Chinese Investments in Emerging Technology Enable a Strategic Competitor to Access the Crown Jewels of U.S. Innovation.*

[22] *Estimating the Number of Chinese STEM Students in the United States,* Center for Security and Emerging Technology, Georgetown University, https://cset.georgetown.edu/publication/estimating-the-number-of-chinese-stem-students-in-the-united-states/

[23] Michael Brown and Pavneet Singh, *China's Technology Transfer Strategy: How Chinese Investments in Emerging Technology Enable a Strategic Competitor to Access the Crown Jewels of U.S. Innovation*, DIUx, January 2018, https://admin.govexec.com/media/diux_chinatechnologytransferstudy_jan_2018_(1).pdf. DIUx is now DIU having dropped the "x" as the organization was no longer considered experimental.

[24] Statista.com, https://www.statista.com/statistics/188935/foreign-direct-investment-from-china-in-the-united-states/.

And of course, China invests in its own indigenous R&D activities. Investments in its domestic R&D totaled a reported $811.9 billion in 2022, as measured in U.S. dollars using PPP, up 15.8% over its 2021 investment level.[25]

U.S. UNIVERSITIES AND CHINA

U.S. research universities are a prime target for China due to the billions of dollars they perform annually on leading-edge R&D, including billions performed on behalf of U.S. defense agencies. China uses a complex and broad set of tools to acquire U.S. academic research and knowledge through illicit, gray area, and illegal mechanisms.

Many of these approaches came to light with the Trump Administration's "China Initiative," a Department of Justice (DOJ) effort to counter nation-state threats to the United States. According to DOJ, the initiative sought to:

- Identify priority trade secret theft cases, ensure that investigations are adequately resourced, and work to bring them to fruition in a timely manner and according to the facts and applicable law;
- Develop an enforcement strategy concerning non-traditional collectors (e.g., researchers in labs, universities and the defense industrial base) that are being coopted into transferring technology contrary to U.S. interests;
- Educate colleges and universities about potential threats to academic freedom and open discourse from influence efforts on campus;
- Apply the Foreign Agents Registration Act to unregistered agents seeking to advance China's political agenda, bringing enforcement actions when appropriate;
- Equip the nation's U.S. Attorneys with intelligence and materials they can use to raise awareness of these threats within their Districts and support their outreach efforts;
- Implement the Foreign Investment Risk Review Modernization Act (FIRRMA) for DOJ (including by working with Treasury to develop regulations under the statute and prepare for increased workflow);
- Identify opportunities to better address supply chain threats, especially those impacting the telecommunications sector, prior to the transition to 5G networks;
- Identify Foreign Corrupt Practices Act (FCPA) cases involving Chinese companies that compete with American businesses;
- Increase efforts to improve Chinese responses to requests under the Mutual Legal Assistance Agreement (MLAA) with the United States; and
- Evaluate whether additional legislative and administrative authorities are required to protect our national assets from foreign economic aggression.[26]

According to then-FBI Director Wray in July 2020, "Through talent recruitment programs like the Thousand Talents Program … China pays scientists at American universities to

[25] Author's analysis of Organisation for Economic Co-operation and Development (OECD), Gross Domestic Expenditure on R&D (GERD), Main Science and Technology Indicators (MSTI database), https://data-explorer.oecd.org.

[26] "Information About the Department of Justice's China Initiative and a Compilation of China-Related Prosecutions Since 2018," Federal Bureau of Investigation, November 19, 2021, https://www.justice.gov/archives/nsd/information-about-department-justice-s-china-initiative-and-compilation-china-related.

secretly bring our knowledge and innovation back to China—including valuable, federally funded research. To put it bluntly, this means American taxpayers are effectively footing the bill for China's own technological development. China then leverages its ill-gotten gains to undercut U.S. research institutions and companies, blunting our nation's advancement and costing American jobs. And we are seeing more and more of these cases."[27]

Examples of successful prosecutions under the DOJ's China Initiative include:

- In May 2020, former Emory University professor Xiao-Jiang Li pled guilty to filing a false tax return for failing to report the income he'd received through China's Thousand Talents Program. The FBI stated that it discovered that while Li was researching Huntington's disease at Emory, he was also pocketing half a million unreported dollars from China.
- In May 2021, Song Guo A Zheng, was sentenced to 37 months in prison for making false statements to federal authorities as part of an immunology research fraud scheme. Zheng pleaded guilty and admitted he lied on applications to use approximately $4.1 million in grants from the National Institute of Health (NIH) to develop China's expertise in the areas of rheumatology and immunology. As part of his sentence, Zheng was also ordered to pay more than $3.4 million in restitution to NIH, and approximately $413,000 to The Ohio State University.
- In December 2021, Charles Lieber, chair of Harvard University's Department of Chemistry and Chemical Biology, was found guilty by a jury of two counts of making false statements to federal authorities, two counts of making and subscribing a false income tax return, and two counts of failing to file reports of foreign bank and financial accounts (FBAR) with the Internal Revenue Service (IRS). He was sentenced to time served (two days) in prison; two years of supervised release with six months of home confinement; a fine of $50,000; and $33,600 in restitution to the IRS.
- In January 2022, Simon Saw-Teong Ang, a University of Arkansas scientist conducting research for NASA pleaded guilty to making a false statement to the FBI about the existence of patents for his inventions in China. The FBI asserted that Ang committed fraud by concealing his participation in Chinese talent recruitment programs while accepting millions of dollars in American federal grant funding.

Additional examples of FBI China Initiative efforts can be found at: https://www.justice.gov/archives/nsd/information-about-department-justice-s-china-initiative-and-compilation-china-related.

In February 2022, after a review under the Biden Administration, the DOJ announced it was shutting down the China Initiative. "DOJ will no longer use the framework of the China Initiative to organize or to describe our efforts to counter threats by the PRC government,"

[27] "The Threat Posed by the Chinese Government, and the China Communist Party to the Economic and National Security of the United States," Christopher Wray, Director, Federal Bureau of Investigation, July 7, 2020.

said Assistant Attorney General for National Security Matthew Olsen. "We are ending the China Initiative." [28]

The Administration and the FBI faced criticism from Asian-American organizations, civil liberty organizations, and others that believed the initiative fostered discrimination against Asian-Americans, broadly, and Chinese-Americans in particular. A number of these groups have asked President Trump not to revive the initiative.[29] Olsen further explained the agency's reasoning saying, "By grouping cases under the China Initiative rubric, we helped give rise to a harmful perception that the department applies a lower standard to investigate and prosecute criminal conduct related to that country or that we in some way view people with racial, ethnic or familial ties to China differently."[30]

U.S. ACADEMIC BIAS TOWARDS FREE-SHARING, OPEN PUBLISHING OF KNOWLEDGE

A key ideal of U.S. universities is the commitment to advancing the state of knowledge. Central to this belief is one of communal sharing of knowledge. In fact, for U.S. academics, historically the path to career success has been enshrined as, "publish or perish," that is the sole path to tenure and esteem is to put your research into the public record.

While this allows scientists and industrialists to build on the advances in knowledge of all, in a world with fierce economic competitors and military adversaries, it also provides them with the tools to compete and win—in the market and on the battlefield–especially in today's technology-driven, technology-enabled times. When the United States was the world's largest investor in R&D (say in 1960 when the United States accounted for 69% of global R&D) sharing knowledge was less risky because most countries were not in a position to assimilate and use that knowledge. This is no longer the case and hasn't been for quite some time.

In the 1970s and 1980s, Japan's acquisition of U.S. S&T knowledge and application of it to its industrial sectors played an important role in aiding in its rapid economic ascension.

Today, China does the same, except China is a military adversary, as well as an economic competitor. This creates a new environment with different challenges. And, as discussed previously, China is engaged in a Whole of Nation effort to acquire and use U.S. and other foreign technology.

---

[28] DOJ Shuts Down China-Focused Anti-Espionage Program," *Politico*, February 23, 2022.
[29] See "Letter to Congress: Do Not Revive the China Initiative," from a variety of organizations to congressional leaders, September 9, 2024, https://stopaapihate.org/2024/09/09/letter-to-congress-do-not-revive-the-china-initiative/.
[30] DOJ Shuts Down China-Focused Anti-Espionage Program," *Politico*, February 23, 2022.

U.S. UNIVERSITIES ARE EXTRAORDINARY ASSETS, BUT…

America needs its academic community not only to be the discoverers, inventors, and innovators, but to also recognize that they are on the front line of defense against adversaries acquiring knowledge that can be a threat to U.S. security.

American universities have been and remain a pillar of American strength. U.S. academia is the best in the world. It's why hundreds of thousands from around the world flood to U.S. schools for post-secondary education. Their work in the classroom—preparing our workforce— and in the laboratory—creating valuable new knowledge—are essential to almost all aspects of American life and security.

The contributions made by American universities are countless. And we should all be grateful for their work, past and present. Nevertheless, America needs this community to pivot once again, in recognition of the nefarious actors who would apply the knowledge they create against the United States and its allies.

Change is hard, and I believe for America's academic community—largely free from external controls and market forces—I think it is particularly challenging. However, U.S. academia has shown itself adept at changing to meet pressing national needs and objectives—from building agricultural schools and departments in the 19th century under the Land Grant acts, to graduating a new generation of scientists and engineers after WWII (many under the GI Bill), to creating nuclear programs with the advent of nuclear power, to expanding aeronautical and astronautical programs with the Space Race.

Much has been done over the past eight years—by presidents, congresses, and the academic community—to better protect U.S. universities from nefarious actors, and keeping the products of their research from falling into their hands. And yet, here we are again, still trying to tamp down the seemingly ceaseless efforts by China and other adversaries to acquire U.S. scientific knowledge. Too often, government efforts have met resistance from the academic community, which, in large measure, would prefer to go about its business with no restrictions. I believe this attitude is detrimental to U.S. national security. It should be a core patriotic duty of every U.S. university to support, protect, and defend the country that provides them with a home, physical security, civil liberties, and protection of their IP, as well as billions of dollars for research and development and billions more toward educating students. This includes financial aid for students (e.g., scholarships, work-study, and loans) and funding for R&D and R&D facilities and equipment through grants and contracts

Many in the academic community revere Vannevar Bush for his support for free exchange of ideas in academia. However, this support was not asserted in a vacuum, but very much in the context of his WWII experience, well-grounded in concerns about future adversaries.

> *Our defense against aggression demands new knowledge so that we can develop new and improved weapons…*

> *The bitter and dangerous battle against the U-boat was a battle of scientific techniques—and our margin of success was dangerously small.*
>
> —Vannevar Bush, *Science: The Endless Frontier, 1945*

Too frequently, many in the academic community fail to recognize Vannevar Bush's foundational belief that U.S. government investment in academic research is justified and essential to protect the country and to drive its economic growth objectives (as well as to make advancements in human health and to address other societal needs). Bush was acutely aware of the role of science and technology in protecting the United States given his role as director of the Office of Scientific Research and Development during WWII.

MOVING FORWARD

America needs its academic community as a full partner in the protection of our country and its investments in academic research and development. We need a sea change in the way researchers understand their obligations to the country. We need the academic sector come to the table with Feds to strengthen and further develop research security protocols. And we need to more fulsomely implement what's in place. In addition, there is room for thought about whether new regimes are needed altogether.

And to emphasize one more time, we should start with the rebuttable presumption that S&T cooperation with China is not in the U.S. national interest. We should be asking (1) whether any proposed research with China is absolutely essential and indispensable to U.S. national security, the U.S. economy, or U.S. public health; (2) whether China is the only partner in the world with whom we can do such proposed research with effectively; and (3) whether the proposed research advances U.S. national security, economic, or public health interests more than it does China's.

Biographical Sketch of John Sargent

John Sargent recently retired following 30 years of federal service in science and technology policy, including 15 years with the Congressional Research Service and 15 years with the Department of Commerce.

At CRS, John conducted quantitative and qualitative analyses on a wide range of science and technology policy topics; authored/co-authored more than four dozen reports; conducted seminars; prepared confidential memoranda; and consulted with Members and staff on issues and legislation. John's work focused on federal, national, and international research and development (R&D); research security; manufacturing; semiconductors; nanotechnology; science and engineering (S&E) workforce; and technology transfer. John served as lead CRS analyst on Department of Defense research, development, testing, and evaluation (RDT&E) funding; the National Institute of Standards and Technology; and the White House Office of Science and Technology Policy.

At the Commerce Department's Technology Administration, John conducted analysis on issues affecting U.S. scientific and technological innovation, leadership, and competitiveness, including R&D, nanotechnology, and the S&E workforce for the Under Secretary for Technology and Assistant Secretary for Technology Policy. John co-authored *Technology in the National Interest*, a seminal White House report on the nation's technology policy, and a legislatively mandated report from the Secretary of Commerce to Congress on the education and training of the information technology workforce. John also served as Director of the Secretariat for Partnership for a New Generation of Vehicles, a Clinton Administration flagship R&D program between seven federal agencies and the U.S. automobile industry (including GM, Ford, and DaimlerChrysler), universities, and national laboratories.

John earned a bachelor of science in systems engineering from the University of Virginia's School of Engineering and Applied Sciences. He also served as an officer in the U.S. Army Reserve, graduating from the Engineer Officer Basic Course and the Defense Information School Public Affairs Officer Course.

Chairman MCCORMICK. And thank you for your testimony.

Mr. Jeffrey Stoff is the Founder and President at the Center for Research Security, a not-for-profit organization dedicated to the protection of research and innovation from harmful foreign influence and interference. Mr. Stoff previously spent over 18 years in the U.S. Government as a China analyst and is recognized as an expert in technology protection issues.

Please give your opening statement.

TESTIMONY OF MR. JEFFERY STOFF, PRESIDENT, CENTER FOR RESEARCH SECURITY & INTEGRITY

Mr. STOFF. Subcommittee Chairman McCormick, Ranking Member Sykes, distinguished Committee Members, thank you for the opportunity to testify today on this critically important topic. Over the last 15 years, I focused on China's research ecosystem and its state-driven technology transfer apparatus. While in government, I worked closely with most Federal agencies that fund scientific research, as well as law enforcement and intelligence components. That support exposed me to deficiencies and vulnerabilities in both academia and government, which I describe in detail in my written testimony.

For several years, starting in 2019, a few colleagues and I exerted considerable effort compiling analyses, briefing government leadership, and proposing programmatic changes to address knowledge gaps and structural impediments to safeguarding innovation security. Unfortunately, most of those efforts fell on deaf ears. My frustrations with continued inaction by agencies charged with protecting Federal research investments and our national and economic security drove me to leave Federal service in 2021 after 18 years.

It is past time we have candid and perhaps uncomfortable conversations on how China's largely unfettered access to our research ecosystem undermines our national and economic security and that China exploits and corrupts our research, often through the willing participation of U.S. institutions. And because universities are primarily run like businesses in that bringing in revenue is their primary objective, the financial incentives of universities often run counter to U.S. national and economic security interests.

Academia continues to demonstrate a systemic disregard for national security considerations and an indifference to or lack of awareness of ethical risks when collaborating with China. These issues persist in part because of a lack of regulatory oversight regarding fundamental research, which worked fine through the cold war but now fails to address geostrategic realities. Even where there are rules in place in terms of Federal grant contract conditions, the evidence suggests continued and widespread noncompliance by academia.

Currently, only NASA (National Aeronautics and Space Administration) and the Department of Defense (DOD) have certain research funding restrictions concerning collaborations with China. No other activities or sources of funding are proscribed. Researchers and institutions are free to partner, collaborate, establish cooperative programs, et cetera, with any PRC entity of their choosing. Academia has claimed that they now understand the risks much

better and have a good handle on security concerns. Empirical studies I've produced and data I compiled in my written testimony prove otherwise, such as low estimates of over 27,000 articles published in just the past 5 years involving collaborations between U.S. institutions and PLA (People's Liberation Army) entities, PRC defense weapons design and production facilities, state-owned defense enterprises and key defense research universities. Additionally, neither academia nor the U.S. Government has taken any observable policy measures to mitigate PRC practices that undermine research integrity issues.

In addition to academia's disclosure failures to the Department of Education on foreign sources of funding as required by law, nondisclosures on Federal grants of current and pending support, often coming from China, persist. Many of those grants could have gone to other universities that didn't have this PRC support. For the universities acting in good faith, losing out on these grants can result in smaller budgets and fewer resources to hire Ph.D. students, attract top talent, et cetera, which in turn makes them less competitive on future grant proposals. This also translates to fewer opportunities for our children in the United States and an erosion of STEM talent pipelines.

Compounding these issues are structural problems in the government to identify and mitigate threats from China and monitor and force academia's noncompliance. These include each agency has its own research security and due diligence process. A lack of interagency data sharing results in duplicative risk assessments when done at all and inconsistent standards for assessing risks across Federal agencies. The U.S. Government also has few resources or processes in place to monitor for national security risks post-award of a grant or contract. And further handicapping these efforts is a dearth of subject matter expertise within both the intelligence and law enforcement communities.

A key recommendation in my testimony is to consolidate government research security functions into a centralized organization that closes persistent knowledge, regulatory, and policy gaps; creates efficiencies and cost savings; builds subject matter expertise through training analysts and investigators; bolsters compliance monitoring and enforcement; serves as a resource to assist universities in conducting risk assessments; disrupts China's unfettered access to federally funded research; and imposes real costs to China when it violates values of integrity and reciprocity.

Thank you, and I look forward to your questions.

[The prepared statement of Mr. Stoff follows:]

Written Testimony of Jeffrey Stoff
Founder of the Center for Research Security & Integrity

Before a Hearing of the U.S. House of Representatives Committee on Science, Space, and Technology – Investigations and Oversight Subcommittee
"Assessing the Threat to U.S. Funded Research"

Subcommittee Chairman McCormick, Ranking Member Sykes, distinguished subcommittee members:

Thank you for the opportunity to testify today on this critically important topic. Now that I am no longer working in the government, I can speak candidly about the persistent challenges in identifying and disrupting China's exploitation of US federally funded research. Over the last 15 years, I have focused on China's research ecosystem and its state-driven technology transfer apparatus. The collection and analysis programs I ran while serving in various capacities in the government provided insights into China's technology and knowhow acquisition strategies and exploitation of US R&D in public and private sectors.

While in government, I worked closely with most federal agencies that fund scientific research – including the National Science Foundation, National Institutes of Health, NASA, the Departments of Defense, Energy, and Commerce – as well as law enforcement and intelligence components. That support has exposed me to a range of deficiencies and vulnerabilities in academia and the US government, including inaction by federal agencies charged with protecting our national and economic security, which was a key source of my frustration and the reason I left federal service in 2021 after 18 years. Two years ago, I started a non-profit organization called the Center for Research Security & Integrity in part to address the impediments to knowledge building and threat mitigation.

In this testimony, I highlight numerous ways in which the PRC exploits federally funded research, academia's systemic non-compliance with federal grant rules and appropriations laws, and the US government's structural impediments and lack of sufficient policy responses to address research security vulnerabilities. I offer illustrative case studies based on my observations while working in the government as well as subsequent research I have conducted post federal service. It is important that we have honest and sometimes uncomfortable conversations about what is taking place so that we can address the issues effectively. Some of the information I provide is rarely discussed publicly, perhaps because it can expose the shortcomings of academia and the government.

The final section lists specific recommendations, some of which involve revising or expanding existing regulations and policies. *However, a key recommendation will require paradigmatic shifts in how the US government approaches research security, particularly in response to China's threats to our research enterprise*.

Table of Contents

Introduction: PRC Methods to Exploit Our Research Ecosystem 3
Research Collaborations of Concern 6
National Security Risks 7
Ethical Risks: US Research Support to PRC Surveillance and Public Security Apparatus 12
US University Non-Compliance on Federal Research Grants and Contracts 15
Section 117 Non-Compliance 15
Current and Pending Support Disclosure Failures 16
Example 1: Stanford University Settlement Agreement 17
Example 2: University of Maryland Settlement Agreement 18
'Wolf Amendment' Non-Compliance 19
Case Example: University of Delaware 20
Case Example: University of Maryland's Apparent Violations of the 'Wolf Amendment' 21
Other PRC Threats, Influence Over Federally Funded Research 24
Example A: Corrupting NOAA Research and Operations 25
Example B: Former UCLA Professor 27
Example C: Influence Over NSF Grant Award Processes 28
Example D: Hijacking NSF CAREER Awards 28
Example E: Exploiting SBIR Programs 29
US-Based Support Networks for PRC Technology Transfer Activities 29
China's Role in Undermining Research Integrity and US Inaction 30
Case Example: 'Comfort Letters' 31
Reciprocity 32
US Government Challenges and Impediments to Building Robust Research Security Programs and Policies 32
Policy Gaps 33
Intelligence Community and Law Enforcement Shortcomings 34
Lack of Expertise 34
Grant and Contract Compliance Monitoring and Enforcement Shortcomings 35
Deficiencies with Vetting, Due Diligence, and Compliance Investigations 35

Recommendations for Policymakers 36

1. Pass the DETERRENT Act 37

2. Require recipients of NSF CAREER awards to sign a continuing service agreement with the US government. 37

3. Create new legislation that places restrictions on all federal sources of fundamental research funding if recipient institutions collaborate with select PRC entities. 38

4. Federal funding agencies should more aggressively use grant suspensions and debarments. 38

5. Revise appropriations law or require federal agencies to insert new requirements on all federal research grants and contracts that state that all recipients of federal funding will be subject to the False Claims Act. 38

6. Authorize NSF to Create a National Research Security, Integrity, and Compliance Center and enable a corresponding interagency investigative task force. 39

NRSICC Lines of Effort 39

Introduction: PRC Methods to Exploit Our Research Ecosystem

The threats and malign influence posed by the PRC on our research and innovation ecosystem and their implications are under-recognized problems. There is insufficient knowledge on how the PRC has and continues to benefit economically and militarily through its mostly unfettered access to federally funded research as well the corrupting and corrosive effects of its influence activities. This testimony seeks to provide insights into the enormity of the problem that the US government has inadequately addressed.

A *sampling* of some of the threats and exploitation by the PRC include:

- Converting or diverting US government-funded research into intellectual property that is commercialized in the PRC that may be in violation of research grants or university terms and conditions or, at minimum, solely benefit the PRC economically.
- Repurposing US research, including in seemingly innocuous fields like climate change research, to PRC defense programs and weapons system development that can undermine or eliminate US military superiority.
- Directing or redirecting US critical technology research funded by US industry and federal and state governments for China's benefit by selectees of PRC talent recruitment programs who are under contract with and tasked by the PRC government.
- Improperly influencing or manipulating federal research grant evaluations and award decisions.

- Applying US research to enable or enhance the PRC's domestic surveillance apparatus and human rights abuses.
- Influencing or co-opting US academics' hiring or sponsoring of PRC national PhD students, postdoctoral fellows, and visiting researchers that circumvent merit-based processes and build talent and training pipelines that predominantly benefit China.
- Establishing or co-opting networks of organizations in the US that enable knowledge transfer, talent recruitment operations, and PRC state-backed venture capital investments intended to offshore critical technology to China. A subset of this effort includes targeting recipients of US Small Business Innovation Research programs.
- Influencing or tasking researchers at federal research facilities and laboratories to facilitate formal cooperative agreements with PRC institutions, sometimes violating internal conflicts of interest and ethics policies.
- Engaging in behaviors that violate norms of transparency, reciprocity, and other aspects of integrity that equate to deception, fraudulent publications, or other forms of dishonest research and publication practices.

In some respects, academia has been victimized by China's exploitation and malign influence through vulnerabilities inherent in the open nature of how science is conducted. It is unrealistic to expect individual institutions (and even large technology firms that engage in research) to be able to sufficiently protect themselves against the predations of the PRC party-state and the massive resources and infrastructures it has put in place to target the U.S. (and allied nations).

Some of China's exploitation comes from a natural evolution of how scientific and engineering research is conducted. Academic institutions have traditionally viewed science as a borderless endeavor; they have argued that pursuing the frontiers of knowledge and betterment of humanity supersedes transitory geopolitical concerns. Governments in liberal democracies have also shared this view: science and technology diplomacy and academic freedom (and freedom to pursue any partnerships and flows of talent) have greatly benefited technological and economic development and such benefits have in the past outweighed any risks. That principle held true for at least half of a century after the Second World War. But this era of progress was partly because the U.S. and allied nations were so much stronger technologically and economically that authoritarian regimes played a very small role – or even participation in – the scientific enterprise.

Today, the US and most of our key allies, have failed to adapt or address a contradictory reality: one of the most significant contributors to and participants in the global scientific enterprise is also our greatest adversary and strategic rival; one of the world's largest and technologically advanced economies is also one of the most oppressive authoritarian regimes in history, and has a primary objective of dominating and displacing the US technologically and militarily to reshape the world order and to preserve Chinese Communist Party (CCP) interests.

But this is not the whole story. *An uncomfortable truth is that much of China's efforts to exploit, influence, and corrupt our research ecosystem require the willing participation of US academia*. Academic institutions, especially at the individual faculty level, tend to mirror image key aspects of our system with that of the PRC and fail to recognize the incompatible elements – that the PRC's authoritarian system controls and drives most research activities and decisions. While many individual Chinese researchers who work with US academics may share the same values and passion as Americans do in their research endeavors, they are under a system that has specific objectives that run counter to our core values and interests, and those individual PRC researchers have no control over where and what happens to their research. This holds particularly true regarding any data sharing or intellectual property (IP) agreements – it is impossible for any foreign entity to control where data, materials, research, and potential or actual IP goes once it enters China's borders. In fact, the PRC has codified into law its total control and access to all data, information, and materials under the guise of national security, cybersecurity, and anti-espionage statutes.

It is worth noting that based on my observations from supporting federal investigations and conducting due diligence research, most researchers are cooperating with PRC entities (such as defense and surveillance research programs) willingly and voluntarily. The PRC and the CCP has created enormous incentives and opportunities for personal gain by helping the PRC; most of China's efforts to transfer US critical technology do not appear to be coercive in nature.

Federal funding agencies, law enforcement, and intelligence community (IC) elements have done a good job of raising awareness among universities on national and economic security risks associated with some PRC research partnerships. US research institutions conceptually understand that there are real risks and concerns that need to be addressed and mitigated. But this often conflicts with academia's primary goal of attracting sustaining revenue sources (and human capital) from anywhere. Security and compliance, like the private sector, is a cost burden, not an operational priority. *Consequently, the financial incentives and operations of universities often run counter to US national and economic security interests.*

Previous administrations and academia have argued that any protections or restrictions regarding collaborations with China and other authoritarian regimes should be limited to specified critical technology areas as a so-called "small yard - high fence" approach. Everything outside these designated areas should remain free and open for collaboration. The problem with such an approach is that the PRC has become increasingly adept at diverting many types of STEM research to defense applications, including in fields that may not be included on sensitive or critical technology lists. This is particularly apparent in certain health and climate change fields, such as hearing aid R&D being used to enhance PRC submarine warfare development or climate change research, like remote sensing and marine ecology, enabling next-generation military/surveillance satellites and PLA naval operations.

National Security Decision Directive 189 (NSDD-189), a policy that has been in place since the 1980s, states that the US government will not restrict sharing or collaboration in

fundamental research domains except in rare circumstances where national security concerns require classifying the information. This also means that fundamental research, which is defined as both basic and applied research that is published openly, is not subject to export controls or other regulatory restrictions or oversight. There are currently only two exceptions where Congress has put in place restrictions concerning fundamental research collaborations with adversarial nations including China.

The first restriction (commonly referred to as the "Wolf Amendment") prohibits recipients of NASA research funding from collaborating with most PRC entities on a strictly bilateral basis. I provide further details and case examples of non-compliance with this rule later in this testimony. The second is a restriction stipulated in Sec. 238 of the recently passed FY25 National Defense Authorization Act (NDAA) that makes institutions ineligible for Department of Defense funding for fundamental research if the US institution collaborates with a set of PRC entities listed in other provisions of the NDAA (Sec. 1286 of the FY19 NDAA).

All other sources of federal funding currently have no restrictions; researchers and institutions are free to partner, collaborate, establish cooperative programs, etc., with any PRC entity of their choosing. Like other countries except Canada,[1] the government can merely provide guidance on national security risks (if they do at all), but universities can ignore this provided they are compliant with federal grant requirements. From a legalistic perspective, there are few incentives for universities to create robust security policies that restrict their fundamental research activities or partnerships if there are no specific rules that proscribe such activity. However, compliance failures on federal research grants or contracts by US institutions also appear to be widespread and often relate to some form of PRC partnership. The next sections explore these issues in detail.

Research Collaborations of Concern

A key challenge is that responsibility for conducting due diligence and risk assessments currently falls on individual research institutions and faculty overseeing research projects. This is problematic as individuals and institutions do not have nearly enough information or subject matter knowledge on China and its research ecosystem, the current landscape of geostrategic risks and challenges, etc. to make such determinations. It is unreasonable to expect a faculty member who is charged with carrying out scientific research to be able to handle such a task. A lack of information sharing, scholarship, and expertise on the PRC within the US government, including the national security community, is another impediment. If the US government lacks the capabilities and resources, how can an individual faculty member or university handle this on their own?

[1] The Canadian government issued a policy that will deny federal funding for research grants if that research involves collaborations with specific PRC (and Russian and Iranian) institutions in specified critical technology fields. This policy on "Sensitive Technology Research and Affiliations of Concern" was established in the Fall of 2024. Canadian institutions are still free to collaborate with PRC, Russian, and Iranian entities, but no federal funding would be provided to them.

National Security Risks

What about partnerships and collaborations with PRC entities that are *widely known to represent national security risks*? The data collated here is a current snapshot of very high-risk US-China scientific and engineering research collaboration. The data is limited to a *sampling* of PRC military entities, weapons R&D facilities, and select defense-affiliated civilian universities. This data **demonstrates US academia's systemic unwillingness to examine national security risks or ethical concerns regarding their research collaborations with China**. Furthermore, the huge scale of these high-risk collaborations suggests dependencies and vulnerabilities that China then exploits.

Tables 1 through 4 break down the number of articles published in 2019 through January 2025, coauthored by researchers from a US-based institution and researchers affiliated with specific PRC entities part of the People's Liberation Army (PLA), the Central Military Commission (the CCP organ overseeing the PLA), and select PRC state-owned defense conglomerates. This data reflects collaborations that represent the highest risks to national security. The data was compiled using the *Dimensions* tool by Digital Science that aggregates bibliographic metadata of journal articles, conference proceedings, preprints, patents, and other data related to published research. **Disturbingly, a total of 9,398 unique articles were identified involving coauthors based at US institutions and researchers affiliated with select PRC military institutions in just the past five years. This understates the actual amount of US collaborations with PRC military entities** due to the scoping limitations of this testimony and persistent knowledge gaps on other PRC research institutions that conduct defense research.

Table 1 lists a *sampling* of PRC military medical units that have coauthored the most articles with US partners. This is not an exhaustive list of all US-China collaborations with PRC military medical entities. (Note: totals in these tables may exceed the total number of unique articles as there can be more than one of these PRC entities listed in the same article)

Table 1: US Institution Collaboration with Select PRC Military Medical Entities

PLA / Central Military Commission Medical Entity	Number of Articles with US-based Coauthors
Chinese PLA General Hospital	1,526
Army Medical University	1,012
Air Force Medical University	888
Academy of Military Medical Sciences	289

Some medical research conducted by these entities may be considered low-risk or beneficial (such as cancer research). However, the PRC party-state does not share the same values and ethical principles as liberal democracies concerning research involving human subjects, and thus even research that is innocuous in nature may be diverted to military or unethical purposes. Examples of where this matters include: China's horrific and well-documented record of human organ harvesting, incarceration of political dissidents in psychiatric

hospitals, involuntary collection and use of genetic information of its citizenry for mass surveillance purposes, and medical research with military applications such as fighter pilot and solder performance enhancements, human-computer interfaces for weapons programs, etc.

Consequently, collaborations with PLA medical entities can pose national security, ethical, and reputational risks for US and allied nation collaborators and funders. It is also worth noting that both US government and private sector entities are acknowledged as funders (presumably funding the US researchers). **Government funders include (but are not limited to): the Agricultural Research Service, Air Force Office of Scientific Research, Centers for Disease Control and Prevention, Congressionally Directed Medical Research Programs, Defense Threat Reduction Agency, Department of Veterans Affairs, NIH, and NSF.** A sampling of private companies and foundations credited as funders include Abbott, Amgen, Biogen, Boston Scientific, Bristol-Myers Squibb, Eli Lilly, Intel, Intuitive Surgical, Johnson & Johnson, Medtronic, Pfizer, the American Cancer Society, American Red Cross, Bill & Melinda Gates Foundation, Mayo Clinic, Memorial Sloan Kettering Cancer Center, and the Welch Foundation.

Table 2 lists the number of collaborations with the China Academy of Engineering Physics (CAEP) and a few of its subdivisions that are often named separately in English-language publications, i.e., CAEP is not listed as the parent organization. CAEP is China's nuclear weapons design and production complex, which also includes development of other advanced weapons, components, and delivery systems.

Table 2: US Institution Collaboration with PRC Nuclear and Advanced Weapons Complex

China Academy of Engineering Physics (CAEP)	Number of Articles with US-based Coauthors
CAEP (including subdivisions naming CAEP as a parent entity)	308
CAEP Subdivisions NOT Stating an Association with CAEP	
Beijing Computational Science Research Center	425
High Pressure Science & Technology Advanced Research	398
Institute of Applied Physics and Computational Mathematics	160
Science and Technology on Surface Physics and Chemistry Laboratory	16

Notes: The Beijing Computational Science Research Center works with (and is possibly subordinate to) the Institute of Applied Physics and Computational Mathematics, also known as CAEP's 9th Institute, responsible for numerical / computer simulations for nuclear and other weapons designs. The Science and Technology on Surface Physics and Chemistry Laboratory is subordinate to CAEP's Institute of Nuclear Physics and Chemistry located at CAEP's primary facility in Mianyang.

Table 3 offers a *sampling* (not an exhaustive list) of PLA technical schools whose researchers have collaborated with US entities.

Table 3: US Institution Collaboration with Select PLA Scientific Institutes

PLA / Central Military Commission Entity	Number of Articles with US-based Coauthors
National University of Defense Technology (NUDT)	601
PLA Army Engineering University	69
PLA Information Engineering University	66
PLA Air Force Engineering University	36
PLA Academy of Military Science	32
China Aerodynamics Research and Development Center	29
Naval University of Engineering	19

Notes: The National University of Defense Technology is the PLA's premier scientific and engineering research institution and is sanctioned by the US Treasury Department. The China Aerodynamics Research and Development Center is the PLA's premier hypersonics R&D facility, although no English-language source indicates the center is affiliated with the military.

Table 4 offers a *sampling* of US collaboration with some of China's largest state-owned defense conglomerates and a few of their subsidiaries. Subdivisions of these state-owned enterprises have research institutes, some of which house state key laboratories and function like academic institutions. Although some of these firms do engage in civilian research and technology areas, they are run by the PRC central government with a primary mandate to support the PLA through the development of weapons systems and components, including China's missile programs. Even if US researchers claim that their research is strictly for commercial purposes (with no dual-use potential), collaboration with these PRC defense firms can improve these conglomerates' commercial operations and bolster their financial position. This provides the firms more resources to advance their primary purpose of developing defense or weapons R&D and production programs, strengthening the PLA and emboldening China to become more hostile toward its neighbors, supply other autocratic regimes (especially Russia), and challenge US military superiority and deterrence in strategic areas such as the Taiwan Strait and the South China Sea.

Table 4: US Institution Collaboration with Select PRC State-Owned Defense Conglomerates

PRC Defense Enterprise	Number of Articles with US-based Coauthors
China Academy of Space Technology	166
China Electronics Technology Group Corporation	133
China Aerospace Science and Technology Corporation	103
China State Shipbuilding (includes China Shipbuilding Industry Corporation)	77
Aviation Industry Corporation of China	56
China North Industries Group Corporation (NORINCO)	52

China Academy of Launch Vehicle Technology	29
Aero Engine Corporation of China	24
China South Industries Group	21
China Aerospace Science and Industry Corporation	18

Notes: The China Academy of Space Technology and the China Academy of Launch Vehicle Technology are subsidiaries of the China Aerospace Science and Technology Corporation. The China Academy of Launch Vehicle Technology is China's largest R&D and production facility for space launch vehicles, liquid-fueled surface-to-surface missiles, and solid-fueled surface-to-surface and submarine-launched ballistic missiles.[2] CALT also produces the Dongfeng series of intercontinental ballistic missiles (ICBM)s, the latest versions equipped with multiple independent nuclear warheads able to strike Europe and the Western United States.[3]

In addition to PRC military institutes and state-owned defense enterprises, there are groups of civilian universities that have a primary mission to support military research and defense industries. These institutions are known as the "Seven Sons of National Defense" and the "Seven Sons of Ordnance Industry" (two of these universities belong to both groups). The former group originated as military academies but is now directly overseen by the State Administration for Science & Technology Industry for National Defense (SASTIND), a PRC government organ responsible for implementing military-civil fusion policies. All these universities work on classified defense programs, house departments and laboratories (including "national defense key laboratories") that work closely with PLA organs, and partner with state-owned defense conglomerates. The latter group was previously under the supervision of the then Ministry of Ordnance Industry and continues to conduct weapons R&D as part of its core mission.

Some STEM research conducted at these universities is in civilian sectors or may lack obvious defense applications; however, it is prudent to assume that these schools will pursue potential military applications as a matter of policy and thus represent high national security risks. **There were 17,630 unique articles published between 2019 and January 2025 involving a coauthor from one of these 'Seven Sons' universities and a coauthor affiliated with a US institution.**[4] Table 5 lists the number of articles involving coauthors from these schools and US institutions.

Table 5: US Institution Collaboration with PRC 'Seven Sons' Universities

Seven Sons of National Defense, Seven Sons of Ordnance Industry Universities	Number of Articles with US-based Coauthors
Beihang University	4,909
Harbin Institute of Technology	3,836

[2] "China Academy of Launch Vehicle Technology (CALT)," Nuclear Threat Initiative, February 1, 1994, www.nti.org/learn/facilities/59/.
[3] "China Academy of Launch Vehicle Technology – CALT 1st Academy," https://www.globalsecurity.org/wmd/world/china/calt.htm.
[4] Articles involving hyper-coauthorship (that list 100 or more coauthors) were excluded. Many articles also list more than one 'seven sons' schools, so the totals in this table exceed the total of unique articles.

Beijing Institute of Technology	3,335
Northwestern Polytechnical University	2,396
Nanjing University of Science and Technology	1,770
Nanjing University of Aeronautics and Astronautics	1,507
Harbin Engineering University	723
North University of China	356
Chongqing University of Technology	208
Changchun University of Science and Technology	127
Shenyang Ligong University	53

The data in the above tables are admittedly a crude measure.[5] The statistics provide no indication of the nature or frequency of the US collaborations, which are often informal and sometimes unbeknownst to federal sponsors or even the US employers. Investigating these collaborations for approximately 27,000 articles is a daunting task. *Additionally, due to persistent knowledge gaps, this data significantly under-represents the amount of collaborations posing national security risks*: there are many defense and state key laboratories, Chinese Academy of Sciences institutes, subdivisions of civilian universities, and research institutes subordinate to state-owned enterprises that also conduct defense research but have not been compiled in this dataset.

Nevertheless, this cursory survey of US research collaboration with high-risk entities demonstrates academia's widespread disregard for national security concerns, despite the increased scrutiny the US government has placed on these PRC institutions and its outreach efforts to academia.

Academia has argued that per NSDD-189, most "fundamental research" should remain unrestricted and any additional rules federal agencies place on international collaborations in fundamental research domains would stifle innovation and cause more harm than it seeks to address. Fundamental research includes both basic and applied research that is published. *But who decides if/when research that is more applied in nature crosses into areas that pose sufficient risk to warrant some form of restricted dissemination?* This appears to be arbitrary and largely at the discretion of the individual researcher.

The incentive is to avoid addressing these issues by publishing openly and, thus by default, designating the research as fundamental. I lack the technical expertise to make such determinations, but some published research funded by DoD involves very specific applications and raises questions on whether it makes sense to publish that research openly. A recent report by the House Select Committee on China provided examples of research disciplines involving US collaborations with China that appear highly applied and intended for the US military. The report noted:

[5] This data excludes Chinese-language publications appearing in domestic PRC sources and probably understate the actual number of coauthored publications.

"These studies found that the relevant collaborations covered a wide range of sensitive technologies crucial to national security, including cryptography, eavesdropping, hyperspectral imaging, lithium-ion batteries, aerodynamic angles of attack, electronic warfare, cyber-attack detection, high-density explosives, high entropy alloys, radar target detection, quadcopters, artificial intelligence, quantum technology, multi-target tracking, missile impact penetration, and surveillance technologies."[6]

Should all of those articles have been published openly? Should any PRC institution have been allowed to participate in or support these research areas?

PRC's exploitation of US federally funded research also goes far beyond just DoD-funded research projects. Entities such as the Department of Energy also fund research in nuclear, weapons and energy development that are dual-use technologies. The same is true for NSF, which funds research on radar, underwater acoustics, artificial intelligence, and many other areas with obvious dual-use applications. Even NIH funding is at risk. My research on US and German collaborations with China revealed multiple instances where scientists developing advanced hearing aids using signal and speech processing techniques funded by NIH had dual appointments and/or work with a PLA Navy underwater warfare research division of Northwestern Polytechnical University and a defense key laboratory on radar signal processing at Xidian University (which is co-supervised by China's largest defense electronics and radar systems developer). Thus, research funded by NIH, NSF, and other agencies may affect future US warfighting capabilities.

Ethical Risks: US Research Support to PRC Surveillance and Public Security Apparatus

Academia's indifference to research security concerns is not limited to national and economic security issues. This section demonstrates **academia's persistent indifference to or lack of awareness of ethical risks to research collaborations with China.** I am referring to collaborations that involve research disciplines that are intended for or can be diverted to mass surveillance technologies or involve partnerships with PRC research institutions that support the CCP's public security apparatus that engage in human rights abuses. I exclude from this discussion ethical concerns regarding how the research is conducted, particularly as it relates to human subjects.

A study I published with the Hoover Institution examined the Chinese Academy of Sciences Institute of Automation (CASIA), one of China's premier AI, computer vision, and neuroscience research institutes. CASIA enjoys global collaboration with academia and industry, including major technology firms like Google, Dell, and Intel. Yet CASIA is extensively involved in developing and commercializing mass surveillance technologies, including facial, iris, and gait recognition, and video surveillance. CASIA owns commercial spinoffs that have developed these surveillance technologies for PRC public security organs,

[6] "CCP on the Quad: How American Taxpayers and Universities Fund the CCP's Advanced Military and Technological Research," House Select Committee on the CCP, Sep. 2024.

including for use in the Xinjiang region used to oppress and detain Muslim minority populations.[7]

I compiled data on US collaborations involving US-based coauthors alongside CASIA researchers published from 2019 to January 2025 and found 676 unique articles. US collaborations with CASIA appear to continue unabated, suggesting academia is not concerned with the ethical or reputational risks of working with CASIA.

CASIA is just one organization in China that extensively supports the party-state's surveillance apparatus and corresponding human rights abuses. To survey a larger sample of ethically troubling research collaborations, I compiled bibliographic metadata on scientific publications whose abstracts contained one or more of the following keywords that have obvious surveillance applications and involve both US and China-based coauthors:

- biometrics
- facial identification
- facial recognition
- iris recognition
- gait recognition
- pose estimation
- person tracking
- person re-identification
- video surveillance
- scene understanding
- emotion recognition
- expression recognition

Researchers from the US who collaborate with China on topics related to these areas may be focused on innocuous, commercial applications. However, when PRC institutions partner in these research disciplines, we must assume the party-state will seek mass surveillance applications that can benefit the PRC's public security apparatus or, in some cases, may be subordinate to or a supplier of PRC public security organs. Data obtained using the Dimensions aggregator by *Digital Science* included **1,472 articles published 2019 through January 2025 involving US research partnerships with PRC-based entities in these obvious surveillance disciplines.**

Table 6 lists the top 20 US universities ranked by the number of articles published in surveillance-related research with PRC institutions.

[7] See Stoff, Tiffert, "Eyes Wide Open: Ethical Risks to Research Collaboration with China," *Hoover Institution*, December 2021, https://www.hoover.org/sites/default/files/research/docs/stoff-tiffert_eyeswideopen_web_revised.pdf.

Table 6: Top 20 US Universities Involved in Surveillance Research Collaboration with the PRC

US University	Number of Articles Published 2019 - Jan. 2025
Harvard University	67
Carnegie Mellon University	65
University of California, Los Angeles	59
Johns Hopkins University	54
University of Washington	52
State University of New York at Buffalo	43
Georgia Institute of Technology	41
University of California, Berkeley	41
University of Southern California	40
Stanford University	38
University of Michigan–Ann Arbor	36
University of Illinois Urbana-Champaign	33
Michigan State University	32
University of Pennsylvania	32
University of California, San Diego	32
Temple University	31
Massachusetts Institute of Technology	30
University of Missouri	30
Texas A&M University	29
Cornell University	29

This data represents a small sampling of articles that are easy to recognize as raising ethical concerns. More scholarship is needed to build comprehensive keyword ontologies associated with research disciplines with potential surveillance use and identify PRC research institutions involved. Nevertheless, **this data suggests that US universities have made little to no effort to restrict collaborations with the PRC on ethical grounds and calls into question academia's sincerity in upholding the core values of scientific research they espouse.** Collaborations in these ethically troubling areas can enable or enhance China's continued surveillance and oppression of its citizens *and* the export of related technologies to authoritarian regimes around the world. *If US-based researchers who collaborate with the PRC in this type of research receive federal funding, then this needs to be addressed by relevant agencies and policymakers as part of any effort to bolster research security and compliance efforts.*

I am not aware of any US government efforts or capabilities to monitor formal and informal research partnerships and exchanges between US institutions and PRC entities in areas that have clear surveillance applications. Further complicating any potential compliance or policy objectives are the persistent knowledge gaps on PRC institutions extensively involved in surveillance research and support public security organs. *The US government, particularly the national security community, has failed to systematically identify such entities and share that information with the public.* The Bureau of Industry and Security (BIS) does periodically add some PRC firms to the Entity List for export control purposes if those firms contract with or supply PRC public security organs; but few, if any, efforts have been made to look at PRC academic institutions in this space. Nevertheless, export controls rarely apply to fundamental research, so BIS efforts in this area have little to no impact on research security policies.

US University Non-Compliance on Federal Research Grants and Contracts

In simplistic terms, US universities are run like businesses in that their primary objective is to bring in revenue. This is partly due to the fact the federal and state governments do not provide enough funding to universities for them to operate; academia must rely on a diverse set of revenue sources. This creates inherent vulnerabilities that foreign entities - especially the PRC - can exploit for their benefit and create incentives that are often not aligned with US national interests.

This section discusses universities' known or suspected non-compliance with federal research grant and contract rules and, in some cases, inadequate monitoring and enforcement by federal funding agencies and the national security community in identifying and mitigating the threats to taxpayer-funded research investments. Types of non-compliance are broadly divided into the following areas, though there can be substantial overlap, i.e., university non-compliance with multiple federal regulations simultaneously. These areas relate to:

a) Section 117 of the Higher Education Act
b) Current and pending support disclosures on federal research grant submission documents
c) An appropriations law regarding NASA funding (also known as the "Wolf Amendment")

Section 117 Non-Compliance

An uncomfortable truth is that US universities have a history of accepting gifts, contracts, and grants from nearly any entity in the world without discrimination (or due diligence) on those funders. Additionally, one observed way PRC entities funnel money into US academic institutions is through US academics that hold concurrent positions at PRC universities (such as visiting professors), often recruited through one of the hundreds of PRC state-sponsored talent programs. The US academics holding these PRC positions then serve as a proxy for PRC institutions, brokering gifts, contracts, grants, and cooperative agreements with the US institutions where they are employed. Consequently, *it can be financially advantageous to a US university if they have faculty that holds concurrent appointments in China, regardless of*

whether such appointments or commitments comply with federal grant and contracting rules.

Section 117 of the Higher Education Act requires institutions that receive any form of federal funding to disclose foreign sources of funding to the US Department of Education on a biannual basis.[8] However, both Congressional and Department of Education investigations found widespread non-compliance with this law. An early 2019 report by the US Senate Permanent Subcommittee on Investigations found that foreign funding in America's higher education system is "effectively a black hole," with up to 70% of colleges and universities failing to disclose mandatory foreign funding.[9] A report issued in late 2020 by the Department of Education revealed more than $6.5 billion in previously undisclosed foreign funding (from China, Russia, Iran, and Qatar) and found that "historically, fewer than 300 of the approximately 6,000 U.S. institutions self-report foreign money each year."[10] Federal agency enforcement of this law has been minimal, partly due to a lack of willingness by the Biden administration to devote resources to investigate and prosecute non-compliance. Passage of the DETERRENT Act by Congress would go a long way in bolstering reporting requirements by universities and punitive measures for non-compliance.

Given the widespread non-compliance of Section 117 reporting requirements, a few investigators at Offices of Inspectors General (OIG) have initiated proactive investigations with the Department of Justice to determine whether university non-disclosure of foreign gifts or grants (especially from China) was also not disclosed on federal research grants. Civil litigation against universities has demonstrated this to be the case. However, as discussed in the **Recommendations** section of my testimony, to date, such efforts by federal investigators have been quite limited in scope due to a lack of subject matter expertise, experience, and resources.

Current and Pending Support Disclosure Failures

Federal agencies that award research grants require applicants to disclose current and pending support, the details of which have been clarified and expanded on through National Security Presidential Memorandum-33. Nevertheless, based on my experience working with federal investigators, *non-disclosures by university grant applicants persist and appear to be widespread.* The types of current and pending support that are required to be disclosed on grant submissions include any material support to a research endeavor, such as personnel or equipment and sources of funding (contracts, grants, etc.) that relate to the proposed research (or during the conduct of the research if already underway).

Some universities have not disclosed contracts, gifts, or research grants they received from China as current and pending support on federal grant applications and periodic report

---

[8] See 20 U.S. Code § 1011f.
[9] "China's Impact on the U.S. Education System," U.S. Senate Permanent Subcommittee on Investigations (Feb. 2019), www.hsgac.senate.gov/wp-content/uploads/imo/media/doc/PSI%20Report%20China's%20Impact%20on%20the%20US%20Education%20System.pdf.
[10] "Institutional Compliance with Section 117 of the Higher Education Act of 1965," U.S. Department of Education, Office of the General Counsel (Oct. 2020), www.ed.gov/sites/ed/files/policy/highered/leg/institutional-compliance-section-117.pdf.

submissions. The disclosure failures can be attributed to individual principal investigators (PIs), university administrators, or both. Technically speaking, universities are the recipients of federal grant monies, which are then disbursed to the PIs; thus the universities are the responsible parties that certify the accuracy of information on grant submission documents. This also means that it is more effective for federal agencies to hold universities accountable through civil remedies (e.g., using the False Claims Act) than attempting to indict or convict an individual faculty member (PI) on criminal charges for providing false statements to the federal government.

That said, it is important to understand that PRC state-sponsored talent programs often contractually obligate and instruct selectees (in this case, US PIs and co-PIs on federal grants) not to disclose details on their level of commitment, sources of funding, projects, or positions in China to their US employers. This means that the US universities that employ them may not always be aware of these commitments, which leads to federal grant non-compliance as the PIs are also failing to disclose their current and pending support on grant applications. Universities have recognized this as a problem, and many have revised or bolstered internal activity reporting and related policies and procedures so that administrators can be more fully aware of the engagements and commitments of their faculty.

However, this is not the whole story. *Federal investigations discovered that some universities have been complicit in grant disclosure failures*. Their motivations are probably monetary in nature. What is usually missing from public discourse related to these issues are the secondary effects and implications that undermine integrity, trust, fairness, and equity in our institutions of higher education. To be fair, it is important to note that US academia is not monolithic; I am not suggesting every institution operates in the same unscrupulous ways described in this testimony. Some universities, for example, have robust research security and compliance programs that seek to serve as responsible stewards of taxpayer money and cooperate closely with federal agencies to ensure continued compliance.

Two recent civil cases described below are illustrative of these disclosure failures and their implications.

Example 1: Stanford University Settlement Agreement

The United States alleged that on 16 grant proposals submitted to the Army, Navy, NASA, and NSF, Stanford University "knowingly failed to disclose current and pending foreign funding that 11 Stanford PIs and co-PIs had received or expected to receive in direct support of their research." The United States further alleged that Stanford "knowingly failed to disclose to the Army, Air Force, and NSF that a Stanford professor received research funding in connection with his employment at China's Fudan University and from a foreign government's national science foundation" (refers to the PRC).[11] The US alleges that these disclosure failures violate the False Claims Act. The case was resolved through a settlement

[11] https://www.justice.gov/opa/pr/stanford-university-agrees-pay-19-million-resolve-allegations-it-failed-disclose-foreign

agreement between Stanford University and the US government, whereby Stanford agreed to pay $1.9 million to resolve allegations of False Claims Act violations.

Interagency efforts to pursue civil remedies should be lauded as they are a much more effective and fairer approach to mitigating these concerns compared to pursuing criminal prosecutions. However, a cursory survey of the grants listed in the settlement agreement that were (allegedly) fraudulent totaled over $14 million. The False Claims Act allows for damages of *up to triple* the amount of the federal grants, plus a flat penalty per occurrence of each false claim submission. Consequently, this small settlement agreement is unlikely to create any real deterrent for universities to change their behavior. The penalties to date largely equate to a modest cost of doing business; universities can maintain the status quo of receiving an unknown amount of funding and support from PRC entities and, in essence, "double dip" by taking federal grant dollars to do the same research.

Example 2: University of Maryland Settlement Agreement

In July of 2024, the University of Maryland (UMD) entered into a settlement agreement with the Department of Justice that also involved funding from Huawei. The United States alleged that UMD "knowingly failed to disclose current and pending foreign funding that three UMD researchers had sought and received, in five research grant proposals submitted to the NSF and the Army. Specifically, the United States alleged that UMD failed to disclose to NSF gift funding from Huawei Technologies Co., Ltd. to a PI[12] for research in 'high energy density FeF3 conversion cathode materials and Li metal anodes.'" The government also alleged that UMD failed to disclose to the NSF and Army funding provided to two other PIs from Taobao (China) Software Co, a subsidiary of Alibaba titled, "Large-Scale Behavior Learning for Dense Crowds" and "Cyber-Manufacturing of Customized Apparel."[13] Note that the first project clearly has mass surveillance applications. UMD agreed to pay $500,000 in the settlement agreement. Like the Stanford case, this represents a small percentage of penalties UMD may have been liable for if a court ruling was pursued.

This UMD case appears to be consistent with other investigations I supported when I was in the government, where PRC entities basically contract with US academia to conduct research on specific projects led by specific PIs. Yet the recipient US institutions have claimed those sources of funding are unrestricted gifts, meaning that they are donations to US institutions that are free to use the funds in any way they see fit. Academia has argued that they do not have to report that as current or pending support on federal grant applications because those "gifts" do not relate specifically to the research grants.

In at least some observed cases, these gifts are really contracts or grants in disguise; they "recommend" specific US faculty work on specific research projects at the PRC's behest. PRC institutions are directing US institutions to perform research by specific personnel. Naturally, US universities will abide by the wishes of the PRC "donors" to avoid jeopardizing those revenue streams.

---

[12] PI refers to principal investigator, the researcher(s) that leads a project funded by federal research grants.
[13] https://www.justice.gov/usao-md/pr/university-maryland-college-park-agrees-pay-500000-resolve-allegations-it-failed

A secondary and largely unaddressed compliance concern may also be taking place. Unrestricted gifts may not be counted when universities calculate the administrative / overhead costs associated with the federal grants they receive. Universities charge a portion of each federal grant to cover the administrative costs of executing the research. The implication is that if a university receives a federal grant to perform research that is materially similar to the research sponsored by a "gift," then in essence, the university may be overcharging the US government on its administrative costs. That could be considered fraud.

There are other secondary and corrosive effects that are not being adequately discussed in public discourse. When universities or their faculty fail to disclose these outside sources of funding (regardless of whether they are characterized as gifts, grants, or contracts), *that affects federal grant award decisions.* This violates the principles of integrity and transparency that universities espouse as core values. Furthermore, federal research grants are highly competitive; only a fraction of the total grant submissions are usually awarded. There are finite taxpayer dollars; if universities are, in essence, double-dipping by taking both PRC and US government funding, this means that other universities – especially those with fewer resources like smaller institutions and Historically Black Colleges and Universities – are denied those federal research dollars that could have otherwise been awarded.

This creates a vicious cycle of inequity in the system: schools that are being honest but denied federal funding means they have smaller budgets and fewer resources to hire PhD students, attract top talent, etc., which then makes them less competitive on future grant proposals. This also translates to fewer opportunities domestically.

How pervasive is this problem, and how much PRC funding and resources are being funneled to (and hidden by) US universities? A lack of awareness of this problem means it is impossible to determine the level of influence the PRC is exerting over the conduct of US research that may be overwhelmingly (or unilaterally) benefitting China to our detriment.

'Wolf Amendment' Non-Compliance

An appropriations law in effect since 2012 places "Chinese Funding Restrictions" on any NASA-funded grants or contracts. The law, which is also referred to as the "Wolf Amendment," statutorily prohibits recipients of funding from NASA from engaging in bilateral participation, collaboration, or coordination with the People's Republic of China, Chinese-owned companies, or Chinese universities.[14] Multilateral research exchanges involving China and any additional country are exempt from this restriction. NASA has provided clear guidance to universities on this rule since it has gone into effect. Nevertheless, an unknown number of US institutions receiving NASA funding have violated this law through bilateral research collaborations with PRC institutions. A cursory analysis of research collaborations a colleague and I have conducted suggests that university non-compliance is widespread.

Universities receiving NASA research funding must comply with this appropriations law and by receiving such funding, they certify compliance. Universities that violate the Chinese

[14] Pub. L. No. 112-10, § 1340 and Pub. L. No. 112-55, § 539.

funding restrictions are submitting false claims to the federal government (i.e., fraud). An example of a Wolf Amendment violation is a recent case against the University of Delaware.

Case Example: University of Delaware

On December 10, 2024, the Department of Justice (DoJ) announced that the University of Delaware (UD) would pay a $715,580 fine for failing to disclose a prominent UD researcher's "affiliation with and support from" the PRC government.[15] The UD professor, Dr. Xiao-Hai Yan, was a PI on a NASA grant identified in the settlement agreement who concurrently served as a prominent research faculty member at China's Xiamen University. Professor Yan received substantial research funding from the PRC government and was a "Thousand Talents Program" selectee.

A colleague and research partner LJ Eads[16] and I conducted our own research on Professor Yan and his activities in China. Dr. Yan is a recognized expert in oceanography and remote sensing research; his contributions to deep ocean remote sensing and climate change research have been recognized by both the US and PRC governments. Yan served as Director of UD's Center for Remote Sensing and Associate Director for the NASA-Delaware Space Grant Consortium beginning in 2005[17] (to which NASA obligated nearly $10 million in federal grants and a cooperative agreement with UD).

Dr. Yan was a PI or co-PI on numerous NASA grants (as well as Navy and National Oceanic and Atmospheric Administration grants). At the same time, Yan held appointments in China, including positions at Xiamen University from at least 2007 to the present, thus engaging in ongoing and substantial, bilateral collaborations with PRC entities (a violation of the Wolf Amendment since 2012). Professor Yan also played a key role in establishing several cooperative agreements and joint training programs between UD and Xiamen University, including a joint remote sensing research center and the construction of a satellite ground station at Xiamen University. Some of these formal agreements were established *after* the Wolf Amendment became law. It is not known whether UD received any funding from the PRC, such as a gift or contract, as part of these cooperative agreements. Nevertheless, at least some of these activities almost certainly involved NASA funding sources. In other words, both Professor Yan and UD leadership demonstrated willful negligence or disregard for US appropriations law.

Even more troubling is the fact that Professor Yan led a research and engineering project at Xiamen University to develop a new synthetic aperture radar (SAR) satellite in partnership with several PRC defense state-owned enterprises. One of these PRC firms, Spacety China, is now sanctioned by the Treasury Department for its role in providing satellite imagery to Russia for targeting Ukrainian infrastructure.[18] Yan's activities in China and his involvement in US federally funded research that threatens US national security are extensive and far exceed the scope of this testimony.

---

[15] https://www.justice.gov/usao-de/media/1380506/dl?inline
[16] LJ Eads is a former US Air Force intelligence analyst and now the founder of Data Abyss, an S&T intelligence platform of Parallax Advanced Research.
[17] https://www.udel.edu/content/dam/udelImages/ceoe/documents/smsp/Yan_Xiao-Hai_2page.pdf
[18] https://sanctionssearch.ofac.treas.gov/Details.aspx?id=40477

The Chinese funding restrictions stipulated in the Wolf Amendment are intended to prevent the transfer of technology and knowhow from NASA-funded programs to China. The DoJ and NASA were right to investigate UD for its false certifications that NASA funding was not being used in scientific collaborations with China and hold UD accountable for its non-compliance. However, the UD settlement appears quite low compared to UD's potential liability and may not serve as much of a deterrent for non-compliance. The settlement agreement is the only publicly known action the government has taken to date. If it has not already, the US government should also address these questions:

- There were several grants whose period of performance were after the 2012 appropriations law went into effect, during which time Yan held concurrent positions in the PRC. Why did prosecutors limit litigation to just one of the many NASA grants Yan served as PI or Co-PI on? Why did it take 12 years for investigators to identify non-compliance?
- Were the UD centers that receive NASA funding also a potential Wolf Amendment violation? What about the other UD-Xiamen University cooperative agreements?
- Professor Yan's concurrent positions in China have taken place for over 20 years, some of which have involved partnerships with very high-risk defense entities. Why didn't the US national security community attempt to mitigate or disrupt this activity?

In my opinion, most of the government's shortcomings relate to a lack of investigative resources or priorities (or both) to aggressively pursue compliance monitoring and enforcement and a lack of subject matter knowledge on how to identify these threats and mitigate them when they do not involve illicit activities.

Case Example: University of Maryland's Apparent Violations of the 'Wolf Amendment'

Through our own research, LJ Eads and I have identified another case where violations of Chinese funding restrictions of the Wolf Amendment are probably taking place. A summary of findings of apparent non-compliance follows, which were based exclusively on self-funded efforts: we have received no materials, information, funding, or any other form of support from any federal agency that relates to this matter. This information is derived from surveying the University of Maryland's (UMD) receipt of NASA research grants and cooperative agreements, as well as concurrent bilateral research collaborations with PRC researchers and institutions that likely violate Wolf Amendment restrictions.

Due to its proximity to NASA's Goddard Space Flight Center in Greenbelt, Maryland, UMD has cultivated a close research partnership with NASA. Since 2010, a memorandum of understanding has underpinned joint activities in space-based science, engineering, biosciences, earth sciences, and education. This longstanding relationship has enabled UMD to be one of NASA's top sources for future scientific and engineering talent.[19]

Through analysis of public information on grant and contract award data,[20] we determined that Since 2013, UMD has been the recipient of at least 36 NASA research grants and contracts. We also examined the Earth System Science Interdisciplinary Center (ESSIC) at UMD, which operates under a $95 million cooperative agreement with NASA. To date, NASA

[19] https://research.umd.edu/partnerships/government/partnership-overview-nasa
[20] Federal award data was retrieved from usaspending.gov.

has obligated approximately $85.4 million under these awards in aggregate. However, public reporting discrepancies and potential unrecorded awards likely underestimate actual NASA award amounts.

Surveys of scientific publications and supplemental research suggest widespread non-compliance with the Wolf Amendment by dozens of UMD faculty and staff researchers at ESSIC. This includes over 40 research publications coauthored by at least 30 UMD personnel - professors who are PIs / co-PIs on NASA grants or ESSIC staff researchers – that have engaged in what appears to be strictly bilateral collaborations with PRC institutions. Additionally, a few UMD faculty members involved in NASA-funded research appear to hold or have held concurrent positions at PRC universities, which may also be a violation. To assess non-compliance, further investigation is required to determine the exact nature of these collaborations and the research involved (i.e., to determine if the underlying research was based on NASA funding).

Some of the observed research papers credit both NASA and PRC government funding sources as supporting the research, including PRC defense funding. This raises national security concerns as it may facilitate the transfer of sensitive technology and data to the PRC institutions.

A few examples of strictly bilateral US-China research collaborations that have dual-use applications include:

- UMD Associate Professor Dongdong Wang led a study published in January 2018, titled *"Evaluating Land Surface Albedo Estimation from Landsat MSS, TM, ETM+, and OLI Data Based on the Unified Direct Estimation Approach."* This project is particularly concerning because the PRC funding sources clearly show China's strategic interest and defense application potential. PRC funders included the National 863 Program, the National Natural Science Foundation of China, the National Key Research and Development Program of China, and a National Defense Project of China.[21] China's 863 Program (now consolidated into a newer funding line) was focused on applied research and heavily involved in defense programs.

- UMD Professor Ning Zeng coauthored a December 2020 article titled *"Spaceborne Detection of XCO_2 Enhancement Induced by Australian Mega-Bushfires."* This study involved PRC co-researchers from Nanjing University and the Chinese Academy of Sciences. Some of the acknowledged funding includes multiple NASA grants as well as the National Natural Science Foundation of China and the National Key R&D Program of China.[22] The research involved sophisticated remote sensing techniques that could be repurposed for military applications.

- In June 2021, UMD Professor Sylvain Veilleux coauthored a study titled *"A Broadband Si_3N_4 Polarization Beam Splitter Based on Asymmetric Directional Couplers."* The study included a Chinese co-researcher from the Key Laboratory of Quantum Information at the University of Science and Technology of China.[23] Although primarily funded by NASA, the involvement of a

[21] https://doi.org/10.1016/j.rse.2017.10.031
[22] https://iopscience.iop.org/article/10.1088/1748-9326/abc846
[23] https://ieeexplore.ieee.org/document/9597974

leading PRC quantum information laboratory in developing advanced photonic technologies at a PRC university known to be extensively involved in defense research raises serious national security concerns. Such dual-use technologies are critical in the realms of secure communications and defense applications.

Additionally, several UMD researchers have maintained dual appointments or affiliations with PRC institutions. These positions are not merely honorary; they often entail active participation in research projects, curriculum development, and strategic collaborations with their Chinese counterparts. Such arrangements can facilitate the regular exchange of ideas, methodologies, and, in some cases, sensitive research findings. Notable examples include, but are not limited to:

- UMD Associate Professor Dongdong Wang has held a concurrent position at Peking University's Institute of Remote Sensing and GIS at the School of Earth and Space Sciences, *while serving as a NASA PI on several grants*.[24] The Institute of Remote Sensing and GIS faculty webpage of lists Wang as an Associate Professor and Changjiang Chair Professor.[25] The latter refers to the Changjiang Scholars Award Program, one of China's most prestigious talent recruitment programs that seeks experts from overseas to transfer technology and knowhow to China.
- Professor Zhanqing Li from UMD's ESSIC held a concurrent affiliation with the State Key Laboratory of Earth Surface Processes and Resource Ecology at Beijing Normal University.[26] *While Professor Zhanqing Li was a NASA PI*, he was also a PI for China's "973 Program" on a project titled "Observation and Modeling of Climate Effects by Clouds and Aerosol." That project appeared to run from January 2013 to August 2017 at the State Key Laboratory of Earth Surface Processes and Resource Ecology.[27]
- (Now Emeritus) Professor Shunlin Liang held a dual appointment at UMD and Wuhan University[28] and led significant remote sensing projects in China while working on NASA-funded research.

We identified numerous other examples of bilateral collaborations that may violate Wolf Amendment restrictions, such as multiple UMD researchers who visited China to provide lectures and participated in exchanges at PRC institutions (e.g., visits to Beijing Normal University, Peking University, and the Chinese Academy of Sciences) while concurrently serving as NASA PIs. *The examples discussed here merely scratch the surface of identified bilateral research collaborations and exchanges involving NASA-funded researchers. The scope of this activity suggests a systemic, institution-level disregard for compliance with NASA grant and contract rules.*

In addition to the government's lack of sufficient personnel and subject matter knowledge to pursue investigations of federal grant non-compliance, there may be another reason why OIG offices and DoJ have not aggressively pursued False Claims Act (FCA) cases against

---

[24] https://www.sciencedirect.com/science/article/abs/pii/S0048969724069407?via%3Dihub
[25] https://irsgis.pku.edu.cn/ls/ygcs/wdd/index.htm
[26] https://acp.copernicus.org/articles/18/8995/2018/
[27] https://espre.bnu.edu.cn/english/research/presentprojects
[28] http://www.lreis.ac.cn/kfji/sjlt/201807/t20180716_416275.html

UMD and other public universities: fear that public universities may assert 11th amendment-based sovereign immunity protections against their misdeeds.[29] This area of the law appears to be unsettled and largely untested. Therefore, perhaps understandably, risk-averse prosecutors may sometimes prefer not having to face that challenge, *potentially slowing the successful pursuit of civil claims against noncompliant public universities.*

It is encouraging that DOJ's recent FCA civil actions against the universities of Delaware and Maryland discussed earlier in this testimony indicate that both DOJ and the public universities it pursued the claims against did not believe assertions of sovereign immunity by public universities in these sorts of cases would be successful. However, it is also possible that the universities of Delaware and Maryland simply decided it was in their best interests to cut their losses and tie up those matters as quickly as possible, particularly given that the scope of their FCA violations could have been far greater than the (small) amounts of the settlement agreements.

Other PRC Threats, Influence Over Federally Funded Research

PRC state-sponsored talent recruitment programs number in the hundreds and play an instrumental role in China's economic development and military modernization efforts. They are statutorily designed to transfer technology and knowhow from overseas through any and all means at the PRC party-state's disposal. There has been considerable US government scrutiny on these programs - often described in various policies as "malign foreign talent recruitment programs" to differentiate them from scholarships and talent programs of other nations. Primers on the PRC's talent programs have been published elsewhere and thus are not included in this testimony. This testimony sheds light on lesser-known or understood elements of these programs that have affected federal funding of scientific research.

Some academics argue that the US government has exaggerated the risks and threats posed by China's state-sponsored talent programs. Some arguments center around the mirror imaging of our systems with the PRC – that most countries have talent promotion programs of various kinds, such as government-sponsored fellowships and scholarships that send citizens abroad to gain knowledge and experience and attract talent from the international community to further domestic endeavors. At a basic level, the PRC's government-led human capital investments do share similarities with those of the US and other nations: to help advance science and technology to bolster a country's economic development.

However, this overlooks key differences between programs in allied democracies and those in the PRC concerning the methods, requirements, supporting infrastructures, and how PRC talent programs integrate into and support a state-directed strategy to acquire technology and knowhow from around the world. The arguments downplaying the risks also overlook China's system of governance and *rule-by-law* approaches. This is particularly relevant as

---

[29] The 11th Amendment of the Constitution states: "The judicial power of the United States shall not be construed to extend to any suit in law or equity, commenced or prosecuted against one of the United States by citizens of another state, or by citizens or subjects of any foreign state."

PRC talent program selectees, regardless of nationality, are under contract with the PRC government: they are tasked and funded by party-state organs and subject to PRC law.

Many elements of PRC talent programs encourage insidious behaviors. Selectees of these programs can have corrupting effects on our academic institutions, exploit individual and institutional vulnerabilities through money and resources, undermine core values of academic research such as integrity and transparency, engender conflicts of interest or conflicts of commitment, and incentivize intellectual dishonesty and academic fraud. Depending on the academic institution, administrators have been unaware, turn a blind eye to (or admit they do not want to know), or are complicit; all of which demonstrate the corrosive nature of China's influence. The following case examples illustrate some of these insidious behaviors that threaten the security *and integrity* of our research enterprise.

Example A: Corrupting NOAA Research and Operations

An investigation I supported when I was in the government illustrates ways in which talent programs can involve malign influence and create corrosive effects on our research. This case is also important because it shows federal research facilities (such as our national laboratories) are also affected, not just universities. In this case, the government pursued a criminal investigation in part because the subject was a federal employee - a climate scientist at the National Oceanic & Atmospheric Administration (NOAA). The scientist was recruited through two nationally run PRC talent programs to take a part-time position at a PRC university while retaining his full-time employment with NOAA. The criminal elements of the case centered around prohibitions against government employees taking outside, concurrent employment with a foreign government.

However, the requirements of the PRC talent program appointments were the most concerning with respect to malign influence, many of which are not illicit acts. For instance, the NOAA researcher's contracts with the PRC government obligated him to:

- Sponsor specific PRC national researchers to work in his NOAA lab *as directed by the PRC*. The subject failed to evaluate multiple candidates for these positions as required; he bypassed merit-based hiring processes and systematically and repeatedly denied US applicants.
- Work on research projects at NOAA as determined by his PRC sponsors; collaborate on PRC government-funded research projects with specific scientists using NOAA facilities.
- Travel to and work in China for two full months per year which exceeded federal annual leave accruals. This meant the researcher was certifying time and attendance reports that he was working at NOAA and lying to his supervisors about his China-based commitments.
- Publish research that credited the PRC institution as the primary affiliation, even if the research was principally (or entirely) conducted at NOAA facilities. A literature review showed that the scientist published some papers listing his NOAA affiliation and other papers that listed him as exclusively affiliated with a PRC institution during his tenure at NOAA.

- Facilitate academic exchanges and formal partnership agreements between NOAA and the PRC institutions the subject held concurrent positions at, thus representing both parties during negotiations and violating US government ethics rules.

Clearly, most of these activities undermine the basic values of research integrity. Another highly disturbing element was discovered when federal investigators interviewed at least one of the PRC national researchers the subject hired. At least one of these PRC nationals stated that the NOAA researcher pressured him or her to work exceedingly long hours in the lab: they had to sleep and work in the lab on the weekends and do the lion's share of the research and drafting of publications that the NOAA researcher would claim as his own. The NOAA researcher exploited a power dynamic where the PRC nationals needed positive performance reviews for their careers back in China; if they complained to NOAA management, the NOAA researcher would take retaliatory measures against those PRC nationals.

Other investigations I supported involving talent program selectees at US academic institutions resulted in similar findings. Many part-time talent program selectees (those that retain their US positions) are tasked by their PRC employers or party-state organs to hire or sponsor specific PRC national PhD students and postdocs to work at US institutions to gain access to and support the research done there. Many of these talent program selectees were PIs on federal grants. Investigations also discovered that some of these US faculty members who were talent program selectees coordinated with the China Scholarship Council to provide funding for the PRC graduate students and postdocs' study in the US. A few of these cases *also found abuse and exploitation of the PRC national students, unbeknownst to the US institution.*

Academia has argued that recruiting individuals from personal and professional networks is a normal practice. However, it is important to differentiate this from the activity I am describing, which involves direct taskings - often under contractual obligations - by the PRC government to sponsor specific individuals and ignore merit-based hiring practices. At a minimum, this undermines the integrity of our open system; more damaging is when individuals are carrying out research projects conducted by specific individuals at the behest of the PRC party-state in critical technology fields and creating/controlling a talent pipeline strictly for China's benefit.

We do not know the scale or scope of this phenomenon. Nevertheless, when we examined numerous talent program selectees in prominent positions at US universities who are PIs on federal research grants, it was not uncommon to find that the majority of their graduate student body are PRC nationals, typically from select (and often high-risk) PRC institutions with which these faculty members have formal relationships via PRC talent recruitment programs. This calls into question oft-used arguments that there is insufficient US and other allied nation STEM talent available to fill graduate degree and postdoctoral programs at US universities or laboratories; that we are critically dependent on PRC talent. When some US faculty are financially obligated by their overseas (PRC institution) sponsors to appoint personnel, domestic STEM talent is simply overlooked or a lower priority. This practice has

been observed to take place for two decades, making this "dependency" on PRC talent highly concerning and a self-fulfilling prophecy.

Example B: Former UCLA Professor

While in government, I also supported efforts that identified then-UCLA Professor Songchun Zhu as part of a larger survey of US-China collaboration on AI and computer vision disciplines. We looked closely at Professor Zhu because of his extensive partnerships with PRC entities representing national security, integrity, and grant compliance concerns. Zhu had worked on DoD and NSF-funded research *totaling over $30 million* while simultaneously having significant commitments with PRC organizations, including via China's flagship Thousand Talents Program. In addition to suspected disclosure failures of current and pending support on grant applications, Zhu appeared to divert federally funded research to private companies he founded (based in China and the US). In other words, he was commercializing federally funded research for personal (and arguably China's) benefit.

Professor Zhu also partnered with and had talent program appointments at the Beijing Institute of Technology (BIT) and other PRC research institutions heavily involved in defense R&D. BIT is a "Seven Sons of National Defense' university involved in weapons and defense program research. Even if he was not violating US law, his PRC collaborations and appointments represented serious national security and conflicts of interest and commitment concerns.

In 2019, I provided extensive information on Zhu to DoD counterintelligence components as well as senior DoD leadership to demonstrate the nature of these threats. No actions appear to have been taken at least while I remained in government. Zhu recently relocated to China and now leads a massive AI research effort there, as reported by *Newsweek.*[30] The decades of knowledge and research projects he conducted for DoD are presumably furthering China's AI efforts, including in applied domains through his companies. Many of the PhDs and postdocs he sponsored and trained at UCLA subsequently worked at his companies. Some of those individuals are now in China leading major AI, computer vision, and related research that have mass surveillance and military applications. Thus, the US taxpayer – especially through DoD – funded and trained multiple generations of PRC scientists in critical technology fields that are now at institutions supporting PRC military and public security organs.

It is highly probable that Zhu's appointments in China and activities with his companies may have violated federal grant rules, especially regarding disclosures of current and pending support and affiliations in China. Even if Zhu's actions were not illicit in nature and thus a criminal investigation was not warranted, the US government could have pursued civil remedies, such as through OIG investigations, and would have likely found systemic non-compliance with federal grants. Through civil and administrative remedies, federal agencies could have denied funding to Zhu and his programs at UCLA, which in turn could have prevented him from building a hiring pipeline of PRC nationals for his (and China's) benefit;

---

[30] Didi Kirsten Tatlow, "Exclusive: U.S. Gave $30 Million to Top Chinese Scientist Leading China's AI 'Race'," *Newsweek,* November 1, 2023, https://www.newsweek.com/us-gave-30-million-top-chinese-scientist-leading-chinas-ai-race-1837772.

and his lack of access to DoD funding would also make him less desirable to PRC institutions that recruited him. If US government national security elements had worked with OIG components and acted swiftly, much of the knowledge transfers to China, funded largely by DoD, may have been prevented. We must learn from these unforced errors.

Example C: Influence Over NSF Grant Award Processes

NSF relies heavily on Intergovernmental Personnel Act (IPA) assignees - typically academics in scientific and engineering fields - to take temporary assignments to serve as program directors and grant managers. These individuals oversee NSF grant application submissions, evaluation and award processes, and related grant program management functions. IPAs are not federal employees but are subject to provisions of law governing the ethics and conduct of federal employees.[31]

While in government, as part of my interagency efforts to assess risks and threats associated with PRC talent programs, my colleagues and I discovered a troubling issue: some talent program selectees who were faculty at US universities took IPA assignments at NSF to serve as grant managers. We compiled data on the NSF grants those individuals were responsible for (which included making grant award decisions) and found that some of the grants were awarded to researchers who were also selectees of the same PRC talent programs. Additionally, several of the awardees (PIs) of these NSF grants who were recruited by PRC talent programs subsequently become IPAs at NSF themselves and then awarded grants to *other* PIs who were PRC talent program selectees and to former IPAs. One of the talent programs that the identified IPAs were affiliated with was established around the year 2000; the first IPA position of one of these talent program selectees began around 2005.

Consequently, we observed a vector of influence where individuals simultaneously under contract with the PRC government were making NSF grant award decisions for nearly two decades. The number of individuals we found implicated in this scheme was small. However, due to limited resources, our focus was only on one NSF division. We do not know whether this type of activity has taken place at other NSF divisions. Additionally, *I am not aware of any efforts since that discovery to identify similar activity at other federal agencies that employ academics (typically as IPAs) as part of their grant management structure.* This is just one method of PRC malign influence over federally funded research.[32] *Based on my experience, it appears that the scale and scope of PRC influence activities over federal grant award decisions are largely unknown.*

Example D: Hijacking NSF CAREER Awards

The PRC government clearly prioritizes the recruitment of individuals who received or supported federal research grants. PIs on DoD grants are obviously of very high interest for China to recruit, but talent programs have also recruited many recipients of other agency funding. A troubling trend is China's recruitment of academics who recently completed or

---

[31] https://new.nsf.gov/careers/rotator-programs/intergovernmental-personnel-act-ipa-assignments

[32] NIH has discovered and disclosed publicly a situation where the confidential peer review process of grant applications was compromised by some PRC-affiliated actors. This represents a similar type of influence, but here again, it is not known to what extent this has taken place.

are nearing completion of their term as an NSF CAREER awardee. "The Faculty Early Career Development (CAREER) Program is an NSF-wide activity that offers NSF's most prestigious awards in support of early-career faculty who have the potential to serve as academic role models in research and education and to lead advances in the mission of their department or organization. Activities pursued by early-career faculty should build a firm foundation for a lifetime of leadership in integrating education and research."[33]

In other words, NSF's CAREER program is an investment in future science and engineering leaders, where they are given a prestigious line of funding to *kickstart their promising and lengthy careers in the US*. PRC talent programs have been observed to recruit some of these individuals to work in China, thus benefitting from (and exploiting) the significant investments made by the US government and further eroding our STEM talent pipeline.

Example E: Exploiting SBIR Programs

PRC talent programs and state-backed investment entities have also targeted recipients of DoD-funded Small Business Innovation Research (SBIR) programs. A small (government-use only) study I supported while I served in government found that China has benefited from DoD's SBIR programs and revealed vulnerabilities to potential future DoD supply chains. Not all of China's exploitation of SBIR contracts involved the use of talent programs, but in many observed cases, key personnel (founders, chief scientists or engineers, CEOs, etc) of startups receiving SBIR funds were recruited through a talent program or received PRC state-backed start-up capital.

- Some key employees of US firms receiving SBIR contracts were recruited via a PRC talent program and relocated to China, but they continued research collaboration with officers of the US companies where they were previously employed.
- US firms established PRC-based subsidiaries, receiving funding through PRC state-funded entrepreneurial contests that function similarly to talent programs. In some cases, the firms subsequently dissolved their US operations.
- In one observed case, a recipient of multiple DoD SBIR contracts established another firm in China based on the same technologies, developing combat vehicles in partnership with the state-owned defense conglomerate China North Industries Group Corporation (NORINCO).

US-Based Support Networks for PRC Technology Transfer Activities

There are organizations in the US that demonstrably partner with, take tasking and direction from, or serve as a proxy to Chinese Communist Party (CCP) organs and the PRC diplomatic missions. In the US, these entities are typically non-profit professional associations that claim to be NGOs. While many of these organizations engage in professional networking and entrepreneurial activities that are not illicit in nature, they often support PRC state-directed activities, *including substantial involvement with PRC talent programs*. Details on specific organizations and case examples cannot be provided in this testimony, as the preparation

[33] https://new.nsf.gov/funding/opportunities/career-faculty-early-career-development-program

and dissemination of that information is considered government use only.[34] However, I can offer some key findings:

- Key leadership of some of these non-profit organizations are federal government researchers at NOAA, NASA, the Department of Energy, etc. Yet these organizations routinely meet with and receive taskings from CCP organs and PRC diplomats (especially in the S&T and Education sections of the PRC Embassy and its consulates).
- Some organizations organize, host, and serve as judges for talent programs and start-up contest activities operated or sponsored by the PRC government. Leadership of these organizations run venture capital and angel investment structures in the US.
- Some of these organizations also routinely meet with (and likely take instruction from) CCP United Front organs and PRC diplomatic mission personnel in the US.

China's Role in Undermining Research Integrity and US Inaction

Research security, research integrity, and malign influence are often intertwined, especially when dealing with the PRC. Governments and research institutions in liberal democracies espouse and stress the importance of values such as academic freedom, transparency, integrity, and reciprocity concerning the conduct of research and international research collaboration. The G7 Security and Integrity of the Global Research Ecosystem Working Group defined a set of "Common Values of Research Integrity," which included transparency concerning disclosures of researcher affiliations, conflicts of interests, and sources of funding, and honesty regarding proposing, undertaking, reviewing, and communicating research.[35]

However, PRC party-state organs and research institutions routinely violate these norms and values that are critical to beneficial research collaboration and trust in science. **When both the US government and academia espouse "common values" of transparency, integrity, and reciprocity but impose no cost to PRC researchers and institutions that violate these values, they signal to PRC entities that the status quo is acceptable.** *The US government has taken no observable policy measures to mitigate PRC practices that undermine research integrity, even when federal research funding is affected.*

My non-profit's latest publication catalogs numerous ways China has violated these norms and the implications of academia and government inaction.[36] My colleagues and I examine China's lack of transparency, which often is intentional to mislead the international community, as well as types of fraud in published scientific literature. Academic fraud in publications is a global phenomenon and by no means unique to China. However, China is

---

[34] Note however, that some organizations, particularly those principally engaged in technology transfer activities, are described in the edited volume, *China's Quest for Foreign Technology: Beyond Espionage,* Hannas and Tatlow eds., Routledge, 2021)

[35] "G7 Best Practices for Secure & Open Research," Security and Integrity of the Global Research Ecosystem (SIGRE) Working Group, May 2023.

[36] Stoff, McIntosh, and Lee, "Transparency and Integrity Risks in China's Research Ecosystem: A Primer and Call to Action," *Center for Research Security & Integrity*, 2024.

by far the world's largest producer of fraudulent publications, which has a profound impact on trust in the global research enterprise.

The issues described in this study should warrant rigorous policy responses from both the government and academia, yet their silence is deafening. The incentives and interests of individuals and their research institutions probably drive inaction. Research institutions routinely make exceptions to their espoused values and core principles of academic research when dealing with China. A *sampling* of China's practices include:

- Adding foreign coauthors who had no material involvement in the research to bolster the reputations of the other coauthors and institutions
- Listing a PRC institution as the only affiliation when most or all of the research occurred outside of China
- Creating fictitious coauthors with stated affiliations to reputable foreign institutions
- Producing fake papers in paper mills; intentionally using falsified or manipulated images or data
- Denying access to PRC websites of institutions from outside China or removal of content
- Obfuscating or misrepresenting PRC entity names, missions, projects or funding sources, parent organizations, etc.; discrepancies between English and Chinese information that strongly suggest intentional deception
- Failing to disclose financial conflicts of interests or outside involvement (as a shareholder, company board member, founder or chief scientist/engineer of commercial firms) on any CV, faculty page, grant, or (co)authored publication

PRC entities that lack transparency or integrity undermine trust, complicate the US government and academia's due diligence and risk assessment efforts, and create an unsecured research environment. Additionally, fraudulent publications can be harmful when scientists, clinicians, or even policymakers make decisions based on fake or manipulated science.

Case Example: 'Comfort Letters'

I advised on other investigations when I was in government – some of which involved instances where a PRC institution provided a letter to NIH that contained demonstrably false information to mislead a grant compliance investigation. The cases involved PIs at US research institutions under investigation for allegations of failure to disclose outside appointments or affiliations with a PRC institution. In a few cases I supported, the PIs were assigned to work 12 months per year on a federal grant; thus, undisclosed appointments can represent conflicts of commitment and violate NIH grant terms.

NIH posted an illustrative case on its website. A Senior Deputy Director of Research at a PRC university provided an official "comfort letter" (as NIH describes it) to the scientist and the US institution, stating that the scientist under investigation was merely honorably invited as a guest professor, did not hold any official faculty position, and had no formal contract

through a PRC state-run talent program; the individual just had a "gentlemen's agreement" with the PRC entity. However, the employing US institution reported to NIH that it discovered documents indicating the researcher did, in fact, receive a talent program position and had a formal agreement with the foreign university to work as a "distinguished part-time professor" for three years.[37]

This "comfort letter" provided to the US institution was intended to deny and deceive NIH, and it being sent by a senior leader from a PRC institution indicates institutional-level dishonesty. NIH has received an undisclosed number of "comfort letters" from PRC research institutions. Thus, it is not known how many PRC institutions were involved or how pervasive this dishonesty has been. **Regardless, this problem calls into question whether US researchers should receive federal research funding on projects that involve collaborations with PRC entities that have sent false and misleading information to federal agencies**. *I am not aware of any policy at federal funding agencies that addresses this issue.*

Reciprocity

Issues of reciprocity are also not receiving scrutiny, and the US government and academia's inaction raises important policy questions. Here are two examples:

US-China research collaboration also takes place at federal agencies via national laboratories, federal facilities, and other government-run infrastructures that carry out their own research. Some of these agencies oversee collaborative projects with the PRC through formal cooperation agreements. When I was in the government, officials at several federal agencies discussed the fact that sometimes the partnering PRC institutions failed to abide by the terms of a research agreement, such as failing to provide the promised resources, data, or personnel. In some cases, an agency decided to cease or not renew such a partnership. In other cases, however, collaborations continued despite the PRC not meeting its obligations - perhaps in the interest of furthering diplomacy or gaining cooperation from the PRC in other areas.

Another issue is that PRC data/information laws can restrict or prohibit PRC research institutions from sharing the underlying data on published research with the rest of the world. When findings are published based on specific data, but the PRC prohibits its release, then the research community cannot validate or replicate the research results or methods elsewhere. *I have seen very little investigation or scholarship on when and how often this occurs, whether federal research funding was involved, or whether the US government has developed any policy response.*

US Government Challenges and Impediments to Building Robust Research Security Programs and Policies

Up to this point, I have described the numerous ways in which the PRC exploits federally funded research, academia's systemic non-compliance with federal grant rules and

[37] Posted case studies are available on the Policy and Compliance page of the NIH website: https://grants.nih.gov/policy/foreign-interference/case-studies.

appropriations laws, and a lack of policy responses by both academia and the government in addressing research security vulnerabilities. This section focuses on the US government's structural impediments, failures, and knowledge and policy blind spots that impede its ability to monitor and enforce compliance on federal research grants and contracts and to protect our early-stage research and innovation ecosystem more broadly. (The final section of this testimony offers recommendations that the legislative and executive branches can implement that specifically address these deficiencies.)

Most of the structural impediments and failures by the US government to adequately protect federal research investments discussed below are based on my observations supporting national security, law enforcement, policy, and OIG elements, as well as engagements with executive leadership of federal agencies. I will break down the challenges by first examining strategic and structural issues, followed by more tactical areas. It is worth noting that a few individuals in the US government (in addition to myself) have pointed out these challenges and have recommended to executive branch leadership some of the solutions described in this testimony since early 2021 or, in some cases, even earlier. To date, however, these problems have persisted and remain laregly unaddressed.

Policy Gaps

As noted in this testimony, there are only two rules currently in effect that restrict research collaborations or partnerships with PRC entities within fundamental research domains: a) the Wolf Amendment that bars recipients of NASA research funding from engaging in any bilateral collaborations with China unless a Congressional waiver is applied; and b) a newly instituted provision (Sec. 238) of the FY25 NDAA that will restrict recipients of DoD funding in fundamental research areas if they collaborate with a select group of PRC entities. However, the current list of entities that apply to this policy is inadequate and needs to be expanded.

Recipients of fundamental research grants or contracts from any other federal source face *no other restrictions or limitations on national security grounds*. Academia is free to work with any PRC organization of their choosing, even if those same entities face trade restrictions (export controls) or sanctions. The over 27,000 articles involving US researchers and the PLA, PRC weapons R&D and production facilities, and other defense research organizations attest to the fact that academia does not take research security seriously when there are no specific prohibitions in place.

Similarly, there is no clear policy proscribing research funding if recipients partner with authoritarian regimes on research with potential applications in mass surveillance and human rights abuses. Program managers overseeing federal research grants and contracts do not appear to take this into account when awarding research dollars to institutions. Universities are either unaware that ethically troubling research collaborations are taking place or turn a blind eye to them.

The government also lacks policies to address integrity, transparency, and reciprocity issues, even when federal research funding is affected. For instance, federal agencies like NIH do not share information on the "comfort letters" it has received from PRC institutions that

provide false statements to obstruct grant compliance investigations. The PRC entities engaging in dishonest practices do not appear to face any repercussions for their actions, i.e., agencies have set no restrictions or conditions on funding to entities that partner or collaborate with these dishonest PRC organizations. The same goes for situations where a partnering PRC institution fails to share data or materials that went into published findings, including research (co-)funded by the US government. Neither the government nor academia appears willing to impose any costs on PRC institutions when they violate the core principles and values of academic research.

Intelligence Community and Law Enforcement Shortcomings

Structural impediments persist within the intelligence community (IC) and law enforcement components such as the FBI and military department investigative units. China's state-supported technology transfer apparatus targeting unprotected and unregulated areas dwarfs illegal or espionage activities, yet the latter have monopolized US government attention and resources. Messaging by the US government that China is stealing secrets from academia is misleading and misguided. The following are examples of the shortcomings that leave federal research investments vulnerable to exploitation by China.

- Law enforcement elements focus largely on identifying criminal activity; in cases of technology transfer, this means critical knowhow or intellectual property has already been transferred or stolen, i.e., cases usually involve showing the damage that has been inflicted, rather than protection and disruption efforts.

- The counterintelligence community has not sufficiently adapted to post-Cold War realities, especially with China. A myopic focus on chasing PRC spies leaves most of our research unprotected, given China's tactics within fundamental research domains rarely involve its security services. While I was in the government, my support to counterintelligence elements in the FBI and DoD showed that those offices prioritized criminal investigations over leveraging operational approaches to deny and disrupt PRC state-directed technology transfer activities.

- The IC's over-reliance and imputed value on classified information sources limits the government's ability to share information with public and private sectors. This situation has been worsened by a multi-decade erosion, descoping, and devaluation of open-source intelligence within the IC and has led to unaddressed and yawning knowledge gaps.

Lack of Expertise

A dearth of Mandarin language-capable analysts and subject matter experts in the IC and law enforcement has led to a fundamental lack of understanding of the magnitude and complexity of China's state-supported technology acquisition and transfer apparatus. This has created additional challenges, including:

- A lack of understanding of how China has built a massive apparatus to recruit experts globally and exploit US (especially federally funded) research. Experts are primarily targeted by the PRC *after* gaining knowledge and experience overseas. The argument that high percentages of PRC nationals stay in the US after receiving advanced degrees and thus benefit the US is too simplistic; much of China's strategy is to tap into overseas-based

experts who "serve in place." Creating incentives to stay with no corresponding protections has allowed the PRC to exploit and influence our research to its benefit with impunity.

- Ineffective messaging to the public by the national security community. Most officials conducting public outreach do not have relevant experience or knowledge, which limits their ability to address specific questions from audiences or have information available that is tailored to those entities. The standard model of providing general talking points for law enforcement agency field offices' use is not effective at building trust and confidence with the private sector and academia.

- Analytic components in the IC are not mandated to perform or are evaluated on due diligence or vetting requests. The lack of any significant support to US research institutions regarding research security and integrity has placed the burden of conducting due diligence and risk assessments almost entirely on individual institutions.

- Persistent knowledge gaps on PRC academic and commercial entities conducting R&D tied to defense and public security apparatuses limit the government's ability to identify risks, especially in critical and emerging technology fields.

Grant and Contract Compliance Monitoring and Enforcement Shortcomings

The aforementioned challenges also negatively affect the US government's ability to monitor and enforce compliance with federal research grants and contracts. Much of the shortcomings listed below stem from a lack of common standards for assessing risk, minimal capacity to conduct due diligence, an unwillingness to share data among agencies, and a critical shortage of experienced investigators who have the requisite subject matter expertise to pursue civil, administrative, and criminal investigations relating to federal grant compliance.

Deficiencies with Vetting, Due Diligence, and Compliance Investigations

Each agency has its own research security and due diligence process; there are no consistent methodologies or standards for assessing risks across federal agencies. Within the DoD, different program offices conduct varying levels of due diligence (if any) and have their own standards or rules that may be inconsistent and uncoordinated across the defense enterprise. There is also no central place where offices can check for existing derogatory information on grant or contract applicants to do simple due diligence checks.

Proposers on grants or SBIR contracts have been observed to "shop around" – if one agency or component denies an award based on assessed national security risks (e.g., foreign ownership, control, or influence), they will apply to another element and sometimes get awarded due to no common standards for risk. When I worked in the DoD, on more than one occasion, due diligence checks by one intelligence component found derogatory information showing ties to hostile foreign entities that pose a national security risk. Several DoD components chose to decline to award a contract, but one component ignored the derogatory information and allocated funding anyway.

Other deficiencies include, but are not limited to:

- Many program offices that award research grants or contracts to academia lack comprehensive tools, technical solutions, or capabilities to assess risk or screen grant applicants for potential national security concerns. In one observed case, an academic applied for a research grant on a project that was already funded by the PRC, but this was not discovered until after the grant was awarded due to a lack of capabilities and subject matter knowledge of the program offices. Additionally, some DoD program offices lack sufficient information on grant applications and documentation on all individuals supporting the research other than principal investigators (PIs).

- Vetting of foreign nationals prior to grant or contract award, if done at all, is insufficient: the PRC party-state targets, recruits, and co-opts individuals *after* they have expertise and access to critical research in the U.S. (many of whom are US citizens). The US government has few resources or processes in place to monitor for national security risks *post award* of a grant or contract.

- A lack of data sharing between agencies results in duplicative due diligence and risk assessment reviews. This also handicaps fraud or other grant compliance investigations when more than one agency is affected, which is not uncommon. When I was in the government, I supported a Foreign Influence Investigations Working Group (FIIWG) made up of OIGs, DOJ prosecutors, and military investigative elements. The working group's intent was to share data and information and assist investigations across agencies. However, information sharing was voluntary, and different agencies had varying priorities and data-sharing rules that led to a general unwillingness to share information.

- Inadequate resources and personnel in Offices of Inspectors General severely constrain their ability to investigate fraud, compliance failures, and malign foreign influence or interference in federally sponsored research.

- A dearth of analytic and subject-matter expertise to conduct due diligence and knowledge on how to investigate criminal, civil, administrative, and compliance issues related to research security. I am aware of only a few individuals who remain in the government who have a high level of understanding and experience of how to conduct the analysis and investigations related to university non-compliance with federal grants and contracts.

Recommendations for Policymakers

The challenges we face in protecting federally funded research are daunting due to extensive exploitation and malign influence by China, systemic non-compliance by universities on federal awards, a lack of sufficient research security measures or policies by either academia or the US government, and structural deficiencies within the national security and law enforcement communities.

On February 21, 2024, the White House issued a new presidential memorandum titled "America First Investment Policy." This document calls for developing new measures to "reduce the exploitation of public and private sector capital, technology, and technical knowledge by foreign adversaries such as the PRC." The policy also includes creating or expanding restrictions on US outbound investment in the PRC relating to critical

technologies, such as semiconductors, artificial intelligence, quantum, biotechnology, hypersonics, aerospace, advanced manufacturing, and directed energy areas that all have dual-use/defense applications.[38]

Interagency efforts to prevent PRC's acquisition and further development of these areas outlined in this new investment policy will not be effective if there are no corresponding policies and protection measures put in place within our research ecosystem, as this is where the talent and technology development originate. To address the problems described in this testimony, we must aggressively break down silos and build new paradigms within the government. *Simply appropriating additional resources for existing research security efforts, for example, will achieve little if the structural and knowledge deficiencies are not addressed.*

This final section offers recommendations that seek to: a) address persistent knowledge, regulatory, and policy gaps; b) re-align academia's incentives that better comport with US national interests; c) create efficiencies and cost savings to the US government in compliance monitoring and enforcement; and d) limit the PRC's near unfettered access to federally funded research and impose real costs to China when it violates commonly accepted norms and values.

It is worth noting that my recommendations *exclude* much-needed efforts to bolster domestic STEM research and education to reduce dependencies on adversarial nations like China. Research security is pointless if we lose the technology at the point it is ready to leave the lab because we lack the ability to manufacture it competitively or an engineering workforce and risk capital to support pilot projects and work through scaling challenges. We have allowed many of the links in the chain to atrophy by outsourcing so much of our inputs, including human capital. Reducing federal investments in R&D will complicate any protection and research security measures we put in place, as this will incentivize academia to further pursue partnerships with and/or accept money and resources from China to make up the shortfalls.

1. Pass the DETERRENT Act.

The Defending Education Transparency and Ending Rogue Regimes Engaging in Nefarious Transactions Act (H.R. 1048), also known as the DETERRENT Act, has been re-introduced in the House as the last Congress failed to pass the bill. This Congress *should review and pass this bill largely in its current form.* The bill would go a long way in bolstering enforcement of foreign gift, contract, and grant reporting requirements of higher education institutions, especially when supplemented with the other recommendations of this testimony.

2. Require recipients of NSF CAREER awards to sign a continuing service agreement with the US government.

The PRC has benefitted from substantial NSF investments in future scientific leaders by recruiting recipients of NSF CAREER awards that relocate to China. To prevent this, NSF

[38] https://www.whitehouse.gov/presidential-actions/2025/02/america-first-investment-policy/

should create a new condition that CAREER award recipients must stay in the US and work at a research institution or in the US government for a specific length of time as determined by NSF and Congress, but should at minimum be equal to the period of performance of the award.

3. Create new legislation that places restrictions on all federal sources of fundamental research funding if recipient institutions collaborate with select PRC entities.

Sec. 238 of the FY24 NDAA[39] restricts DoD fundamental research funding to institutions if they collaborate with academic entities listed pursuant to provisions of Section 1286 of the FY19 NDAA. This is a significant and positive step in curtailing research collaborations with PRC military-affiliated research institutions. *This rule should be applied to all federal funding,* and the list of "covered entities" to which funding restrictions apply needs to be expanded to other government-restricted lists.

The current list associated with the requirements of Sec. 1286 is too narrow in scope. Federal funding on fundamental research should also be denied to institutions collaborating with PRC organizations on the BIS Entity List, the OFAC sanctions list, and DoD's 1260H list of military-affiliated companies (as some of those entities conduct and publish research). Efforts are also needed to revise and expand the entities on these various lists. This should be a line of effort discussed in more detail in Recommendation 6.

4. Federal funding agencies should more aggressively use grant suspension and debarments.

Federal funding agencies should institute policies that more aggressively suspend and debar federal grants to institutions that have lapses in institutional governance and grant compliance. Research institutions need to bear greater costs for non-compliance with federal awards. For instance, agencies should suspend all new awards to an institution that has submitted false claims until it can demonstrably show remediation measures have been put in place.

5. Revise appropriations law or require federal agencies to insert new requirements on all federal research grants and contracts that state that all recipients of federal funding will be subject to the False Claims Act.

One legal interpretation of the 11th Amendment is that any state institution, including public universities, is immune from False Claims Act civil suits as this equates to the federal government suing a state government, which would violate a state's sovereign immunity. This hampers the ability of federal agencies to pursue False Claims Act cases against state universities. *Any public institution should be subject to the same responsibilities, standards of compliance, and fraud provisions as private entities. Waiving any 11th Amendment*

---

[39] "LIMITATION ON AVAILABILITY OF FUNDS FOR FUNDAMENTAL RESEARCH COLLABORATION WITH CERTAIN ACADEMIC INSTITUTIONS"

immunity claims should be a condition for a public university to accept grants or contracts from the federal government.

6. Authorize NSF to Create a National Research Security, Integrity, and Compliance Center and enable a corresponding interagency investigative task force.

The NSF Office of the Chief of Research Security, Strategy & Policy and NSF's OIG have arguably been the most effective and forward-leaning within the US government in building an infrastructure for leading and enhancing research security policies, programs, grant compliance investigations, and information sharing efforts across the US government. Some of these efforts are still in their early stages, but the infrastructures and knowledge already in place allow for greatly expanded efforts to address the government's impediments and deficiencies described in the previous section. **Policymakers should support the establishment of a new structure at NSF, notionally referred to here as the National Research Security, Integrity, and Compliance Center (NRSICC), that greatly builds upon existing efforts AND consolidates all US government-wide approaches to research security and integrity policy development, vetting, due diligence, risk assessments, and grant and contract compliance monitoring and enforcement.**

Consolidating all efforts into one central entity should lead to very substantial cost savings and greatly improve the US government's efficiencies and effectiveness in securing our research ecosystem from China's (and other adversarial nations) predations, as well as address the systemic non-compliance by US research institutions. **The recommended functions of the new center would be self-sustaining in terms of costs to operate; i.e. no additional appropriation of funds would likely be needed.** A detailed concept of operations exceeds the scope of this testimony; the following summarizes key lines of effort, structure, goals, and cost savings.

NRSICC Lines of Effort

A. Consolidated Data Analysis, Due Diligence, Risk Assessments, and Support to Government Investigations

All applications, periodic submission reports, and related documents pertaining to all fundamental research grants, cooperative agreements, and SBIR/STTR contracts awarded by all federal agencies should be housed at the Center. All government offices conducting fundamental research and SBIR/STTR due diligence will be detailed to the Center. This will streamline and ensure fundamental research due diligence is done by a single entity with a single set of risk assessment standards and mitigation framework.

- NRSICC will create and manage a single list of foreign entities and programs that are sanctioned, violate export control laws, or represent national and economic security risks. This includes but is not limited to: foreign malign talent programs, foreign defense research and industrial base entities, entities involved in committing human rights abuses, and any other entity or program that engages in the transfer or diversion of human/intellectual capital, technology, knowhow, or other ethically troubling activities.

- NRSICC analysts will conduct deep-dive due diligence research and analysis on all government (fundamental) research grants and SBIR/STTR contracts to determine risk levels and/or prohibitions/denials of funding. Analysts will also perform data analysis and research to generate leads for law enforcement when suspected criminal, civil, or administrative violations are identified.

While not directly part of the proposed Center, a law enforcement task force made up of OIG agents, auditors, and support personnel, DoJ prosecutors, and other law enforcement components across the government, will formally work with the Center. *This task force will be assigned to exclusively pursue civil (such as False Claims Act) and criminal compliance investigations based on the data and analytic support provided by NRSICC*. NSF's Office of the Chief of Research Security, Strategy & Policy has already built an internal tool for identifying potential non-compliance by NSF PIs or co-PIs. This capability would be incorporated into the functions of NRSICC and be expanded to ingest and analyze all other federal agency data.

B. Due Diligence, Risk Assessment Support to Academia, Private Sector

NRSICC data analysis, due diligence and risk assessment efforts would not just be limited to government award decisions and compliance investigations. The Center would also provide direct support to public and private institutions that have received or are applying for federal research grants, cooperative agreements, or SBIR/STTR contracts or grants. NRSICC would serve as the government's central point of contact to assist institutions that lack the capabilities and resources to conduct robust due diligence on their own.

The due diligence support efforts outlined in parts A and B can also inform and enhance the creation of a consolidated knowledge base on foreign entities posing national, economic, or ethical risks to the U.S. that the government currently lacks.

C. Research Security and Integrity Policy Development, Refinement

NRSICC will develop new government-wide policies on research security and integrity issues, including addressing the policy gaps described in this testimony. Through coordination with relevant agencies and White House offices, NRSICC would develop and design policies that would apply to all federal research grant awards and contracts in fundamental research domains. Policy development activity should include the following:

- Coordinate and implement all policy changes proposed at the interagency to be implemented by all federal funding agencies.
- Create or refine standardized application forms, periodic reports, and supporting documents on all federal research grants and SBIR/STTR awards.
- Track information on and develop new policies in response to China's integrity and reciprocity failures affecting federal research investments.
- Develop and refine due diligence and risk assessment methodologies and set standardized (government-wide) rules on federal award approval and denial decisions.

- Build a collection and analysis program to close persistent knowledge gaps on PRC entities that pose risks to US national interests and oversee the process for nominating entities that would be restricted. This effort would also include harmonizing the lists DoD is required to maintain with our export control and sanctions regimes.

- Develop and deploy training programs to build subject matter expertise among data analysts and risk assessors. Build separate (but related) training programs in coordination with NSF's OIG for investigators and prosecutors on how to conduct research grant and contract compliance investigations across the federal enterprise.

D. Cost Savings and Revenue Generation

- Consolidating all contracts, subscription services, and licenses into NRSICC, rather than having those duplicated across many federal funding agencies and research security offices, would save the government at least several million dollars annually.

- Initial automation and data aggregation tasks would save time and effort spent on initial due diligence, which would translate into potentially faster outputs and cost-savings through utilizing one IT infrastructure to produce and review materials.

- Incorporating the efforts of the newly established NSF SECURE Center[40] (Safeguarding the Entire Community of the U.S. Research Ecosystem) and its functions into the NRSICC will provide additional resources and could save taxpayer money.

- The increased civil grant compliance investigations, especially through False Claims Act litigation that result from dedicated NSRICC and investigative task force functions, would generate millions of dollars per year in recoveries from universities found liable and may cover most of the center's operating budget.

- Adding a 0.1% to 0.4% "due diligence tax" on all fundamental research grants and SBIR/STTR contracts would likely cover all costs associated with NRSICC's due diligence operations that support both federal agencies and research institutions requesting assistance.

NSRICC's functions and activities are partly intended to establish a genuine, whole-of-government approach to research security. The policies, subject matter expertise, and training programs developed by the center could also be used to support key allies and partners around the world that face many of the same threats and challenges from China as we do and, in many cases, have even fewer resources and capabilities to mitigate research security threats on their own.

---

[40] The current (nascent) tasks of NSF's SECURE Center, which is run by a consortium of universities, largely focus on awareness, training, and government-university engagements. Its functions are much more limited in scope than the proposed NRSICC.

Biography of Jeffrey Stoff

Jeffrey Stoff is the founder and president of the Center for Research Security & Integrity (CRSI), a US non-government, 501(c)(3) non-profit organization dedicated to the protection of research and innovation from harmful foreign influence and interference. Mr. Stoff is also a Non-Resident Senior Research Fellow at the newly established Stockholm Center for Research and Innovation Security.

Mr. Stoff spent over 18 years in the US government as a China analyst and linguist and is a recognized expert in technology protection issues. He has advised the White House Office of Science and Technology Policy and National Security Council; Office of Director of National Intelligence (ODNI); FBI; Department of Defense leadership, the Departments of Commerce, Energy, and State; the National Science Foundation; and the National Institutes of Health. Mr. Stoff received two ODNI awards, including the National Counterintelligence and Security Center Director's Award for Excellence, and the 2020 FBI Director's Award for Excellence. Mr. Stoff has presented at dozens of workshops, seminars, and conferences on research security and technology protection issues and has provided research security training to Canadian, Danish, Dutch, and German governments and research institutions. He has presented at dozens of conferences and seminars for US and foreign government, academic, and private sector leaders on research security and technology protection issues.

Mr. Stoff earned a master's degree in international affairs at the University of California, San Diego, and is a contributing author of *China's Quest for Foreign Technology: Beyond Espionage* (Routledge, 2020); coauthor of "Global Engagement: Rethinking Risk in the Research Enterprise" (Hoover Institution, 2020); coauthor of "Eyes Wide Open: Ethical Risks in Research Collaboration with China" (Hoover Institution, 2021); contributing author of *Chinese Power and Artificial Intelligence: Perspectives and Challenges* (Routledge, 2022); author of *Should Democracies Draw Redlines around Research Collaboration with China? A Case Study of Germany* (Center for Research Security & Integrity, 2023); and coauthor of "Transparency and Integrity Risks in China's Research Ecosystem: A Primer and Call to Action" (Center for Research Security & Integrity, 2024).

Chairman MCCORMICK. Thank you for your testimony.

And now Dr. Maria Zuber is a Professor of geophysics and Presidential Advisor for Science and Technology Policy at Massachusetts Institute of Technology. And from here on, we can actually use MIT as an acronym since I've just explained it. Most people have never heard of it. She's a leading university voice on research security and co-chaired the National Academies' National Science, Technology, and Security Roundtable. We welcome your remarks.

TESTIMONY OF DR. MARIA ZUBER,
E.A. GRISWOLD PROFESSOR OF GEOPHYSICS
AND PRESIDENTIAL ADVISOR FOR SCIENCE
AND TECHNOLOGY POLICY, MIT

Dr. ZUBER. Chairman McCormick, Ranking Member Sykes, and Members of the Subcommittee, thank you for inviting me to testify today.

Striking the right balance on how the U.S. research enterprise should interact with China is critical to U.S. national security and competitiveness. Getting that balance right is not easy or obvious. We know that China is an economic, geopolitical, and military rival and that China has sought to advance through illicit means. Even now, when China has considerable strengths of its own, it tries to take undue advantage of U.S. research efforts. Yet cutting all ties to China would likely hobble the U.S. competitiveness as much as it would harm China.

Finding the right balance starts with clearly assessing current practices at U.S. universities. While many universities were slow to appreciate the threat posed by China, that has changed. From what I have seen as co-chair of the congressionally mandated National Academies' Roundtable on Science, Technology, and Security, universities are now largely aware of the legitimate concerns about China, and they have put in place new procedures, still a work in progress, and many coordinate regularly with law enforcement.

MIT has been a leader in responding to the changing nature of China. MIT was the first university to cut ties with Huawei more than 6 years ago. We created a special review process for research collaborations with China in 2019 and issued a public report laying out our approach to China in 2022. At MIT, any proposed collaboration with China is reviewed for its potential impact on national security, economic security, and human rights.

We do not believe, though, that research collaborations should be cutoff entirely. Properly structured engagement can be beneficial to U.S. researchers. Collaboration is also a way to stay abreast of developments in China, which is now a leader in key fields. There are also still some areas like climate science, food safety, and certain areas of health where there is much to gain from joint work and little risk. This is all publishable basic research.

Research funding from China should, of course, be disclosed. Congress has usefully clarified and tightened disclosure requirements in recent years, and National Security Presidential Memorandum 33 (SPM 33), with input from both the Trump and the Biden Administrations, and from me, by the way, provides an effective framework for disclosing foreign collaborations.

Perhaps above all else, it has been a critical competitive advantage to the United States that we are able to attract the top scientific talent from around the world, including from China. The vast majority of Chinese Ph.D. students, more than 80 percent remain in the United States after getting their degrees, and more likely would if our policies were more supportive. Students pose a relatively low security risk since they work in an environment where research is published. Visa applicants should be more rigorously vetted, but I am not aware of evidence that students are extensively involved in illicit activities. If such information exists, I'd love to see it.

In my written testimony, I go into some detail on existing policies to protect U.S. technology, where they could be shored up, and where they should be left alone. But I'd like to close here with a broader point. Protective policies are needed, but they're not enough. We have to strengthen our own research enterprise. One need look no farther than the recent announcement by the China—Chinese AI firm DeepSeek to know that restrictions may buy us some time but they will not prevent Chinese technological advancement.

We must win this race by running faster, not just by trying to trip up the competition. We must continue to ensure that the United States is a magnet for the world's top talent by investing in U.S. science and technology and by offering reliable funding for competitively awarded research projects. That means taking steps like funding the National Science Foundation, as envisioned in the *CHIPS and Science Act* that this Committee helped draft on a bipartisan basis. Instead, we seem to be fighting about how much to slash its budget and personnel, including personnel hired to bolster research security.

We shouldn't be naïve about China, but that includes not denying its strengths. We're not going to compete successfully just by building a moat around the United States. We'd better be sure that everything we need from others, especially talent, can get across that moat, and we'd better be sure that nothing inside our moat is deteriorating.

Thank you, and I look forward to answering your questions.

[The prepared statement of Dr. Zuber follows:]

Maria T. Zuber
Written Testimony for House Committee on Science, Space and Technology
Subcommittee on Investigations and Oversight
March 5, 2025

Chairman McCormick, Ranking Member Sykes, Members of the Subcommittee,

Thank you for inviting me to testify on this vitally important topic. Striking the right balance in how the U.S. research enterprise interacts with China is critical to U.S. national security and competitiveness.

In my testimony, I will primarily be discussing academia, the part of the research ecosystem with which I am most familiar, and I will be speaking primarily in my role as the co-chair of the Congressionally created National Science, Technology and Security Roundtable at the National Academies, which recently completed its work. I will also be drawing on my experience at MIT, including my years as the vice president for research, and my service in the first Trump Administration as chair of the National Science Board, and in the Biden Administration as co-chair of the President's Council of Advisors on Science and Technology.

Let me begin with a few premises with which I imagine we can all agree. China's rapid rise presents a perhaps unprecedented challenge to the U.S., economically, geopolitically and militarily. And China's rise was facilitated by science and technology it obtained from other countries, especially the U.S., by licit and illicit means. China now is a science and technology powerhouse in many fields, but it still tries to build on its success by gathering information and skills from others, including illegally.

The question for the U.S. now is how best to compete successfully with China, given these premises. And that is a question that requires a clear-eyed assessment of when the U.S. can gain from interactions with China and when we are, to put it bluntly, being played for fools. But that assessment is not always easy to make.

Cutting all ties to China is likely to hobble the U.S. at least as much as it does China. Focusing exclusively on tripping up China is a less successful strategy than a combined approach that includes protection and also investing in enhancing the U.S. ability to win the race. There are additional steps that the government and universities could and should take to limit China's ability to take undue advantage of U.S. research, but we also need to strengthen U.S. science.

Before talking about what needs to be done, let me set the stage by describing the current situation. It is true that many universities and researchers were slow to appreciate the challenge posed by China and the way that nation was changing under President Xi. There were many reasons for this, but two primary ones were probably the sense that scientists have of science as an open, international effort to advance humankind, and the fact that for several decades U.S. policy under administrations and

congressional leadership of both political parties had encouraged increasing scientific cooperation with China. It also didn't help that the government often offered vague fears instead of specific information.

Academics are a data-driven community and not easily persuaded by vague descriptions of threats. The scientific culture is ironically opposite to that of law enforcement, which reveals as little as possible until a conviction is obtained. Bridging this cultural divide was one of the tasks of the Roundtable, and there has been real progress in this regard.

Today, universities have long since gotten the message that things have changed – China has changed; U.S. policy has changed; the needs of our nation have changed. Universities approach interactions with China with increased caution and scrutiny. Many universities have ongoing conversations with the FBI and other law enforcement, helping both. Does that mean there are never issues? Of course not. But I think we are past the point where there is any kind of systemic failure causing universities not to take questions about China seriously.

I can point to the way MIT has been handling China issues, and MIT is seen in the academic community as a leader in this arena that others often seek to follow. In 2018 – 2019, MIT was the first U.S. university to cut off research with Huawei, after I received information in a classified briefing. I then began talking to my counterparts in other universities about the threat (without providing the classified details), and they began to follow suit.

Also in that period, MIT instituted an elevated risk process, which is still in effect. Any proposed research or education cooperation with a Chinese entity goes through enhanced scrutiny, and the toughest calls go to the Senior Risk Group (SRG), composed of the Vice Provost for International Activities, the Vice President for Research, and the General Counsel. They are assisted by MIT's chief research security officer – who is a former assistant U.S. attorney with experience in national security investigations, staff from the General Counsel's office, and the head of our Washington Office. Though I stepped down as vice president for research, I continue to participate in my role as the MIT president's senior advisor on science and technology policy.

Over the past five years, SRG has approved projects, rejected projects, and modified quite a few – often by clarifying MIT's control over Intellectual Property Rights and our ability to exit any agreement. In recent years, the number of proposed research agreements with China has slowed to a trickle, in any event.

SRG examines each proposal considering its potential impact on U.S. national security and economic security, and on human rights. It also looks to ensure that the project provides real scientific benefits to MIT – and therefore to the U.S. We are long

past the point of assuming that any international cooperation inherently is a benefit to us, or that monetary benefit alone is sufficient to merit MIT taking on a specific research or educational collaboration. As I hope is clear, this review goes far beyond compliance with U.S. law, which is a starting point and a given.

The process has had broad support from our faculty from the outset, as they know they are not able to judge all the ramifications of work they might do with, or in China. Building on the elevated risk process, in November 2022, MIT released the report, "University Engagement with China: An MIT Approach," which continues to be MIT's guide and a model for schools in the U.S. and Europe.

The report, requested by then-President Rafael Reif, and written by a committee of experts from across the university, embraced a balanced approach. The report summarized its approach as "combin[ing] selective engagement with targeted risk assessment and management."

The report rejected a complete cut-off of research collaboration with China because there are fields where China is ahead – and a properly structured engagement could give us access to ideas, people and equipment that would help us – and because collaboration is also a way to stay abreast of developments in China. There are also areas, like climate science, food safety, and some areas of health where there is much to gain through international collaboration and little risk.

A complete cut-off of academic engagement in basic science and engineering is not necessary or desirable even now, though great care is needed in any collaboration. Academic collaboration produces openly publishable research that is several, and often many steps away from resulting in any product or process. Also, collaborations don't necessarily involve working together in the same lab, where know-how may be picked up from each other.

We can't ignore what we have to gain from such cooperation even though that needs to be balanced against the risks. Bills like the DETERRENT Act, which would effectively outlaw cooperation, go too far. (This is separate from the transparency provisions of that bill.)

It is essential that researchers and universities be transparent about any collaboration and about any money received from Chinese entities. Congress has rightly tightened the laws on disclosure and on foreign talent program participation over the last several years. Higher education groups and schools, including MIT, have helped Congress draft those provisions.

The Trump and Biden administrations, through National Security Presidential Memorandum (NSPM)-33, have also put in place disclosure requirements, while trying to streamline and standardize them across agencies. Individual agencies have also enhanced their apparatus for screening grant applications and have made their criteria

public. While there have been bumps in the road, this has all been movement in the right direction.

Violations of disclosure rules should be addressed and corrected, but unless there is evidence of malicious intent or illegal activity, criminal prosecution is the wrong way to deal with failures to disclose. The China Initiative picked up far too many innocent people in its dragnet, pushed excellent scientists away from federally funded work, and spurred discrimination.

For example, MIT's Gang Chen, a top mechanical engineer, was mired in China Initiative charges for a year that were ultimately dropped, and now he will not apply for any federal grants. The original charges included an accusation that he had hidden information about a collaboration with a Chinese university that MIT had actually publicly announced. (That research collaboration has since expired.)

So far, I have not mentioned Chinese students, but they may be the most important aspect of U.S. academic interaction with China. For decades, U.S. doctoral programs in the physical sciences and engineering have depended on Chinese students. Chinese post-docs in the life sciences are also a key part of the U.S. scientific workforce. It's frankly hard to imagine how the U.S. research enterprise would function at its preeminent level without international students and post-docs. This is not a matter of revenue; it's about getting the talented people we need to do the work.

While as a nation we obviously need to do much more to get U.S. students to go on to graduate degrees in these fields, the U.S. has benefited enormously from this influx of top talent. Even if we had all the domestic students we needed to fill graduate programs – and that will take years to do – we would still benefit from attracting to the U.S. top talent from around the world.

It's essential to point out that most of these international graduate students remain in the U.S. after their studies are completed – and more probably would if our policies did not seek to chase them away. It's long since time to pass legislation that would "staple a green card" to a STEM Ph.D.

The stay rates are remarkably high. A National Science Foundation study in 2021, found that 88 percent of students from China who had received a STEM Ph.D. five years earlier were still in the country, and 81 percent of students from China who had received a STEM Ph.D. 10 years earlier were still in the country. In the same study, NSF also found that almost 43 percent of individuals in the U.S. science and engineering workforce with Ph.D.s were foreign-born.

No one could argue that Chinese students present absolutely no risk to the U.S. Some students return home and bring the skills they gained in the U.S. Probably some engage in illegal activities, and they should be apprehended and deported. But there is

no question that by far the net beneficiary of having Chinese students in the U.S. has been, and is, the U.S.

Cutting off Chinese graduate students or discouraging them from coming (purposely or inadvertently) would be a colossal mistake that would cut the U.S. off from some of the world's best future scientists and engineers. Other nations are chomping at the bit to take advantage of such U.S. folly.

This is even truer because the risk is so low. Very few charges have been filed against Chinese grad students; they are the least risky Chinese entrants to the U.S. Obviously, the U.S. should vet all visa applicants from China closely, but there should not be a general goal of reducing U.S. access to talent.

Since the first Trump Administration, Presidential Proclamation 10043 has blocked visas for those who have worked on "civil military fusion." The criteria for that should be made public. The Chinese no doubt know who is being kept out, but U.S. institutions are left in the dark.

At MIT, we vet students and scholars from several countries that present heightened risk before a visa is ever applied for. If we had clearer information, we could save time and frustration for our research leaders and for the government by steering clear of individuals who pose risks.

There are some sensible limits that can be put on recruitment. For example, in its China report, MIT decided it would not take post-docs coming from any of the schools in China known as the "Seven Sons of National Defense." Not every individual connected with those schools is a security risk, but for that group of schools, the risks did seem to outweigh any benefits. Similarly, MIT will not appoint as post-docs or visiting researchers individuals who are known to be members of China's armed forces or otherwise currently employed by Chinese military and security institutions.

But vague, broad concerns about Chinese students are not warranted by the evidence I have seen. It is true that the Chinese government could go after the family of any Chinese student, but I am not aware of any evidence that this has resulted in any significant loss of scientific information from the U.S. What *is* mathematically demonstrable is the loss the U.S. would experience if it lost access to Chinese students.

So where do we go from here?

First, universities should continue to scrutinize any collaborations with China and should be in regular dialogue with law enforcement agencies, including the FBI and the Export Enforcement Office of the Bureau of Industry and Security at the Department of Commerce. This is more likely to happen if the massive improvements in university practices toward China are acknowledged by senior government officials. Many special agents on the ground seem to appreciate that there have been significant improvements

in their relationships with universities over the past several years. But that appreciation is not widely understood.

The government needs to continue to enhance its efforts to inform universities about real risks. Vague generalities do not help universities figure out what to do or build confidence in the seriousness of the issue. The more specific the government can be about threats – including by giving classified information to those with the appropriate clearances on campus – the better universities will be able to respond. MIT's action on Huawei mentioned above is an example of what is possible.

Within reason, lists of specific Chinese universities or entities to avoid are better than general descriptions, and easier to follow.

Government, and especially law enforcement, also needs to be more precise in talking about threats. Concerns about openly published research – more on that below – are very different from concerns about illicit activities, and they should not be treated as if they are the same thing.

The government also ought to acknowledge that academia is not the main problem when it comes to theft of technical information from the U.S. Industry – which, after all, keeps more things confidential and makes actual products – is a much bigger target for China. Academia gets a disproportionate amount of attention from those concerned about China because of universities' connections to the federal government and their openness. But the focus on academia is a little like the drunk looking for his keys under the streetlight because that's where he can see, even though he lost the keys elsewhere.

The government no doubt will continue to issue guidelines under NSPM-33, as it should. Universities have been waiting for a long time now to hear greater specifics regarding the kind of security plans they will need and how they are to certify to the adequacy of those plans. This is another area where specificity would be helpful. Schools have been taking actions in response to guidance that has come out under NSPM-33, for example, providing training modules on research security for faculty and other researchers, whether through models offered by the National Science Foundation SECURE Center, or by developing training more specifically tailored to their specific institution's profile, and by enhancing the tools for registering international travel.

There are some areas where government should think carefully before moving forward. For example, while open science has its risks, the U.S. has benefited enormously from the free flow of scientific information. U.S. agencies are supposed to follow National Security Decision Directive (NSDD) - 189, issued during the Reagan Administration, which says the default for fundamental research should be that it is open, and when it can't be, it should be classified.

Despite NSDD -189, publication restrictions and other limitations have proliferated in recent years. This should not be happening without a thoughtful examination of the impacts on science as well as on security. In 2019, the National Science Foundation commissioned a study from the JASON group – the independent advisory group put together by the Pentagon – that concluded that NSDD -189 should be reaffirmed. Perhaps a new look is needed, but prior studies should not be ignored. The recent tendency of some agencies to place "Confidential Unclassified Information" labels on research that is clearly both fundamental and basic is confusing and counterproductive; it makes it harder to effectively categorize information that truly does require confidential unclassified treatment. It also represents an additional compliance burden that is particularly problematic for small and not-well-resourced universities that are already challenged by the growing internal infrastructure needed to support STEM research.

Research agencies are also increasingly putting in place grant restrictions that limit the participation of Chinese students. In general, once a student has been admitted to the U.S., he or she should be treated as every other student is except when restricted by export controls or similar limitations. We want to fully benefit from these students, and we want them to stay after they complete their degrees.

There are sometimes good reasons to restrict foreign nationals from a project, and in those cases, restrictions should be used for specific studies of concern rather than blanket restrictions on programs for students with approved visas.

There is an area where additional information and restrictions may be needed. The government should increase its scrutiny of the funding of start-up companies. In start-ups developed with IP owned by a university, the university often has no way of knowing whether, say, a Chinese entity is an investor at the time of the start-up's creation, or at some later point. But such a start-up would not be subject to review by the Committee on Foreign Investment in the U.S. (CFIUS) because the IP would not be foreign owned.

But as I noted at the outset, all the defensive measures in the world are unlikely to do more than slow China's technological advance a bit, temporarily. China has substantial assets of its own to draw on. Slowing China – if done in ways that don't do greater harm to the U.S. – is worthwhile, but hardly enough to guarantee future U.S. success. The only way to do that is to ensure the U.S. is taking the steps needed to succeed.

Those steps include continuing to ensure that the U.S. is a magnet for the world's top talent, offering a stable economy that can take for granted the rule of law, and continuing to invest in U.S. science and technology.

This Committee, on a bipartisan basis, played a key role in crafting the "CHIPS and Science Act," which authorized significant increases for NSF, in part to promote U.S. competitiveness. And yet, Congress cut NSF's budget in FY 24 – a very rare step –

and funding is now frozen, while massive cuts are rumored for FY 26. We can limit China all we want, but we're never going to succeed if we limit ourselves more. China's own spending on science and technology is not being curtailed.

One need look no further than the recent announcement by DeepSeek, the Chinese AI company, to see the irrationality of assuming that defensive maneuvers alone are enough to guarantee U.S. success. Limits on exports of U.S. chips didn't keep DeepSeek from creating an AI system that is giving the U.S. competition a run for its money. And note that DeepSeek is open source – it is publishing its methods.

We shouldn't be naïve about China, but that includes not denying its strengths. We're not going to compete successfully just by building a moat around the U.S. We'd better be sure that everything we need from others – especially talent – can get across that moat, and we'd better be sure that nothing inside our moat is deteriorating.

Thank you. I look forward to answering your questions.

Maria T. Zuber
Presidential Advisor for Science and Technology Policy
E. A. Griswold Professor of Geophysics
Massachusetts Institute of Technology

Maria Zuber is MIT's E. A. Griswold Professor of Geophysics and presidential advisor for science and technology policy.

Zuber served as MIT's vice president for research from 2013 to 2024, responsible for research administration and policy, and oversight of more than a dozen interdisciplinary research laboratories and centers.

Zuber's research bridges planetary geophysics and the technology of space-based laser and radio systems. Since 1990, she has held leadership roles associated with a dozen scientific experiments or instrumentation on ten NASA missions, most notably serving as Principal Investigator of the Gravity Recovery and Interior Laboratory (GRAIL) mission.

Zuber holds a B.A. from the University of Pennsylvania and an Sc.M. and Ph.D. from Brown University. She is a member of the National Academy of Sciences, American Philosophical Society and a fellow of the American Academy of Arts and Sciences, the American Association for the Advancement of Science, the Geological Society of America, the Royal Astronomical Society and the American Geophysical Union.

Professor Zuber is the first woman to lead a science department at MIT and the first to lead a NASA planetary mission. In 2004, appointed by President George W. Bush, she served on the Presidential Commission on the Implementation of United States Space Exploration Policy. In 2002 Discover magazine named her one of the 50 most important women in science and, in 2008 she was named to the USNews/Harvard Kennedy School List of America's Best Leaders. In 2013, President Obama appointed her to the National Science Board, and in 2018 she was reappointed by President Trump and served as Board Chair during the first Trump administration. In 2021, then President-elect Biden named her as co-chair of the President's Council of Advisors on Science and Technology (PCAST).

Chairman MCCORMICK. Thank you to my witnesses for your opening remarks, and now I will recognize Representative Harrigan from North Carolina. Welcome to our Committee, and I look forward to your questions.

Mr. HARRIGAN. Thanks, Mr. Chairman, and thank you to all of our witnesses for your testimony today.

I wanted to talk about Chinese espionage in science and academia from the CSIS report and give you a couple examples here that will frame my question. In January 2020, a Harvard University professor and two Chinese nationals, Yanqing Ye and Zaosong Zheng, were indicted for attempted theft of biological research. Dr. Lieber was a participant in the Thousand Talents Plan, while actively accepting National Institutes of Health (NIH) and Department of Defense funding. Ye, a lieutenant of the PLA, compiled information on U.S. military projects for the CCP. Zheng committed the theft of 21 biological research vials to promote Chinese projects.

In July 2020, Saw-Teong Ang, a University of Arkansas professor, was indicted for wire fraud for his acceptance of U.S. contracting funds related to NASA and the Air Force while being simultaneously employed by Chinese entities.

In August 2020, Zhendong Cheng, a professor at Texas A&M, was charged with wire fraud for concealing his affiliation with Chinese universities and enterprises while accepting a NASA grant. His position allowed him access to sensitive NASA projects. He was also a participant of the Thousand Talents Plan.

I have only 5 minutes, so I cannot read the other countless examples of CCP infiltration into our national research apparatus, but my team compiled 58 different instances of various forms of research espionage that has occurred just in the last 6 years. So after reading this report and after listening to your testimony today, it is incredibly troubling, and I simply want to know one thing. Why do we still have any Chinese nationals inside of our research institutions, especially within institutions that participate in research that is critical to our national interests and our national security? Mr. Sargent?

Mr. SARGENT. I have no idea. I have no idea. I don't think it makes any sense at all. I think we need to be far more secure in who we allow into this country and who we allow to conduct research, especially on U.S. taxpayer-funded dollars. And I think it's very dangerous for us not to carefully vet all the people that are coming to the United States to study to make sure that they in fact are not linked to PLA institutions or universities.

And one thing we know for sure is that not only is China after our technology, they are constantly adapting and adopting new strategies to acquire it, so we can't think we have now, after 4 years of efforts, reached the pinnacle of security and put everything in place we need to do because the Chinese are going to adapt to it, and they're going to find ways around it. So we need to—as I say, you know, eternal vigilance is the price of liberty, and we've got to continue to remain vigilant. And, again, going back to the answer to your question, I don't think they should be.

Mr. HARRIGAN. Thank you. Mr. Stoff?

Mr. STOFF. Obviously, I think this is a very complex issue. I think that definitely—and I agree with Mr. Sargent that at least

within critical technology fields, within STEM fields, a far more rigorous process—and I talk about this in my testimony—that needs to be done that requires the kind of vetting and due diligence and assessments that have.

There may be other areas—like, from my perspective, any of the humanities and social sciences and other things, I—that's not a concern to me. The Chinese should come here and learn how our democratic governance systems work, our legal structures, things like that. So I think a complete and total ban doesn't—isn't necessarily—meet the objectives that you're seeking.

But I also want to point out something that I think is not really well understood, and that is the examples that you're describing relate primarily to these constructs of economic espionage, espionage, and intellectual property theft. And most of the problems and the threats that were occur—that's occurring on campus are none of those things. They're not illicit. And the scale and scope of the other ways in which they're acquiring technology and knowhow, is often not espionage, and that is completely underrepresented, not understood in the scale and the scope, and we need to be more diligent about that.

Mr. HARRIGAN. I have very limited time, so, Dr. Zuber, I don't know that we're going to get to you, but I think we've got to keep in mind here, we've got access, and we have placement with all of these individuals, and the CCP will exert leverage. That is a problem for our country. We need to deal with this, and we need to deal with it swiftly in our research institutions.

Mr. Chairman, I yield back.

Chairman MCCORMICK. The gentleman's time has expired.

With that, I recognize Ranking Member Sykes for her questions.

Mrs. SYKES. Thank you. Dr. Zuber, I am extremely concerned that the weakening of our scientific enterprise will lead to self-inflicted research security catastrophes. On Friday, CNN reported that the Naval Criminal Investigative Service has determined that China and Russia are attempting to recruit Federal employees who have been laid off. Scientists are specifically being targeted by Chinese institutions, as seen in advertisements to recruit researchers in institutes in China. I ask unanimous consent to enter the article and the advertisement into the record.

Chairman MCCORMICK. No objections.

Mrs. SYKES. Thank you, Mr. Chair.

And as the Trump Administration casts off scientists and destabilizes research in the name of efficiency, our adversaries celebrate and look to fill that vacuum. Dr. Zuber, can you please describe the relationship between funding our research enterprise and bolstering research security?

Dr. ZUBER. OK. Thank you for that question. So absolutely, I mean, the fundamental basis of my testimony was that we absolutely need compliance. We absolutely need to keep critical and sensitive research secure, agree with that, but we're not going to get there if we don't invest, OK? So last week, also in the first round of funding cuts, the NSF SECURE Center, which was noted in the Member statements, had five out of their nine employees laid off in the probationary. They may get one back, OK? So in a

very—area that we all consider high priority, they're laying off people.

So I mean, count me at the front of the line that the Federal bureaucracy could be more efficient and ought to be more efficient, but it ought to be done thoughtfully and strategically, and we ought to be thinking about what functions the Federal Government really ought to be executing and what functions should be done by others, and then we ought to identify the jobs and the employee talent that is needed to fill those roles.

Mrs. SYKES. Thank you, Dr. Zuber. And thank you for highlighting that in your testimony. And I do want to ask you all a question, and if you can answer it in maybe 15 words or less.

Yesterday, during the joint address to Congress, President Trump said, quote, "You should get rid of the *CHIPS Act.*" Your response to that in 15 words or less?

Mr. SARGENT. I would be happy to start. So I covered the *CHIPS Act* for the Congressional Research Service. I know it——

Mrs. SYKES. You're getting a little bit beyond your 15 words. We don't have the time.

Mr. SARGENT. I think we need to be very judicious in what we choose to accept and reject in the *CHIPS Act.*

Mrs. SYKES. Thank you. Mr. Stoff?

Mr. STOFF. I think it needs to be continued, and it's really important for our innovation and security.

Mrs. SYKES. Thank you. Dr. Zuber?

Dr. ZUBER. It needs to be continued, and there's $13 billion of R&D investment, and we have to train a new generation of chip makers in this country.

Mrs. SYKES. Thank you very much. We have heard rumors that DOGE has arrived at the National Science Foundation. This is extremely worrying under the guise of making government more efficient. I think we all have the idea to make government efficient and to curb waste, but as we've identified, some of this has been more of a wrecking ball rather than a scalpel.

When it comes to research security, that means that any information shared between Federal science agencies and universities could be ripe for—by hacking of our—by our adversaries, including China and Russia. Would you have concerns if the information at MIT, Dr. Zuber, has transmitted to NSF will transfer to nonsecure data servers, and what is the risk of research security-related information being accessed by unvetted DOGE representatives and potentially foreign adversaries?

Dr. ZUBER. OK. Well, what I will tell you is that at MIT, we don't do any classified research on campus. When technology gets to the point where it gets complex and concerning for either economic or national security, we send it to a classified area. So nothing on campus is classified. However, it is intellectual property, and if it were to get out, it would compromise the IP of the creators, and it could potentially give somebody maybe a 6-month to a year head start on something. But ultimately, everything we do on campus is unclassified, so it's going to get out there eventually.

Mrs. SYKES. And, Mr. Sargent, if you can do it in 10 seconds—not my rule, but the Committee's—do you have any concern about keeping this data private?

Mr. SARGENT. Of course I do.

Mrs. SYKES. Thank you, Mr. Chair. I yield back. Thank you for cooperating with me.

Chairman MCCORMICK. And obviously, 5 minutes is not much time. We'll do a second round of questioning if anybody's interested to stay on. It'll be rapid, but I just want to make sure that—she's being great, respectful. Thank you, Ranking Member, for staying in your time limit. We'll have a second round for people who want to ask additional questions.

With that, I recognize Chairman Babin for his questions.

Chairman BABIN. Thank you, Mr. Chairman. I appreciate it.

Mr. Stoff, why is it important for agencies to share information regarding research security threats to each other? Is there a better system that the Federal Government could adopt to analyze research security threats?

Mr. STOFF. Thank you for the question, Mr. Chairman. Yes, yes to all. There are—it is essential, both from a compliance, monitoring, enforcement, investigative function to have interagency share in ways that they're not really doing very much now because of different sharing rules, authorities, what have you. And this is a particular problem with academic research because a lot of the issues in the compliance or threats that are coming are often involving more than one Federal funding agency. You know, there are a lot of scientists that get money from NSF but also Department of Defense or NIH or others. And so it is really important that there has to be a much more centralized sort of structure where these can work in a more efficient way where data is shared.

Similarly, I think the U.S. Government needs to do a much better job at sharing not necessarily specific details, but the trends and patterns of behavior when they investigate a lot of these activities. And they, in my opinion, have not done a very good job, particularly law enforcement, explaining to academia, hey, there are all these things that are happening or behaviors, not all of which is illicit but compromises the integrity, the value system, the honesty that you depend on to conduct research and in a trusted fashion.

And we see that, and I've seen that. When I worked in government, I supported a lot of these investigations. Many of them never become an actual public record or an indictment or what have you. And so there's all this information that's not being adequately shared, so you need to have both. And having a centralized structure—in my written testimony, I talk about basically building a national center. A crude analogy would be an NCTC (National Counterterrorism Center).

Chairman BABIN. OK. Thank you very much. And Mr. Sargent, under the first Trump Administration, OSTP established an interagency working group on research security under the Joint Committee on Research Environments (JCORE). Under the Biden Administration, this effort was discontinued. Could you describe the purpose and the role of JCORE Subcommittee on Research Security to coordinate activities for identifying and addressing threats to our academic research enterprise?

Mr. SARGENT. Honestly, that's not an area of my expertise. However, I will just say that, having had extensive experience with the

National Science and Technology Council, of which JCORE is a part of, that the purpose of these interagency activities is the sharing of information, the coordination of best practices, so I imagine that's what they were doing in the context of our research security.

Chairman BABIN. Right. OK. Thank you. And then finally, Dr. Zuber, what resources are available to universities for assessment, identification, and analysis of research security threats, and how are these tools informing and promoting information sharing of risks among universities?

Dr. ZUBER. OK. There's a—senior research officers of the research universities coordinate information. The presidents coordinate information. The NSF SECURE Center, DARPA (Defense Advanced Research Projects Agency) has put out guidance, and the NIH had put out guidance, and the DOE (Department of Energy) had put out guidance. But it's—in many cases, it's vague. And National Security Presidential Memorandum 33 was meant to standardize a lot of the reporting across and the implementation, which is underway but still not finally there. So if it were done properly, that would theoretically take care of all of the compliance that is—the lack of compliance that's accidental, OK, where people thought they reported something, but they reported it there, not here, OK? It would not take care of somebody who truly wants to do something wrong, OK? And those are actually difficult to root out.

But the—you know, we're still—despite two Presidential Administrations that have gone over and SPM 33, the guidance is still sufficiently vague that, you know, universities are supposed to put a research integrity plan in place, but they don't tell us what the plan should constitute and how a university can certify that it's actually meeting those criteria that it has to.

Chairman BABIN. Thank you. I see the others nodding their heads. Would you like to add into that as well?

Mr. STOFF. No, I just—I strongly agree with Dr. Zuber that a lack of clarity, a lack of guidance, a lack of granular sort of level, what is it that we need to do, what are the tools, infrastructures that need to be placed? The SECURE Center may be able to start addressing those issues, but this has been going on, as Dr. Zuber said, for multiple Administrations, and there's still a lot of work that needs to be done, and I don't think we have the time to kind of do this as slow rolling as we have.

Chairman BABIN. Yes. And I'm out of time, Mr. Chairman. I'm sorry, so I yield back, unless you'll——

Chairman MCCORMICK. Thank you, Mr. Chair. We will have a second round for anybody who wants to participate. I just want to keep this on track if you don't mind, sir.

Chairman MCCORMICK. With that, we recognize Ranking Member Lofgren for questions.

Ms. LOFGREN. Thank you, Mr. Chairman.

And I see a lot of agreement among our witnesses. We do need clear standards, we need clarity, we need adherence, we need to protect our country. I think there's bipartisan agreement on those things. But as Ranking Member Sykes mentioned in her statement, there is an unconfirmed report that DOGE has arrived at NSF. Now, reportedly, one of the Musk hackers setting up shop at headquarters is Edward Coristine. Coristine is better known in his var-

ious online communities by the moniker "Big Balls." Now, this 19-year-old is allegedly gaining access to NSF data systems. I'll try and be brief when I go through the laundry list of reasons why I believe this teenager is unfit to serve in government.

I am advised that Mr. Big Balls started a company called Tesla.Sexy LLC, a site that allowed users to share images confidentially. The URLs (Uniform Resource Locators) created redirected images hosted on his website and apparently included references to the sale of child sexual abuse material, among other really horrible topics. It's reported that in 2022 he was fired from an internship after leaking confidential business information to competitors. He bragged about this online, boasting that he had access to every single machine. It's reported that he also participated in chatrooms with U.S. law enforcement that have monitored his cybercrimes, investigating cybercrimes. And now, apparently, he has access to government data systems, most recently, allegedly, NSF.

NSF hosts personally identifiable information of employees, principal investigators, confidential business information, trade secrets when relevant to project proposals and controlled unclassified information related to law enforcement, sensitive information.

Dr. Zuber, you have plenty of 19-year-olds working at MIT labs. If an MIT student admitted to stealing data from a lab in order to share it with people not authorized to access it, do you have disciplinary procedures that would prevent that student from ever accessing sensitive information again?

Dr. ZUBER. Well, so all this is alleged. I——

Ms. LOFGREN. Correct.

Dr. ZUBER. I can't vouch for it. But we do have disciplinary procedures. It's actually potentially a research integrity violation, and we have—you know, there are very clear rules for how to deal with research integrity. And when there is a finding, there are consequences.

Ms. LOFGREN. Let me just say, as a hypothetical because these have been reported. Obviously, we haven't done an independent investigation. But if someone with the alleged background that I've just outlined had access to sensitive information at U.S. research agencies, would that be a cause for concern?

Dr. ZUBER. Well, even if there were no research involved, if there was access to personally identifiable information of, you know, any member of our community or any community, that would clearly be a great concern.

Ms. LOFGREN. Mr. Sargent, you're an expert on our science and technology enterprise, and you feel strongly that certain information must be stringently protected, and I agree with you. What do you think about allowing an individual access to our science agencies' controlled unclassified information if that individual had a history of sharing confidential business information with competitors, or if that person had been known to host images with titles alluding to child sexual abuse, or if that person participated in forms monitored by law enforcement during cybercrimes investigations? If that were the background, would that cause concern?

Mr. SARGENT. Absolutely.

Ms. LOFGREN. Well, I would just like to say, Mr. Chairman, that while we are of one mind that we must protect ourselves from

threats from those abroad, we ought to be alert to the threat that is being posed by this army of teenage and 20-something hackers that have invaded our government, that are accessing our private information, and including our science information, including individuals such as Mr. Big Balls, who is now apparently rooting through the NSF data base.

And with that, Mr. Chairman, I yield back.

Chairman MCCORMICK. Thank you, Ranking Member. Just to clarify as Chair, just to make sure we're on the same page, my Committee staff has just been officially told that no one from DOGE has entered the NSF. That's official. Eighty-four of 86 probationary employees at NSF have been reinstated. No grants at the National Science Foundation have been canceled. There is no funding freeze. All those things are now official.

Since January 20, nearly 500 awards have gone out, and more than 200 panels have taken place. I just want to make sure that we're clarifying the details since we're getting real-time information, just don't want to confuse or confound any real information. And I'm not trying to make this partisan. I just want to make sure it's factual. Thank you.

With that, I recognize myself for 5 minutes of questions.

Mr. Sargent, this is somewhat of a rhetorical question, but are American graduate students any less intelligent or qualified than Chinese graduate students?

Mr. SARGENT. I always forget that. Mr. Chairman, I love rhetorical questions.

Chairman MCCORMICK. It's a yes or no question, sir.

Mr. SARGENT. American students are as capable as Chinese students, or more so.

Chairman MCCORMICK. Of course. And I wouldn't want to be the person who said they weren't. But then, why do you think that certain universities insist on hiring Chinese graduate students when there are plenty of American students available? Literally, up to 50 percent of all graduate students hired are from foreign areas, that go back to foreign areas. Why do we keep doing that?

Mr. SARGENT. Well, a good question. Part of it is momentum. A good deal of universities' prestige is the ability to attract the best international students, and it allows for these connections and relationships to be made back to the home countries of these students. And so by continuing to recruit them and allowing them to, you know, be a part of our university education system, they develop these relationships, and these relationships go on long beyond the time that those students are there because those students then matriculate out, and they go into other positions in academia, they go into industry, and those ties allow that university to benefit from that relationship.

Chairman MCCORMICK. So there's probably a financial incentive of some kind because, otherwise, it doesn't really make sense, right? A lot of that talent goes back to their foreign national lands, and then a lot of talents goes out into the community, but they're not really citizens unless they so—go down that path.

Mr. SARGENT. It's almost always follow the money.

Chairman MCCORMICK. Very good. Putting research security aside, what is the long-term impact of U.S. students if universities

continue to fill graduate posts with foreign nationals? In other words, we're not filling it with Americans. What is the long-term impact?

Mr. SARGENT. Well, it's been self-fulfilling. You know, if you continue to bring foreign students in because they're the best, those spots are not available for excellent U.S. students to go and become Ph.D.'s and themselves become principal investigators. And so then you find yourself in the position of not having Americans to fill these positions, and so it's a self-fulfilling behavior.

Chairman MCCORMICK. And I just want to highlight this. In a university system that's ranked not even in the top 30 in the world, the United States, which puts more money into education than any other country by far, and yet we're spending half of the research dollars—half of the money that we spend to develop instructors goes to foreign nationals here in the United States. We are basically cutting off the head of our future teachers, researchers, innovators, and we're going to fall further behind. If we're not even the top 30 and we're falling further behind, why would we train other countries to subvert our education system? I don't understand.

Dr. Zuber, one of the things I noticed is that we have a lot of money from endowments. Even MIT does. I don't know why, but, you know, they happen to have a lot of pride in their university. Do you think that that's what they intend? When we give U.S. dollars, taxpayers say, hey, you know what? I'm going to give you a lot of money to develop—and I think U.S. students is what most people think. When they give—when U.S. citizens give money to an endowment, they want to see a university develop U.S. talent. And we give money to see U.S. talent develop. Why are we bringing in so many people from other countries when you—literally up to 50 percent of the people? Why do you think that is?

Dr. ZUBER. Yes, Mr. Chairman, thank you for that question. So MIT is 97 percent STEM students, OK, and we accept all the top U.S. students that apply. And let me tell you, when we have a FIRST Robotics Competition for middle school students in the United States, we fill up high school gyms. When the Chinese hold first robotic competitions, they fill up stadiums, OK? So it's a question of students going into STEM, OK?

Then, interesting question—or interesting statistic, U.S. students who graduate, OK, with STEM fields, only 1/3 of them go into STEM careers. So they're——

Chairman MCCORMICK. I would make the case that part of that is because of the way we influence our students to begin with. If you look at even the way that TikTok was used here in America, a Chinese-controlled TikTok, by the way, they want to develop influencers in America instead of scientists, whereas it's used in China on a limited basis to develop people to get into science. This is a systemic problem in the education system. And we are in a competition with these folks that are—we are literally educating and bringing in talent, but we're then divesting from that in the way that we're giving up that talent. And I think it's a very dangerous precedent.

I'm going to go ahead and yield because I'm out of time, and I want to stay on and not be a hypocrite.

With that, Ms. Bomici out of Oregon—Bonamici, sorry, out of Oregon, my hometown, is recognized.

Ms. BONAMICI. Thank you, Mr. Chairman. I know you have some Oregon Connections. And thank you to the Ranking Member. Thank you to the witnesses for your expertise and being here today. I want to join the Ranking Member Sykes in sending deepest condolences to the family of Representative Turner. He will be missed.

So this hearing, Mr. Chairman, you talked about—I didn't have a chance to fact-check your numbers and facts about the NSF, but I do know that they have laid off many people. Even though they may be trying to bring some of them back, they're still facing significant budget cuts, as are most agencies, and the disruption and chaos has been really concerning.

This hearing is titled "Assessing the Threat to U.S. Funded Research," and it is indeed an important topic, but threats to American research and research security do not only come from foreign actors. They also come from the reckless actions of this Administration that are destabilizing our scientific enterprise and purging Federal scientists at NOAA (National Oceanic and Atmospheric Administration), at NSF, at NIST (National Institute of Standards and Technology), at DOE. And Ranking Member Sykes mentioned that intelligence is already showing that China and Russia are eager to exploit that by trying to recruit some of our scientists, particularly scientists with national security experience.

And I want to note as well, and to follow up to Ranking Member Lofgren's comments that—about DOGE, the Trump Administration sent via an unsecure email server the names of CIA (Central Intelligence Agency) employees, which is incredibly dangerous. You might have seen that there—they seem to be pretty good at hacking in but not in protecting data bases. And I'm sure everyone saw the takeover of the screens at HUD (Housing and Urban Development). They couldn't even figure out how to get the images off the screen. They had to go unplug the televisions. So, I mean, my point is, what are these people doing that—is creating a lot of instability, insecurity, and uncertainty about the safety of our data and research.

So instead of strengthening our defenses, the Administration seems to be gutting key research agencies, as I mentioned, and purging experienced scientists, sending a chilling message to researchers that their work might be under constant suspicion.

The so-called China Initiative that was implemented during the first Trump Administration as an example of mismanagement and certainly some racial profiling, it disproportionately targeted scientists of Chinese descent, drove talent away, and ultimately did more harm than good. The Brennan Center for Justice rightly called it a failure, warning against reviving such misguided efforts. And meanwhile, as our institutions are struggling with frozen grants and reduced indirect cost support and uncertainty about whether international collaboration will be discouraged or even criminalized, other nations, especially China, as I mentioned, have seized on the opportunity.

So the United States cannot afford to keep making these mistakes. Our science enterprise thrives on openness, collaboration,

and stability, not on paranoia and politically driven purges. So we need a serious evidence-based discussion. We all take this seriously. I want to ask you, Dr. Zuber, because I know you've been at MIT for a while. and we think back to the China Initiative from the first Trump Administration. Assuming that there's going to be something similar, what would you change and what would you keep the same?

Dr. ZUBER. Well, I think, actually, Mr. Stoff touched on it, I think in his—both in his remarks and in more detail in his testimony. But the—I mean, the China Initiative initially focused on espionage, and they started with industry, and then they moved to universities. And there was very, very little espionage in universities. The kinds of indiscretions within universities are transmission of information that will be published anyway, but it doesn't rise to the level of espionage. And so these should be adjudicated by agencies, you know, if you're caught——

Ms. BONAMICI. And you talk about the balance that's needed.

Dr. ZUBER. If you're caught, you lose funding for 5 years, and that will take care of that problem. And, in fact, there was a report by the JASONs that put out—that said this sort of thing should be treated as a research integrity violation, which is——

Ms. BONAMICI. Thank you. And in my remaining half a minute, Mr. Stoff, you advocated basically for cutting ties with Chinese researchers, but would shutting out top-tier talent like an AI or quantum computing limit our potential?

Mr. STOFF. Well, I don't necessarily agree that we completely cut everything off, but we're not even cutting off—we're not even restricting the most high-risk collaborations or people. We're still letting them in. We're still collaborating with defense and weapons programs and state-owned enterprises in China. So can we start with that? And I would say we need to start restricting that, and then we can be more nuanced.

Ms. BONAMICI. Appreciate that. My time is expired. I yield back. Thank you, Mr. Chairman.

Chairman MCCORMICK. Thank you. And with that, we recognize Representative Begich from Alaska.

Mr. BEGICH. Thank you, Chairman. First question for Mr. Stoff. China has labeled itself a near-Arctic State and has invested in Arctic research collaborations with U.S. institutions. Have Chinese-linked researchers or institutions attempted to establish partnerships with Alaska-based Arctic research programs.

Mr. STOFF. Thank you for the question. Unfortunately, I have no knowledge or expertise in the area with regards to Alaska, but I can quickly say that China has aggressively done this with other polar nations like Norway, for example, where their largest state-owned defense conglomerate that builds radar systems and communication systems for the PLA established ground stations for Norway under the guise of scientific purposes. And this is happening, I believe, elsewhere. I don't know if it's happening in Alaska, but they have a practice of doing this, and it's a big problem because they're actually developing more advanced radar systems as a result.

Mr. BEGICH. Thank you. And given that Arctic focus, are you aware of any efforts that the Chinese have made with respect to Greenland as well?

Mr. STOFF. No, not personally. That hasn't—I haven't looked into it, but I would be surprised if they were not pursuing those regions because of their strategic import that they represent.

Mr. BEGICH. Let me ask you this. Given that Alaska hosts key U.S. Coast Guard operations and Arctic maritime research, are you aware of any instances in which foreign adversaries have attempted to infiltrate federally funded programs tied to maritime security?

Mr. STOFF. Yes, that's actually fairly extensive, but we don't get—we don't have a good handle on it. We do know that a number of civilian PRC defense institutions that are heavily involved in PLA, navy, submarine, underwater warfare, underwater weaponry, systems, communications, et cetera, collaborate extensively almost without any sort of restriction with most U.S. universities, some of which even involve Department of Defense funding. Because it's in a fundamental research area, as I mentioned earlier, there's really no regulatory oversight over it.

Mr. BEGICH. Do you believe that the Coast Guard should be given additional resources to protect research collaborations involving Arctic defense infrastructure?

Mr. STOFF. Possibly, but I do think a better approach is what I mentioned my testimony is if you have a centralized government entity that kind of does this for all Federal agencies, it would be far more efficient and effective.

Mr. BEGICH. Thank you. And an additional question for Mr. Sargent. Do you believe that Congress should require enhanced security screening for federally funded researchers in critical areas such as Arctic security, Arctic energy, or climate studies?

Mr. SARGENT. For U.S. researchers?

Mr. BEGICH. Yes, or any additional researchers that may be coming from an—from a place outside the United States but are working with U.S. researchers?

Mr. SARGENT. Yes, absolutely. I think any area that has potential national security implications, we need to make sure that the people who are working on them don't have any ties that make them of—question their loyalty to the United States.

Mr. BEGICH. So you don't believe the current screening practices are sufficient in order to address the security concerns that we have.

Mr. SARGENT. I can't speak to the adequacy of the current security screenings.

Mr. BEGICH. OK. Thank you. Do you know whether—again, to Mr. Sargent. Do you know whether Federal agencies have conducted comprehensive research security audits of institutions in the Arctic which engage in Arctic science, climate research, or strategic defense studies? Do you know if that's happening?

Mr. SARGENT. I don't know anything of that nature, no.

Mr. BEGICH. OK. Thank you. With that, I yield back.

Chairman MCCORMICK. And now Representative Rivas from California is recognized for 5 minutes.

Ms. RIVAS. Thank you, Chairman McCormick and Ranking Member Sykes.

First, I join my colleagues in expressing condolences to the family of my fellow freshman colleague, Sylvester Turner. He will be missed by all of us.

I'd like to start by taking a moment of personal privilege and thank Dr. Zuber for appearing before the Subcommittee today. As an MIT alum myself, it gives me great pride to see an MIT Professor discussing the importance and the challenges facing the scientific community and the research ecosystem.

Over the last 7 weeks, we have seen a complete disruption and attack to one of America's pillars for the future, our scientific and academic community. Our research ecosystem depends on a steady stream of educated experts. As co-chair of the bipartisan STEM Education Caucus, I take great pride in America's leadership to produce the next generation of researchers and scientists of the future. The future will only come from early and continued STEM investments in every ZIP code in America. I have spent most of my career engaging and preparing students, American students, to get into STEM fields. It's our responsibility to provide the current and future workforce with the tools to innovate and create technological solutions and emerging and essential technologies and industries like AI, healthcare, and the environment.

However, a major threat to U.S.-funded research is this Administration's reckless actions that include layoffs of about 800 employees at NOAA, up to 2,000 employees at the Department of Energy, and more than 150 employees at the National Science Foundation. Despite those dizzying acts against our Nation's science corps, one of the most worrying cuts has been the NIH policy, capping indirect cost at 15 percent. I worry about the capacity of smaller institutions to keep up, and that concern has only grown in recent weeks, as I hear from constituents and organizations serving my district. Indirect costs are expenditures that aren't tied directly to research staffing or supplies, but they nonetheless support infrastructure and activities that are vital to the function of research institutions.

The reality is that this is a drastic reduction in reimbursement that will result in more than 800 million in cuts for my home State of California. This will devastate the development of lifesaving research, inhibit patient access to groundbreaking treatments and clinical trials, and will cede American dominance in biomedical research to our foreign competitors like China, Russia, and Iran for years to come.

Dr. Zuber, I've joined my colleagues in two letters to the acting NIH Director, expressing my deep concerns on these NIH cuts and how they will impact my State and district. Can you elaborate on how these cuts will impact research universities' ability to compete and how you anticipate smaller institutions will be impacted?

Dr. ZUBER. OK. Thank you very much. A lot of thoughts there, and thank you for raising the indirect cost because people don't understand indirect costs, OK? It's—whether a cost is a direct cost or an indirect cost, that's determined by uniform guidance. Both are the costs of doing research. You could put it in one column, or you could put it in the other column, but that's what it costs, OK? If we don't get the indirect cost reimbursement, the larger schools

that have endowments have to use their endowments to cover that. And at MIT, we already—I won't say subsidize; I will say coinvest in research 100 percent, OK? So we—our research volume, we put in an equal amount from our endowment to kind of double the impact from the Federal and other funding that we receive.

Schools with—either smaller schools or R1 research institutions with small endowments, especially those with medical centers, don't have any funds to draw on, OK? So we would do less research, OK, so less impact in the world. And MIT grads have started, as you know, tens of thousands of companies, OK? But it—for schools without endowments and have medical schools, they're going to be out of business, OK? And these are economic drivers in their areas and educational—important educational institutions producing the workforce for tomorrow. So the impacts are potentially huge.

Ms. RIVAS. Thank you. With that, I yield back.

Chairman MCCORMICK. Thank you. And next, we recognize Representative McClain Delaney from Maryland for 5 minutes.

Mrs. MCCLAIN DELANEY. So I thank the panelists and our Ranking Members for convening this important hearing. Can you hear me? Hi. Hello. So thank—I thank the panelists and our Ranking Members for convening this important hearing, striking the right balance between cyber and research vis-à-vis China and Russia with respect to our research universities. And I really appreciated Dr. Zuber's comments how there are legitimate concerns with respect to China with—and research, but how we cannot, you know, throw the, you know, baby out with the bath water, and we really need to not cutoff entirely and really preserve some of this for U.S. competitiveness.

I represent the 6th District of Maryland, and in my district is NIST, parts of NIH, the National Institutes of Cancer, Fort Detrick, which deals with some of our pathogens, you know, our fire academy, and our nearby—my—next door is NOAA, of course, so research and innovation through these incredible agencies. And the hiring freezes by Rep. Bonamici is really important that we drive—continue to understand how these freezes and cuts will really undercut both our cybersecurity and other institutions.

But building on some of the—two questions I have because I have only limited time. In terms of under-resourced universities—and building on Rep. Rivas' questions concerning indirect costs, I ask the panel, but Dr. Zuber first, do indirect costs contribute to universities' compliance with laws, including those related to research security? And do you believe that universities should be able to classify research security support as a direct cost so to ensure the protection of sensitive research and data?

Dr. ZUBER. OK. So I don't know all the details, but I can tell you that indirect costs, part of it is facilities—the larger part of it is facilities and taking care of the buildings that you wouldn't have unless you were doing research in them, OK? And then the other part is administrative costs. And those administrative costs, you know, the compliance has been going through the roof for years and years and years. And it—you know, more rules come in, and no rules ever seem to go away, and so you need staff to be able to handle that.

The recent focus on research security has caused a big increase. We've had to hire a lot more people to do compliance. And most universities in the indirect cost system are out—already maxed out in the administrative part, so, obviously, if you could—you know, it doesn't matter to me if they're direct costed or indirect costed, but all this has got to be paid for.

Mrs. MCCLAIN DELANEY. Yes. Well, our research institutions are our Nation's jewels and why we are where we are in America, and so just making sure that we are able to protect that information and those collaborations.

I want to move on to cybersecurity. I worked at the Biden Administration as Deputy Secretary at NTIA (National Telecommunications and Information Administration) and actually worked on a lot of cyber national security issues vis-à-vis some of—even Huawei and 5G and AI. But just this week, following orders from Defense Secretary—our Defense Secretary, DOD's U.S. cyber command suspended operations and planning for offensive cyber operations against Russia. And we're—weakening our cybersecurity posture with Russia will hurt our national security and make us more vulnerable.

Research conversations have largely revolved around a threat posed by China, but we cannot forget Russia as a serious threat. I guess I ask all of you, can—well, Dr. Sargent, what potential is there for harm if the Trump Administration continues to weaken our offensive cyber operations against foreign adversaries? And to the panel, can the Federal Government play a role in bolstering the cybersecurity defenses of our universities against threats from foreign adversaries?

Mr. SARGENT. Thank you for the question. First of all, let me correct you on one thing. I have not earned my Ph.D. I am a—just a mainstream engineer, systems engineer from the University of Virginia. But—and, by the way, let me say, with NIST in your district, I am a massive fan of NIST. I think they're an outstanding——

Mrs. MCCLAIN DELANEY. We are too.

Mr. SARGENT [continuing]. Institution with great civil servant employees who do a fantastic job in a wide range of areas.

With respect to cybersecurity, I don't think you can begin to overstate its importance. And the risk that we face from both China and Russia to our—every system in the United States, including our water systems, our power systems, our transportation systems, all of them are at risk. And China is—I'm told, I don't have any inside information, but I am told, and I have read that they are dropping all kinds of malware in our systems so that if we find ourselves in conflict with them, they can flip a switch and cause a lot of internal damage in the United States. So I don't think you can overestimate the importance of cybersecurity.

Mrs. MCCLAIN DELANEY. Thank you. Any other comments if I have time?

Chairman MCCORMICK. The Member's time has expired, but thank you very much.

And with that, I'm going to go and give closing remarks. First of all, thank you all for being here today. It's an honor. I know it's at your own expense, and I know that sometimes it's thankless, but

we want to thank you for being here today. I thank Ranking Member Sykes for being here and being a joy to work with.

I want to address a couple things that were brought up during the hearing. Obviously, we talked about NSF funding or—and also staffing. We understand that DOGE is going to make some mistakes along the way. I get it. They're being very aggressive, and they've admitted that they're going to make mistakes.

I want to address the issue of age. Some people say age is a concern for DOGE, those members who are—or those people who are actually doing the hard work and labor, realizing that Einstein, I believe, was, what, 26 years old when he published the theory of relativity, that you have—Zuckerberg invented Facebook at the age of 19, that we have 17-, 18-, 19-year-olds in school right now coming up with brilliant theories on the next evolution of science, that my great uncle was, I think, about 26 years old when he was a division commander as a B–17 pilot and was shot down in the greatest air war of all time and became one of the senior officers in Stalag III.

Age is not really the consideration when we talk about people who are going to create and sacrifice in this next generation. Matter of fact, we should be asking people to step in earlier. Matter of fact, coddling our kids certainly doesn't help them do what we need them to do for this next generation of competition.

And I think the only numbers that we talk about when—it's not about age, but it's about the numbers we need to say because our government is far too invested in waste, fraud, and abuse. and we have a $36 trillion deficit right now. The interest payments alone on the debt that we have incurred exceed not only the military investment we do per year, but also the research we do. If we don't do something to trim the waste, we won't have the amount of money we need to invest in the future generations of America.

And I think this hearing is really all about protecting our investments, the money we spend on education to develop the next generation of science and technologies. When you talk about the most transformational technologies that this generation has ever seen, in AI, in quantum, in other technologies, they're going to literally change the face—the way that we employ, the way we explore, the way we create jobs, and how we fight the next war. We're on the frontline. You are on the frontline.

And we need to make sure that our peers aren't getting advantages from our hard work and our investments. And I think that's what this entire Committee hearing has been about, and I hope we continue this dialog because if we don't—if we're not careful about what we do, it will result in some catastrophic results.

God bless you. Thank you for being here. Thank you for participating. And with that, we are adjourned.

[Whereupon, at 11:30 a.m., the Subcommittee was adjourned.]

Appendix I

Answers to Post-Hearing Questions

ANSWERS TO POST-HEARING QUESTIONS

Responses by Mr. John F. Sargent Jr.

U.S. HOUSE OF REPRESENTATIVES COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

Subcommittee on Investigations and Oversight
Assessing the Threat to U.S. Funded Research

Mr. John F. Sargent Jr., Retired, Specialist in Science and Technology Policy,
Congressional Research Service

Questions submitted by Chairman Rich McCormick, Committee on Science, Space, and Technology

Thank you for the excellent questions you have posed to me in following up to my testimony at the subcommittee's hearing "Assessing the Threat to U.S. Funded Research," which was focused in large measure on the threat posed by the People's Republic of China (PRC) and organizations and individuals working on its behalf.

While the questions you pose to me are directed primarily toward the illicit or illegal acquisition of research and are important, a larger concern I would like to address in advance of my responses to these questions is the threat posed to the United States by the acquisition of leading-edge university scientific and technological knowledge, across a range of disciplines, through perfectly legal means.

The United States university research system leaks like a sieve, with information pouring out to China and other nefarious actors. This is, in part, by design. The university system in the United States is built in large measure to create and share new knowledge, not to control access to it. Research universities, generally, see their mission as pushing back the frontiers of scientific knowledge in virtually every field of science, with new disciplinary fields emerging regularly at the interstitial boundaries between existing fields. University researchers operate on a "publish or perish" basis, which is to say, to earn your doctorate, tenure, and professional recognition you must publish your research in scientific journals and related publications. Some efforts are made by universities to restrict access to these results (for example, by not disclosing information on proprietary equipment (and processes) built uniquely by the lab to facilitate its research). However, when Chinese students, who are under a national mandate to report their work back to the PRC are participating in the research, these are hardly effective methods for controlling the knowledge.

Perhaps as importantly, research universities are not adjunct arms of the federal government's national security apparatus. That is to say, it is not their mission to protect American national security or economic security, and they are not, generally, experts at doing so, either in knowing what may be a risk to disclose or being experts in controlling such risks.

A portion of university research is at the very leading-edge of new fields for which little is known of their potential applications and ultimate utility. Whereas in some established fields risks have been identified and control mechanisms put in place by the federal government (e.g., nuclear weapons-related technology), many fields that universities are working in are emergent, and no laws have been put in place to control the knowledge. And with new fields emerging

regularly from ongoing research—perhaps at an unprecedented rate driven by record level global research and development spending—controlling the knowledge is similar to a game of whack-a-mole, with new potential threats popping up all the time.

In summary, protecting new knowledge is generally not the job of universities, sharing it is; universities have little expertise in knowing what should be protected and few tools and resources to do so; new fields of science and technology are emerging regularly, many with national and economic security implications, making it difficult to establish controls at the speed of discovery; and many universities have Chinese nationals working in their laboratories, some of whom are agents of the Chinese Communist Party (CCP), which increases the likelihood of knowledge transfer to China. (Notably, China's National Intelligence Law makes "everyone responsible for state security," and thus makes all Chinese nationals working in university laboratories responsible for reporting developments with national security implications to the CCP. See Article 7 of the law, among other provisions: "All organizations and citizens shall support, assist, and cooperate with national intelligence efforts in accordance with law.")

Also, very importantly, having access to a treasure trove of open, seemingly innocuous, scientific and engineering knowledge is likely to be increasingly important in the age of artificial intelligence (AI). AI is capable of quickly combing through vast amounts of information and data to identify what is important and what may be able to be linked to each other to synthesize new and unexpected insights. Recall the story of John Aristotle Phillips (known in the media as "The A-Bomb Kid") who, as an undergraduate physics major at Princeton, cobbled together open-source information from a variety of sources to create a plausible plan for a nuclear weapon. This accomplishment was by a single student, working with a faculty advisor but with no access to classified information, who was able to put together a plausible plan for a nuclear device. Imagine what a leading-edge AI program, working across multiple scientific and engineering disciplines, using an array of increasingly powerful supercomputers, working with the entire library of openly published human scientific and engineering knowledge, might be able to "cobble together." In general, with AI, the more data you have and the more powerful your computing power, the more capable the AI program becomes. This argues for limiting Chinese access to U.S. scientific and engineering information, as well as to advanced AI programs and computer chips. Ultimately, it may be impossible to prevent access to such information, but the more barriers that the United States can erect to the PRC's acquisition of this knowledge, the longer it will take for them to put it to use against the United States.

U.S. HOUSE OF REPRESENTATIVES COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

Subcommittee on Investigations and Oversight
Assessing the Threat to U.S. Funded Research

Mr. John F. Sargent Jr., Retired, Specialist in Science and Technology Policy,
Congressional Research Service

My answers to the following answers to your Questions for the Record are based on my knowledge and experience, and what I found in my research of the public record, to which countless people and organizations have contributed.

Also, I believe that the Congressional Research Service (CRS) has done much outstanding work in this area and is a resource that Members of Congress and congressional committees should heavily rely upon as it continues its efforts in deterring the PRC military, intelligence, and industries from acquiring and benefitting from American research funding and activities.

1. Each panel member expressed concerns with respect to the risks associated with foreign influence in university research. What are the key pieces of information that universities are currently lacking that would enable them to conduct more thorough and effective risk assessments?

Among the information that would enable universities to more thoroughly and effectively manage risk are:

- background, work history, educational institutions, affiliations with talent recruitment programs, and affiliations with any PRC military or espionage organizations for students applying from China, to assist universities in their vetting processes;
- best practices in **cybersecurity and data management;**
- **foreign influence goals and methods employed by China;**
- **regular updates on export control laws and enforcement cases**;
- China's funding for students, identifying grants, scholarships, and other financial ties, in general and for specific students;
- a database of China's and Chinese entities' foreign research collaborations;
- best practices for controlling laboratory access and monitoring; and
- data loss prevention tools.

In addition, there are a number of steps that universities can take to prevent and mitigate risks:

- **establish a Foreign Influence and Research Security Office to track and assess foreign collaborations and to assess and make recommendations about proposed collaborations;**

U.S. HOUSE OF REPRESENTATIVES COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

Subcommittee on Investigations and Oversight
Assessing the Threat to U.S. Funded Research

Mr. John F. Sargent Jr., Retired, Specialist in Science and Technology Policy, Congressional Research Service

- **implement mandatory foreign funding disclosure requirements for faculty and researchers;**
- **use AI-driven cybersecurity tools to detect unauthorized access to research data;**
- **conduct regular training on research security for faculty, staff, and students; and**
- **work with U.S. government agencies (e.g., the** Federal Bureau of Investigation **(FBI), National Science Foundation (NSF), Department of Energy (DOE)) to obtain updated risk intelligence.**

Risks Associated with China Acquiring Research Performed by U.S. Universities

The PRC's acquisition of U.S. research poses a range of risks, particularly in areas such as national security, economic competitiveness, and academic integrity. Universities, as hubs of leading-edge research, are particularly vulnerable. Among the top risks:

Intellectual Property Theft and Economic Espionage

- Unauthorized transfer of critical research, particularly in critical and emerging economic and defense technologies, such as artificial intelligence (AI), autonomy, quantum computing, robotics, nanotechnology, biotechnology, and advanced materials.
- Exploitation of academic collaborations and joint research projects to gain access to innovations.
- Infiltration of labs through visiting scholars or researchers affiliated with Chinese institutions linked to the PRC government, civilian or military.

National Security Threats

- U.S. federal funding for classified or export-controlled research may be unintentionally exposed through collaborations with Chinese entities.
- Research in sensitive areas (e.g., defense, cybersecurity, aerospace) could be used for military applications by the PRC government.

Data Privacy and Cybersecurity Risks

- Targeted cyberattacks on university networks to access valuable research data and intellectual property.
- Compromised communication channels leading to leaks of confidential research.

U.S. HOUSE OF REPRESENTATIVES COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

Subcommittee on Investigations and Oversight
Assessing the Threat to U.S. Funded Research

Mr. John F. Sargent Jr., Retired, Specialist in Science and Technology Policy,
Congressional Research Service

- Universities' open-access culture making them vulnerable to unauthorized data extraction.

Influence on Academic Integrity and Research Agendas

- Chinese funding or partnerships potentially influencing the direction of university research to areas of interest to China and targeted in their science, technology, and industrial plans.
- Pressure on researchers to self-censor topics critical of the PRC (e.g., human rights, Taiwan, Hong Kong, Uyghur issues).
- Covert recruitment programs (e.g., the Thousand Talents Plan) incentivizing U.S.-based researchers to transfer knowledge abroad.
- Potential risks from Confucius Institutes or other university-affiliated programs serving as avenues for influence operations.

Supply Chain Risks in Research Equipment and Technology

- Dependence on PRC-manufactured laboratory equipment, which may contain security vulnerabilities.
- Risks of compromised hardware/software in fields such as telecommunications, semiconductor research, and biotech.

Mitigation of Risks Associated with the PRC Acquiring U.S. Research

To effectively mitigate risks associated with China acquiring U.S. research, universities need **better intelligence, monitoring capabilities, and risk assessment frameworks**. This information will better enable informed decision-making about the prudence of engaging with PRC entities on particular research. This includes:

Research Funding and Collaboration Transparency

- **Comprehensive, accessible database of foreign funding sources**: Universities need detailed disclosures of funding from Chinese institutions, including government, corporate, and academic sources.
- **Complete list of partnerships**: A centralized database of research collaborations, agreements, and joint projects with Chinese entities.
- **Foreign talent recruitment affiliations**: Identifying researchers with links to China's talent recruitment programs (e.g., Thousand Talents Plan).

U.S. HOUSE OF REPRESENTATIVES COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

Subcommittee on Investigations and Oversight
Assessing the Threat to U.S. Funded Research

Mr. John F. Sargent Jr., Retired, Specialist in Science and Technology Policy, Congressional Research Service

Research Security and Intellectual Property Protection

- **Tracking of sensitive research areas**: A clear mapping of projects in high-risk fields like AI, quantum computing, biotechnology, and aerospace.
- **Patent filing and commercialization data**: Understanding where research outputs are being patented and whether they are being shared internationally.
- **Export control compliance checks**: Ensuring that university research does not violate U.S. laws on technology transfer (e.g., International Traffic in Arms Regulations (ITAR), Export Administration Regulations (EAR)).

Cybersecurity and Data Protection

- **Real-time network traffic analysis**: Detecting suspicious access patterns or data exfiltration attempts by foreign actors as it is occurring.
- **User access logs for research databases**: Identifying unusual access to/attempts to access sensitive research data by foreign nationals.
- **Supply chain security assessments**: Verifying the integrity of research equipment and software procured from Chinese manufacturers.

Personnel and Visitor Screening

- **Background checks on visiting scholars and researchers**: Understanding affiliations with Chinese military-linked institutions or state-owned enterprises (SOEs).
- **Monitoring of faculty ties to foreign governments**: Disclosure of financial, professional, or advisory relationships with Chinese entities.
- **Visa and travel records of researchers**: Identifying frequent travel to China that may indicate knowledge transfer risks.

Legal and Compliance Risk Assessment

- **Database of U.S. regulations on foreign research collaborations**: Ensuring compliance with evolving laws (e.g., CHIPS Act provisions, National Security Presidential Memorandum 33 (NSPM-33)).
- **Audit trails of disclosures and compliance filings**: Ensuring accurate reporting of foreign funding and affiliations.
- **Case studies of previous research security breaches**: Learning from past incidents to improve internal controls.

Academic Integrity and Influence Monitoring

U.S. HOUSE OF REPRESENTATIVES COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

Subcommittee on Investigations and Oversight
Assessing the Threat to U.S. Funded Research

Mr. John F. Sargent Jr., Retired, Specialist in Science and Technology Policy,
Congressional Research Service

- **Tracking shifts in research focus due to foreign influence**: Identifying changes in research direction that may benefit the PRC's strategic goals.
- **Monitoring censorship or self-censorship trends**: Detecting suppression of research critical of the PRC (e.g., human rights, Taiwan, Hong Kong).
- **Awareness of China's influence operations**: Understanding the role of Confucius Institutes, student organizations, and funding mechanisms in shaping university policy.

Mitigation of Risks Associated with Chinese Students Conducting Research at U.S. Universities

U.S. universities must **balance open academic collaboration with national security interests**. U.S. universities can mitigate risks associated with **Chinese graduate students conducting research in their laboratories** by implementing a **multi-layered security approach** that balances academic openness with national security concerns. This allows PRC students to contribute to innovation in **non-sensitive areas while protecting U.S. national security**. Here are key strategies:

Enhanced Screening and Vetting of Students

- **Stricter Background Checks**
  - Verify academic and professional history, particularly affiliations with PRC **military-linked institutions (e.g., China's Seven Sons of National Defense universities)**.
  - Require disclosure of past and current **foreign government funding, affiliations, or research collaborations**.
  - Conduct **enhanced visa screening** in partnership with the Department of State and Department of Homeland Security.
- **Monitor for Talent Recruitment Program Links**
  - Require students to **declare participation** in Chinese talent programs like the **Thousand Talents Plan**.
  - Cross-check applications with U.S. government lists of foreign entities of concern.
- **Use Restricted Access for Sensitive Research**

U.S. HOUSE OF REPRESENTATIVES COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

Subcommittee on Investigations and Oversight
Assessing the Threat to U.S. Funded Research

Mr. John F. Sargent Jr., Retired, Specialist in Science and Technology Policy, Congressional Research Service

- Limit lab access for foreign students working on **export-controlled or national security-sensitive projects**.
- Implement **tiered access controls** based on project classification and student vetting status.

Research Security and Intellectual Property Protection

- **Limit Collaborations with Chinese Institutions**
  - Prohibit joint research projects with **Chinese universities tied to military or intelligence agencies**.
  - Require **full transparency** in all international research agreements and funding sources.
  - Encourage faculty to **report suspicious collaboration requests** to university leadership.
- **Implement Stronger Cybersecurity Controls**
  - Prohibit and prevent foreign students from accessing **classified or export-controlled research** databases.
  - Use **AI-driven cybersecurity tools** to monitor unusual data transfers or access patterns.
  - Require **multi-factor authentication (MFA)** for all research-related systems.
- **Secure Data Management Practices**
  - Enforce policies against **unauthorized USB usage, cloud storage uploads, and email forwarding** of research data.
  - Use **network segmentation** to limit data access to necessary personnel only.
  - Conduct **regular security audits** of labs working on high-risk technologies.

Faculty and Researcher Awareness Training

- **Mandatory Foreign Influence Training**
  - Educate faculty and staff on the risks of **research espionage, cyber threats, and foreign recruitment programs**.
  - Provide real-world case studies on **how sensitive university research has been compromised** in the past.
- **Encourage Whistleblowing and Reporting**
  - Establish anonymous **reporting channels** for faculty and students to flag suspicious behavior.

U.S. HOUSE OF REPRESENTATIVES COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

Subcommittee on Investigations and Oversight
Assessing the Threat to U.S. Funded Research

Mr. John F. Sargent Jr., Retired, Specialist in Science and Technology Policy, Congressional Research Service

- Work with federal agencies like the **FBI's Office of Academic Engagement** for research security best practices.

Legal and Compliance Safeguards

- **Strengthen Compliance with Export Control Laws**
  - Ensure **ITAR** and **EAR** are enforced for research in sensitive fields.
  - Require **licensing for non-U.S. persons** working on controlled technologies.
- **Mandatory Disclosure of Foreign Funding**
  - Require students and faculty to **disclose all foreign grants, scholarships, and financial ties**.
  - Conduct **periodic audits** to verify compliance with federal laws.
- **Develop a Foreign Research Security Office**
  - Create a **centralized office** to track foreign research collaborations and student affiliations.
  - Assign a **compliance officer** to oversee international research security risks.

Controlled Laboratory Access and Monitoring

- **Restrict physical and digital access**
- Use **badge access and biometric security** for entry into high-risk research facilities.
- Implement **role-based access controls** for lab equipment, research materials, and digital databases.

Monitor Research Output and Data Flow

- Use **data loss prevention (DLP) tools** to track research data movement within university networks.
- Conduct **random audits** of laboratory activities to ensure compliance with security policies.

Prevent Unauthorized Material Transfers

- Prohibit **unauthorized copying, printing, or photographing of sensitive research data**.
- Require **faculty oversight for international conference presentations** involving controlled research.

U.S. HOUSE OF REPRESENTATIVES COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

Subcommittee on Investigations and Oversight
Assessing the Threat to U.S. Funded Research

Mr. John F. Sargent Jr., Retired, Specialist in Science and Technology Policy, Congressional Research Service

a. What specific channels of communication do you believe should be established or improved between law enforcement and universities to facilitate the timely sharing of critical information?

Universities should pursue a **Unified Security Framework** by formalizing communication through dedicated liaisons, secure digital channels, rapid-response protocols, and faculty training, universities and law enforcement. This would allow universities to proactively mitigate national security risks while maintaining academic integrity. To facilitate **timely and effective sharing of critical information** between **law enforcement and universities**, the following **communication channels** should be established or improved:

Dedicated University-Law Enforcement Liaison Offices

- **Establish a University Research Security Office (URSO)**
  - Serve as the **central hub** for coordinating with federal agencies (FBI, Department of Homeland Security (DHS), DOE, and NSF).
  - Ensure compliance with **research security regulations** (e.g., ITAR, EAR, NSPM-33).

- **Assign University Liaison Officers**
  - Universities should designate a **Research Security Officer (RSO)** or **Foreign Influence Compliance Officer** to engage with law enforcement.
  - These officers would act as **primary points of contact** for reporting suspicious activities.

- **Regular Security Briefings and Risk Assessments**
  - Schedule **quarterly or semi-annual meetings** with the FBI's Office of Academic Engagement.
  - Discuss **emerging threats, research espionage trends, and foreign influence concerns**.

Secure Digital Information-Sharing Platforms

- **Use Federal Research Security Portals**
  - Universities should integrate with platforms like **the FBI's Safeguarding Science Initiative** to receive real-time security updates.
  - Develop **a secure reporting portal** for faculty to flag suspicious behavior.
- **Implement Encrypted Communication Channels**

  - Universities should have **secure email and messaging protocols** for law enforcement collaboration.
  - Enforce **end-to-end encryption** for sensitive information exchanges.
- **Access to Law Enforcement Watchlists**
  - Universities should be able to cross-check **applicants, researchers, and visiting scholars** against U.S. government watchlists (e.g., Entity List, Denied Persons List).
  - Establish an **early warning system** for flagged individuals linked to foreign influence programs.

Emergency and Incident Reporting Protocols

- **Real-Time Threat Reporting System**
  - Universities should have **a 24/7 direct communication line** with the FBI and DHS for research security concerns.
  - Create a **formalized reporting structure** for faculty to notify law enforcement about suspicious foreign research ties.
- **Standardized Security Alerts**
  - Establish **a classified briefing mechanism** for sharing **threat intelligence** without jeopardizing ongoing investigations.
  - Enable **campus-wide alerts** in cases of immediate security threats (e.g., cyberattacks, espionage).
- **Rapid Response Teams for Investigations**
  - Form joint task forces between **campus security, federal law enforcement, and IT security teams**.
  - Improve coordination in responding to **cyber intrusions, intellectual property theft, and unauthorized data transfers**.

Faculty and Staff Training on Security Risks

- **Mandatory Research Security Awareness Programs**
  - Require faculty and researchers to complete **annual training** on espionage risks and compliance laws.
  - Integrate **real-world case studies** on research theft incidents.
- **University-Law Enforcement Workshops**
  - Hold **regular briefings with federal agencies** to educate faculty on research security best practices.
  - Provide **customized training for labs working on sensitive research areas**.

U.S. HOUSE OF REPRESENTATIVES COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

Subcommittee on Investigations and Oversight
Assessing the Threat to U.S. Funded Research

Mr. John F. Sargent Jr., Retired, Specialist in Science and Technology Policy, Congressional Research Service

- **Anonymous Whistleblower Reporting Mechanism**
  - Create a **confidential hotline or digital portal** for reporting suspicious research activities.
  - Ensure **whistleblower protections** for faculty and students who report foreign influence concerns.

2. In your judgment, are American universities taking the Chinese threat of research espionage with the level of seriousness that it warrants? Furthermore, are universities urgently deploying decisive measures to combat the escalating and evolving threat of Chinese research espionage?

In a word, no. Too often, government efforts have met resistance from the academic community, which in large measure would prefer to go about its business with no restrictions. However, most American universities have taken steps to address concerns about Chinese research espionage, but the level of seriousness and urgency varies across institutions. While some universities have strengthened security measures, implemented stricter research disclosure requirements, and increased compliance with federal regulations, others have been slower to act due to competing interests such as academic openness, international collaboration, and fundamental disagreement with federal policies.

Key actions taken by U.S. universities include:

- **Enhanced Screening and Disclosure Requirements**: Many universities now require researchers to disclose foreign affiliations, funding sources, and collaborations, aligning with federal mandates like the Department of Justice's China Initiative (though it was officially ended in 2022 due to concerns about racial profiling and unintended consequences).
- **Cybersecurity and Data Protection**: Institutions have ramped up cybersecurity efforts, restricting access to sensitive research, encrypting communications, and monitoring network activity for unauthorized data transfers.
- **Federal Compliance and Funding Restrictions**: Universities receiving federal research funding (especially from the Department of Defense, Department of Energy, and National Institutes of Health) are increasingly required to ensure that foreign

entities, including Chinese researchers, do not have unauthorized access to sensitive projects.

- **Increased Government Scrutiny**: The U.S. government has pressured universities to cut ties with institutions linked to the Chinese government or military, such as those associated with China's Thousand Talents Program.

However, there are ongoing challenges:

- **Balancing Security and Academic Freedom**: Universities value openness and international collaboration, sometimes conflicting with national security concerns.
- **Adapting to Evolving Threats**: The PRC's strategies for acquiring research are constantly changing, making it difficult for universities to keep pace with the methods used for espionage.
- **Uneven Implementation**: Some institutions, particularly those with extensive international partnerships, may be less aggressive in enforcing restrictions, whereas others have taken a more proactive stance.

Overall, while American universities are increasingly aware of the risks and some are taking steps to mitigate them to varying degrees, there is debate over whether their response is sufficiently urgent and comprehensive. Some experts, including me, argue that stronger measures are needed, while others caution against overreach that could stifle valuable international collaboration.

3. To enhance efficiency, security, and transparency within the research and innovation ecosystem, what specific measures should be implemented to establish an 'All of Government' approach?

The following are options for inclusion in an "All-of-Government" approach to research security:

Centralized Research Security Governance

- **Create a National Research Security Coordination Office (NRSCO)**

U.S. HOUSE OF REPRESENTATIVES COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

Subcommittee on Investigations and Oversight
Assessing the Threat to U.S. Funded Research

Mr. John F. Sargent Jr., Retired, Specialist in Science and Technology Policy,
Congressional Research Service

- A **central authority** to oversee security policies, compliance, and interagency collaboration.
- Aligns and coordinates efforts among **federal research agencies, federal law enforcement agencies, federal national security agencies, and academic institutions.**

- **Establish a Unified Research Security Framework**
  - Standardize compliance requirements for **federal grants, export controls, and foreign influence disclosures**.
  - Enforce common **risk assessment methodologies** across agencies.
- **Develop a National Secure Research Database**
  - A **government-wide registry** of federally funded research projects.
  - Tracks **foreign collaborations, funding sources, and research personnel** to detect vulnerabilities.

Real-Time Information Sharing and Threat Intelligence

- **Secure Research Intelligence Exchange (SRIX)**
  - A **classified threat intelligence-sharing platform** for universities and agencies.
  - Provides **real-time alerts** on cyber threats, foreign espionage, and IP theft cases.

Strengthen University-Law Enforcement Collaboration

- Mandatory **quarterly security briefings** between FBI, DHS, and university research security officers.
- Universities should have **direct access** to **restricted federal watchlists** (e.g., denied persons, foreign talent program affiliates).

Cross-Sector Cybersecurity Integration

- Establish **joint cybersecurity task forces** with **the National Security Agency (NSA), the Cybersecurity and Infrastructure Security Agency (CISA), and private-sector tech firms**.
- Require federally funded institutions to **adopt zero-trust cybersecurity architectures**.

Researcher Vetting and Foreign Influence Protection

- **National Security Vetting for Sensitive Research**

U.S. HOUSE OF REPRESENTATIVES COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

Subcommittee on Investigations and Oversight
Assessing the Threat to U.S. Funded Research

Mr. John F. Sargent Jr., Retired, Specialist in Science and Technology Policy,
Congressional Research Service

  - Implement a **tiered clearance system** for researchers working on **high-risk technologies** (e.g., AI, quantum, biotech, hypersonics).
  - Conduct **enhanced background screenings** for foreign researchers funded by U.S. grants.
- **Mandate Foreign Research Disclosure Requirements**
  - Uniform **foreign funding and affiliation disclosure rules** for grant recipients across **federal research funding agencies**.
  - **Severe penalties for non-disclosure**, including funding revocation.
- **Blacklist High-Risk Foreign Entities**
  - Enforce restrictions on collaboration with **Chinese military-linked institutions** (e.g., Seven Sons of National Defense).
  - **Prohibit participation** in foreign talent recruitment programs (e.g., Thousand Talents Plan).

Technology and Intellectual Property Protection

- **Implement National IP Tracking for Federally Funded Research**
  - Centralized database to monitor **patent filings, licensing agreements, and tech transfers**.
  - Ensure **commercialization benefits the U.S. economy, not foreign adversaries**.
- **Secure Research Supply Chains**
  - Restrict the use of **foreign-made lab equipment, software, and cloud storage** in sensitive research.
  - Expand **Cybersecurity Maturity Model Certification (CMMC)** to university research contracts.
- **Establish Export Control Compliance Offices at Major Universities**
  - Standardize **ITAR/EAR enforcement** across all federally funded institutions.
  - Deploy **AI-powered screening tools** for unauthorized research data transfers.

Funding and Innovation Incentives for Secure Research

- **Increase Federal Funding for Secure Research Infrastructure**
  - Expand funding for **onshore semiconductor, biotech, and AI research** under CHIPS Act.
  - Establish **classified research hubs** within U.S. universities for national security projects.

U.S. HOUSE OF REPRESENTATIVES COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

Subcommittee on Investigations and Oversight
Assessing the Threat to U.S. Funded Research

Mr. John F. Sargent Jr., Retired, Specialist in Science and Technology Policy, Congressional Research Service

- **Offer Security-Linked Grants and Incentives**
  - Provide **bonus funding for institutions** implementing **advanced cybersecurity** and **research integrity policies**.
  - Incentivize private sector collaboration to **commercialize U.S.-developed technologies first**.
- **Mandate Risk-Based Federal Funding Allocation**
  - Implement a **three-tier risk model** (low, moderate, high) based on **compliance, foreign ties, and cybersecurity readiness**.
  - Prioritize **low-risk institutions** for sensitive research funding.

Research security would be enhanced through a coordinated national security and innovation strategy. An "All of Government" approach would enhance research security, maintain U.S. innovation leadership, and protect against foreign exploitation.

4. 4. What should research security and due diligence look like within the US government?

A unified national research security strategy would serve to protect U.S. intellectual property, prevent foreign influence, and strengthen national security while maintaining scientific progress and innovation.

Research Security and Due Diligence in the U.S. Government

To protect **U.S. research, intellectual property (IP), and innovation** from foreign exploitation, the federal government should implement **a robust, centralized, and proactive research security framework**. This framework should include **enhanced vetting, compliance enforcement, cybersecurity protections, and interagency collaboration**. Below is an overview of what **research security and due diligence** should look like within the U.S. government.

U.S. HOUSE OF REPRESENTATIVES COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

Subcommittee on Investigations and Oversight
Assessing the Threat to U.S. Funded Research

Mr. John F. Sargent Jr., Retired, Specialist in Science and Technology Policy, Congressional Research Service

Centralized Research Security Governance

- **Establish a National Research Security Office (NRSO)**
  - A centralized **federal agency** under the **White House Office of Science and Technology Policy (OSTP)** to coordinate research security efforts across **federal research funding agencies, the FBI, and the Department of Justice**. The mission of this agency would be to detect and prevent **foreign influence, IP theft, and research espionage** in federally funded projects.

- **National Research Security Compliance Framework**
  - Standardized **research security guidelines and enforcement mechanisms** across all federal research funding agencies.
  - Mandatory compliance with **National Security Presidential Memorandum 33 (NSPM-33)**.

- **Creation of a National Secure Research Database**
  - **Unified repository** tracking all federally funded research projects, researchers, and foreign collaborations.
  - Includes **disclosure of foreign funding, affiliations, and prior international collaborations**.

Researcher Vetting and Foreign Influence Protection

- **Tiered Vetting System for Researchers**
  - Implement a **risk-based vetting system** for individuals working on federally funded research:
    - **Tier 1 (Low Risk:** Open research with no security concerns.
    - **Tier 2 (Moderate Risk)**: Research with potential dual-use applications, subject to **enhanced scrutiny**.
    - **Tier 3 (High Risk)**: Research in **critical national security areas** (e.g., AI, quantum computing, hypersonics, biotech) requiring **security clearances**.
- **Mandatory Foreign Affiliation and Funding Disclosure**
  - Require all researchers receiving federal funding to **disclose all foreign affiliations, funding sources, and international collaborations**.
  - **Automatic disqualification** for researchers with ties to **Chinese military-linked institutions** (e.g., Seven Sons of National Defense universities).

U.S. HOUSE OF REPRESENTATIVES COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

Subcommittee on Investigations and Oversight
Assessing the Threat to U.S. Funded Research

Mr. John F. Sargent Jr., Retired, Specialist in Science and Technology Policy, Congressional Research Service

- **Blacklist High-Risk Foreign Entities**
  - Maintain a **federal restricted entities list** that prohibits funding, collaboration, or employment of individuals affiliated with adversarial foreign programs (e.g., China's Thousand Talents Plan).
  - Require **agencies to cross-check researchers** against the **Commerce Department's Entity List and Treasury Department's OFAC sanctions list**.
- **Polygraph and Background Checks for High-Risk Research**
  - Implement counterintelligence background screening and polygraph **testing for researchers working on classified or export-controlled** projects.
  - Require routine re-screenings for those with access to sensitive information.

Cybersecurity and Data Protection for Research

- **Zero-Trust Cybersecurity for Research Networks**
  - Implement continuous identity verification for access to government-funded research databases.
  - Require endpoint detection and response (EDR) tools to monitor data transfers and prevent leaks.
- **AI-Powered Insider Threat Detection**
  - Deploy machine learning algorithms to identify unusual research data access patterns.
  - Flag researchers attempting **unauthorized data transfers** or **foreign communications**.
- **Controlled Access to Sensitive Research**
  - Require **role-based access control** (RBAC) to restrict research database permissions.
  - Implement geo**-fencing** to block unauthorized access from foreign locations.
- **Mandatory Federal Cybersecurity Standards for Research Institutions**
  - Enforce **Cybersecurity Maturity Model Certification (CMMC)** compliance for all federally funded universities and research centers.
  - Ban Chinese-made **hardware and software** from research infrastructure (e.g., Huawei, Hikvision).

Intellectual Property and Export Control Enforcement

- **Stronger ITAR and EAR Compliance for Federally Funded Research**

U.S. HOUSE OF REPRESENTATIVES COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

Subcommittee on Investigations and Oversight
Assessing the Threat to U.S. Funded Research

Mr. John F. Sargent Jr., Retired, Specialist in Science and Technology Policy, Congressional Research Service

- Require **all federally funded institutions** to implement **export control compliance** offices.
- Mandate export control **training** for all researchers working in **controlled technology fields**.

- **Real-Time Research Data Flow Monitoring**
  - **Track the commercialization and patent filing process** for federally funded research.
  - Prevent **unauthorized technology transfers** to foreign institutions.
- **Federal Research IP Protection Task Force**
  - Establish a joint Department of Justice (DOJ)-Department of Defense (DOD)-Federal Bureau of Investigation (FBI) task force to investigate and prosecute IP theft and research espionage cases.
  - Enforce strict penalties **for unauthorized knowledge transfer**, including **criminal prosecution and financial penalties**.

Interagency Collaboration and Threat Intelligence Sharing

- **Real-Time Federal Research Security Portal**
  - A **classified government-wide platform** to share **threat intelligence on foreign influence, cyber threats, and espionage activities** with federal agencies and universities.
- **Quarterly Security Briefings for Universities and Research Labs**
  - The federal government should conduct research on new and emerging mechanisms by which foreign adversaries are seeking to acquire U.S. research and technology from U.S. universities.
  - FBI, DHS, and DOE should conduct **regular security briefings** with universities and government labs on evolving threats.
  - Provide real-world case studies of **research theft** to faculty and staff.
- **Emergency Response Teams for Research Security Breaches**
  - Establish rapid response teams to investigate and mitigate research security incidents.
  - Deploy cyber forensics teams to **trace and recover stolen research data**.

Research Security Incentives and Compliance Enforcement

- **Federal Research Security Grant Program**

U.S. HOUSE OF REPRESENTATIVES COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

Subcommittee on Investigations and Oversight
Assessing the Threat to U.S. Funded Research

Mr. John F. Sargent Jr., Retired, Specialist in Science and Technology Policy, Congressional Research Service

  - Provide additional funding for institutions that demonstrate superior research security practices.
  - Incentivize universities to invest in **cybersecurity, export control compliance, and insider threat monitoring**.
- **Severe Penalties for Non-Compliance**
  - **Defund universities that fail to comply** with national security regulations (e.g., failing to disclose foreign affiliations).
  - Implement criminal penalties for **willful research data theft and unauthorized foreign transfers**.
- **Government-Approved Research Collaboration Agreements**
  - Require **federal approval for** international research partnerships in high-risk fields.
  - Ban collaboration with adversarial **nations and their research institutions in critical research areas**.

In closing, I want to re-emphasize a point I made in my testimony: The U.S. Government should start with the rebuttable presumption that science and technology cooperation with China is not in the national interest of the United States. We should be asking first whether any proposed research with China is absolutely indispensable to U.S. national security, the U.S. economy, or U.S. public health and the environment; second, whether China is the only partner in the world with whom we can do such proposed research; and third, whether the proposed research advances U.S. national security, economic, or public health interests more than it does China's.

Responses by Mr. Jeffery Stoff

U.S. HOUSE OF REPRESENTATIVES COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

Subcommittee on Investigations and Oversight
Assessing the Threat to U.S. Funded Research

Mr. Jeffrey Stoff, President, Center for Research Security & Integrity

Questions submitted by Chairman Rich McCormick, Committee on Science, Space, and Technology

1. Based on your testimony that federal agencies are not consistently updating universities on research security threats, do you believe the Department of Justice is utilizing all available legal tools to aggressively investigate and prosecute violations of research security, and if not, what specific actions do you believe are lacking?

It is important to understand that there are very few regulations in place that directly pertain to research security, namely restrictions that proscribe collaboration with China on any research funded by NASA, and new rules by the Department of Defense that will restrict DoD funding to US entities that collaborate on fundamental research with select foreign entities. As I state in my written testimony, save for those two exceptions, US institutions are free to collaborate with any organization regardless of any national security, economic security, or ethical risk such activity may pose (especially risks from China). US universities largely ignore these risks; the massive scale of research collaborations with high-risk PRC entities demonstrates US institutions' systemic disregard for research security.

However, research security concerns do intersect with federal research grant and contract non-compliance – where research institutions fail to abide by the terms, conditions, and disclosure requirements. Examples are when universities do not disclose foreign gifts, grants, or contracts relating to research activities and unreported commitments and affiliations of grantees. In most cases, it is prudent for the Department of Justice to pursue civil remedies for grant compliance violations. Thus, continued investment in DoJ's civil division is needed to more aggressively pursue cases based on the False Claims Act and related civil violations. However, in certain cases, criminal prosecutions may be appropriate and pursued in egregious instances and a variety of statutes may apply, such as tax evasion, false statements, visa fraud, and (in rare cases) intellectual property theft. We must expose DoJ to these investigations and ensure the civil division is appropriately resourced to address these issues.

It is also important to understand that the DoJ should not be the sole enforcer. Federal funding agencies should revise policies and bolster administrative mechanisms at their disposal when grant or contract non-compliance is taking place. For example, agencies can more aggressively pursue debarments for violators; suspend funding of awards to an institution that is in violation of grant or contract terms until administrative remedies are put in place; publicize more case

studies of what violations look like – such as tactics and methods that indicate fraud or non-compliance, etc.

2. In your testimony you highlight the critical role of research universities in safeguarding sensitive research. How frequently are university research security protocols assessed and adapted to address evolving threats, and what mechanisms are in place for continuous improvement?

I have no optic or insight into specific protocols, practices, or procedures universities use to deal with evolving threats. These are questions that federal funding agencies should be asking directly of universities that receive any federal research dollars and the government should assess the responses to inform policy making. Per the previous question and my written testimony, I do not believe most universities have the capability nor the incentive to safeguard sensitive research in any meaningful way based partly on the data I have collated, and partly because there are few prohibitions or restrictions on the funding they receive. Thus, it is unreasonable to expect universities to voluntarily, at their expense, create robust security protocols that may restrict potentially risky partnerships when there are few rules against that. There is little incentive to do so.

At the same time, placing the overwhelming burden and responsibility on universities to self-monitor and assess complex national security risks is unreasonable. The US government needs to offer resources to provide training, tool development, due diligence support, etc. to help research institutions get a better handle on both federal grant or contract compliance and understand national security risks. Outside organizations like my non-profit, private sector firms, and possibly some think tanks can provide additional support, partly because of the next question, regarding the US government's inability to tackle this on its own. Capacity building is needed in both academia and the government.

U.S. HOUSE OF REPRESENTATIVES COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

Subcommittee on Investigations and Oversight
Assessing the Threat to U.S. Funded Research

Mr. Jeffrey Stoff, President, Center for Research Security & Integrity

3. Mr. Stoff, from what you have seen, do you think the US government has experts qualified to address research security? Where has the US government failed; where have universities failed; and where has the intelligence community failed?

No. There are only a handful of individuals in the government who have a high-level understanding of and experience in research security issues. This has been a systemic problem for at least a decade. While I was in the government, I proposed multiple projects and programs to address the knowledge and oversight deficiencies but did not get support from leadership.

My written testimony, as well as previous testimonies I have provided, discuss at length the structural impediments and failures by the intelligence and law enforcement communities. Here I summarize some key areas:

- Research security issues intersect with national security issues, but Offices of Inspectors General (OIG) and the Intelligence Community (IC) do not interact with one another in meaningful ways where different capabilities can be combined. In other words, the siloed nature of each agency's mission (and restrictions on or aversion to data sharing) has contributed to a largely transactional and tactical response by the government; little thought is given to strategic approaches to deny, disrupt, dismantle, or mitigate national security threats.
- A lack of expertise on the scale, scope, complexity, and magnitude of research security threats has contributed to knowledge gaps, some of which originate from a devaluation and descoping of open-source intelligence within the IC. This lack of expertise also extends to OIGs and other law enforcement elements. Very few officers know how to effectively conduct the research, analysis, and (mostly) civil investigations into research security-related cases.
- The IC does not appear to have a clear mission or mandate to protect our critical technology or innovation ecosystem from adversarial nations' predations, especially at the earlier stages of R&D. Most efforts are limited to collecting intelligence, not disrupting threats. The IC's continued, multi-decade descoping of open-source intelligence also means that very little information is collected that can be shared with the research community.

The government has a responsibility to protect critical technology and mitigate malign foreign influence within our research ecosystem. This has largely been the purview of the FBI, where it has opened investigations related to professors working on fundamental research under national

security/counterintelligence grounds, such as economic espionage, IP theft, etc. However, proving criminality based on our legal statutes is very challenging in many cases, especially regarding fundamental research. When I was in the government, I was aware that FBI counterintelligence elements would open a case on a person of interest who may be involved in critical technology transfers to China. Those cases would remain open for years with no observable action taken. Some of those cases involved grant or program fraud and other non-compliance that could have been pursued via civil remedies, such as the False Claims Act or grant debarments. But statutes of limitations would run out, preventing such alternative approaches. Counterintelligence cases can sit idle for years and remain in the control of the FBI with little recourse by other affected agencies.

4. To enable universities to more effectively assess potential risks related to foreign influence in research, what essential information gaps exist, both within universities and across relevant government agencies? Furthermore, what specific channels of communication, including intra-agency information sharing protocols, should be established or improved between law enforcement and universities?

I will answer the latter question first. Paradigmatic shifts are necessary to create effective information sharing mechanisms, both within the government through interagency efforts and government-to-academia information sharing. The FBI, for example, is quite limited in what it can share externally, given the nature of its mission in conducting criminal investigations or counterintelligence operations. Yet the government's default has been to rely on the FBI for most engagement and outreach activity to universities. While IC and law enforcement elements have done a reasonably good job at raising awareness among research institutions that threats posed by China are significant, there is a dearth of case material, expertise, and collected (and shareable) information that has hampered the government's ability to relay to academia the scale, scope, sophistication, and pervasiveness of the threats and risks.

Worse still, information sharing among OIG elements of federal agencies and other law enforcement entities that conduct civil or administrative investigations is piecemeal at best. This is also true for any due diligence or vetting efforts done on federal grants or contracts. As I report in my testimony, the lack of sufficient interagency information sharing and coordination has also led to inconsistent standards and practices for assessing risk and exploitation by individuals and institutions that can game the system in seeking grant or contract awards.

U.S. HOUSE OF REPRESENTATIVES COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

Subcommittee on Investigations and Oversight
Assessing the Threat to U.S. Funded Research

Mr. Jeffrey Stoff, President, Center for Research Security & Integrity

I am also not aware of any effort to share information with the research community on examples, trends, patterns, case studies, etc. of violations of integrity and trust that some PRC entities have exhibited. In a recent study my non-profit published, I offer recommendations on some of these issues that both the US and allied nation governments should take on with respect to formalizing information sharing in these areas.

Additionally, the national security community has made very little effort to address persistent and yawning knowledge gaps (at least from publicly available information sources) on the PRC's research ecosystem and what entities and programs pose various types of risks to research security. This is another area where new paradigms are needed – where NGOs and non-profits, think tanks, and private sector data providers should be contributing to efforts to expand the knowledge base and close critical gaps in our understanding; the US government lacks the expertise or mission priority to do this itself. A few examples of persistent knowledge gaps with respect to China include, but by no means are limited to:

- Subdivisions and laboratories at PRC civilian universities and Chinese Academy of Sciences institutes that conduct defense research or develop technologies that can improve or enable China's mass surveillance operations and corresponding human rights abuses
- Key PRC centers of research and engineering excellence in critical technology fields and the key personnel and programs involved, their domestic and international partnerships, sources of funding, etc.
- A catalog of research institutes that are subordinate to PRC state-owned defense enterprises that function like academic entities and collaborate on research internationally
- In-depth understanding of the entities, programs, and key actors involved in PRC efforts to integrate commercial enterprises with research institutions and how PRC academia may be used as instruments of industrial policy that violate norms of trust, transparency, integrity, and influence

U.S. HOUSE OF REPRESENTATIVES COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

Subcommittee on Investigations and Oversight
Assessing the Threat to U.S. Funded Research

Mr. Jeffrey Stoff, President, Center for Research Security & Integrity

5. Mr. Stoff, can you briefly describe how research, technology know-how, and intellectual capital is exploited and diverted by China? What specific policies and statutory loopholes does China use to target and acquire foreign technology?

The list below is a sampling, primarily limited to how China exploits our R&D ecosystem – often with impunity and little regulatory oversight. There is a myriad of other ways China can acquire US intellectual capital and property through legal and illicit means that go beyond the scope of this testimony (e.g., cyber operations / hacking; IP theft; joint venture agreements, etc.)

- Converting or diverting US government-funded research into intellectual property that is patented and commercialized in the PRC; PRC state-linked funding provided to US startups after those entities received Small Business Innovation Research (SBIR) and other US government-backed support and then technology and/or business operations are transferred to China.

- Repurposing US research, including in seemingly innocuous fields like climate change and hearing aid research, to PRC defense programs and weapons system development that can undermine or eliminate US military superiority.
- Directing or redirecting US critical technology research funded by industry and federal and state governments by selectees of PRC talent recruitment programs who are under contract with and tasked by the PRC government.
- Improperly influencing or manipulating federal research grant evaluations and award decisions.
- Applying US research to enable or enhance the PRC's domestic surveillance apparatus and human rights abuses.
- Influencing or co-opting US academics' hiring or sponsoring of PRC national PhD students, postdoctoral fellows, and visiting researchers that circumvent merit-based processes and build talent and training pipelines that overwhelmingly benefit China.

A key regulatory loophole China exploits is based on National Security Decision Directive 189, which directs most fundamental research to be exempt from export controls or other oversight. The argument is that early-stage research that is published is beneficial, and as the information is shared, there is no need to protect such R&D. My written testimony to this Committee and the

Senate Foreign Relations Committee discusses the fallacies of this argument and how the PRC has exploited such regulatory gaps. This will become an increasingly acute problem as the pace of technology development accelerates, i.e., timelines between basic and theoretical research and development of viable military or commercial applications will continue to shrink. This also holds true for the increasing dual-use nature of many STEM fields now, including biotech and environmental research.

6. What should research security and due diligence look like within the US government?

The last recommendation in my written testimony describes in substantial detail what this should look like within the US government. All such efforts must be centralized into a single entity (referred to as the National Research Security, Integrity, and Compliance Center as a suggested name) that has the legal and policymaking authority to oversee all security and due diligence functions for every federal agency that funds fundamental research. By doing so, the aforementioned challenges of siloed missions, information sharing and knowledge deficiencies, and inconsistent risk standards and vetting processes can be mitigated. Additionally, there would be substantial cost savings by removing duplicative efforts; due diligence and vetting functions of multiple agencies would be consolidated into a single organization.

An (approximate) construct in terms of functions is the National Counterterrorism Center (NCTC) stood up after 9/11. Obviously, the missions of the proposed center and NCTC are quite different, but conceptually, housing centralized research, analysis, operations, and interagency cooperation could be similar. Additionally, the proposed center would also directly support an investigative task force led by DoJ, OIG and other law enforcement elements that would be dedicated to pursuing civil, criminal, and administrative investigations on research security issues (i.e., grant and contract compliance). Financial recoveries on civil claims pursued by the Department of Justice could also provide much of the funding to operate the supporting research security compliance center. Lastly, such a center would need to have the authority to refine and develop new policies for all federal agencies regarding grant and contracting rules, create formal information sharing and risk assessment support to research institutions, and provide training and resources to both government and academic elements.

Responses by Dr. Maria Zuber

U.S. HOUSE OF REPRESENTATIVES COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

Subcommittee on Investigations and Oversight
Assessing the Threat to U.S. Funded Research

Dr. Maria Zuber, E.A. Griswold Professor of Geophysics and Presidential Advisor for Science and Technology Policy, MIT

Questions submitted by Chairman Rich McCormick, Committee on Science, Space, and Technology

1. In his testimony, Mr. Sargent called for a "sea change" in how the American research community sees its responsibilities to the U.S. Your testimony supports continued open collaboration with China, citing, among other things, a shortage of U.S. STEM students. However, numerous reports show that China restricts access to its own research, especially in areas like military technology and advanced manufacturing. How do you reconcile this lack of reciprocity with your support for continued open collaboration?

    a. Do you believe that the information and research gained from academic partnerships with China necessitates the partnership?

    b. Do you believe that US institutions are getting as much out of these relationships as the CCP is? Can you provide any examples of research that could not have been done without this collaboration?

RESPONSE:

First, let me correct one assertion in the question. I did not argue that the U.S. needs to collaborate with institutions and researchers in China because of a shortage of U.S. STEM students. I view the issues of research collaborations with China, and the recruitment of Chinese talent to the U.S. as separate, if related issues.

In terms of collaboration with Chinese institutions and scientists, I agree that reciprocity is critical, and that institutions and scientists in China are not always willing or able to behave reciprocally. The report "University Engagement with China: An MIT Approach," issued in November 2022, which continues to guide MIT's thinking about China, makes clear that MIT understands the risks of collaborating with China and that China often tries to take undue advantage of U.S. scientific openness.

That does not mean, however, that there are no research collaborations with China that would have net benefits to the U.S. At MIT, we examine every potential engagement with China carefully – we have a special "elevated risk process" for this purpose – and one of the questions we always ask is whether there would be true, unique, intellectual benefits for MIT that do not pose any threats to U.S. national or economic security, or to human rights. The process has resulted in MIT approving some projects, rejecting others and modifying many. For many reasons, the number of proposed and approved projects has been declining.

I should add that we always require the results of any research collaboration with China to be open and publishable – the standard for science generally at MIT (except at Lincoln Laboratory, which conducts classified research).

There are still areas of research – even in this era of heightened competition – where collaborative research with China can be of help to the U.S. These may include topics like food safety, environmental monitoring and analyzing some health data. In addition, there may be research where access to equipment or data could be enhanced by working with China. For example, with the collapse of the Arecibo radio telescope in Puerto Rico, access to China's Five-hundred-meter Aperture Spherical radio Telescope (FAST) would be beneficial to some U.S. researchers, at least until Arecibo is replaced (and there are no serious plans to do so).

It is also in the interest of the U.S. to understand how China's science is progressing, and some collaborations can provide a window on that. We need to acknowledge that science and engineering in China is now sometimes more advanced than that in the U.S. – and that is no longer because of knowledge transfer, illegal or otherwise, from the U.S. It is because of significant investment by the Chinese government.

It also should be noted that there are many kinds of ways U.S. and Chinese institutions might collaborate. Collaboration does not necessarily mean working in each other's labs. It often means coordinating efforts on projects thar are being otherwise conducted separately.

Finally, your question refers specifically to military technology and manufacturing. U.S. universities should not collaborate with China on military technology or with military institutions. MIT makes that clear in our China report. On "dual use" technology, any project needs to be closely scrutinized, but it's important to remember that most U.S. university research is basic and open, unlikely to be close to any final military product. Projects related to manufacturing must also be closely scrutinized under the standards I described above. The U.S. has much it might learn from Chinese manufacturing but must be careful not to help China advance more quickly or successfully in that arena.

I do also want to comment on Chinese STEM students in the U.S., which you mentioned in your question and which you raised during the hearing. You made three assertions during the hearing on this subject that are simply not accurate. You claimed that universities were "hiring" international graduate students when there were plenty of qualified U.S. applicants; you implied that most international graduate students return to their home countries; and you said that there must be some "financial incentive" that is causing U.S. universities to accept so many international graduate students.

First, as I noted in my testimony, the policy question for the U.S. should be whether our nation is the net beneficiary from recruiting foreign STEM talent. The answer is assuredly yes. Indeed, other nations like Canada and the UK are envious of our ability to attract foreign talent, rightly viewing it as one of the great economic and security strengths of the U.S., and they are doing everything they can to attract students to their countries instead. Attracting the top talent from all over the world enriches the U.S. literally and figuratively. Many of the U.S.'s advances in

science and engineering are due to the talent we attract to our shores. It's no accident that many of the leaders of our top tech companies were born overseas.

I would also note that this is not a new phenomenon. U.S. science got one of its initial boosts by being a haven for scientists escaping the Nazis. After the war, aspects of U.S. science, including the space program, advanced partly by scooping up some of the scientists who had worked for the Nazis, Werner von Braun being a prominent case in point.

The U.S. needs to do much more to educate our students in STEM and encourage them to go on to graduate work in STEM fields. We do not have sufficient students in those fields now. But the U.S. will never have a monopoly on talent, and we will always benefit from attracting bright, aspiring scientists and engineers. We would, though, welcome the day when the U.S. will be less dependent on those foreign scientists – a dependence which goes back several decades.

In terms of the facts, the vast majority of Chinese STEM Ph.D.s remain in the U.S. after receiving their degrees, and more would if we acted like we wanted them. In my testimony I quoted the figures from the National Science Foundation showing that the percentage, while declining, of those who remained in the U.S. post-Ph.D. was 88% after five years and 81% after 10 years.

Most important, MIT and to my knowledge, other leading U.S. universities, are not making money off of international graduate students. Graduate students' tuition is covered and many receive a stipend for the work they conduct research and teaching. Graduate students are the work horses of academic laboratories; U.S. university labs would not function without them. And the international talent in those labs is one reason they are so successful.

There are schools that gain revenue from foreign *under*graduates. MIT is not one of them. We cap our foreign undergrads at about 10 percent, and for financial aid, we treat them the same as domestic students. But there are schools, especially large state schools, that need the revenue from foreign students to make up for the cuts in state funding. International undergraduates have not been considered to be much of a security risk, and the U.S. benefits from having stronger state universities.

Another claim made at the hearing was that every Chinese student should be considered a potential spy, whatever their intention when coming to the U.S., because the Chinese government can pressure their family. It is true that the Chinese sometimes exert such pressure. We have not seen any evidence, however, that this has caused a wide range of inappropriate activity at universities. (If such evidence *does* exist, I would be most interested in reviewing it.) One reason there is little illicit activity is that, as previously mentioned, the results of most academic research are published. But the important thing to recognize, as noted above, is the significant net benefit to the U.S. from having these students. China would do much more damage to the U.S. by preventing its students from coming here for their Ph.D. work than it could ever do by using those students for improper activities.

The U.S. may be engaging – intentionally or not – in a "natural experiment" to see what happens when we discourage foreign talent from coming to the U.S. Visa revocations done on the

slimmest pretexts and other current actions and rhetoric are sending a clear message that the U.S. is no longer interested in benefiting from foreign talent. We are encouraging a brain drain from the U.S. I am not optimistic about the impact.

2. How do you assess ethical risks in research security? For example, research that is utilized for the development of surveillance capabilities being conducted with entities known and well-documented to utilize such technologies to commit human rights violations.

RESPONSE:

As mentioned above, one of the criteria that MIT uses in its elevated risk process is whether a proposed project could contribute to human rights abuses. MIT has rejected proposed projects because of such concerns. It should be, and is an important consideration.

3. Mr. Stoff's testimony highlighted the disturbing interconnection between CCP and U.S. defense research. Given the CCP's military-civil fusion strategy and the targeting of U.S. research by the CCP, what additional information could be provided to universities for early detection of these problematic partnerships?

RESPONSE:

Universities would benefit greatly from, and would welcome more specific information from the government on any nefarious connections. Too often, information we receive now is vague or general, which makes it hard to use and not effective in persuading researchers against collaborating. Lists of Chinese entities that universities should not be doing business with would be helpful, assuming the criteria for listing are clear, and entities are added to such lists for specific, credible reasons. Listings that proliferate simply because of general tensions between the U.S. and China are of limited use. Lists of research topics that would be beyond the pale would also be useful, assuming the topic areas are not overly broad and are added for credible reasons. Universities also would certainly benefit from any specific, credible information the government could provide about suspect activities on a particular campus or happening more broadly. Universities desire more information from the government, and when we receive it, we act on it. As I mentioned at the hearing, MIT was perhaps the first U.S. university to cut ties with Huawei, and that was because I was given a classified briefing that made clear there was a real problem.

As part of my participation in the National Academies Science, Technology and Security Roundtable, we were provided access to extensive information assembled by federal agencies about research security violations. There are unacceptably high numbers of violations related to grant fraud and lack of reporting of foreign funding sources, but there is very little evidence for espionage. The Department of Justice has concluded that the kinds of violations that are most

prevalent are best adjudicated by agencies. A 2019 report by the JASONs commissioned by NSF recommended that grant fraud be treated in a manner similar to research misconduct.[1]

4. What should research security and due diligence look like within the US government?

RESPONSE:

I believe you are asking what the U.S. government should be doing to protect information in its own laboratories and other facilities. For unclassified work, I think following the model used by universities like MIT would be appropriate. In other words, to use the words in our China report, "selective engagement with targeted risk assessment and management." The government of course has access to more information about specific individuals than universities do.

Some government agencies have made recommendations regarding the safeguarding of results of U.S. fundamental research. Chief Technology Officers of the national labs have offered guidance on risky technologies, and the Defense Advanced Research Projects Agency has offered a risk matrix for potentially problematic proposed work. These efforts have been helpful to us at MIT in our research security assessments.

[1] National Science Foundation, "NSF releases JASON report on research security," December 11, 2019, https://www.nsf.gov/news/nsf-releases-jason-report-research-security.

U.S. HOUSE OF REPRESENTATIVES COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

Subcommittee on Investigations and Oversight
Assessing the Threat to U.S. Funded Research

Dr. Maria Zuber, E.A. Griswold Professor of Geophysics and Presidential Advisor for Science and Technology Policy, MIT

Questions submitted by Ranking Member Zoe Lofgren, Committee on Science, Space, and Technology

At the hearing, Representative Harrigan noted that he had compiled "58 different instances of research espionage in the last six years," and asked your co-panelists, "why do we still have any Chinese nationals inside of our research institutions, especially within institutions that participate in research that is critical to our national interest and our national security?" First of all, this appears to be a conflation of so-called "research espionage" with cases of economic espionage and intellectual property theft, which are far more common. I would like the record to reflect the reality of the threat posed by these different categories of misconduct.

1. How does the research security threat being addressed by federal science agencies and research institutions differ from economic espionage and intellectual property theft?

RESPONSE:

Obviously, the U.S. should be doing everything possible to combat espionage, intellectual property theft and other illicit activities that threaten U.S. competitiveness and security. There is no question that China engages in such activities. These activities are more likely to occur in industry than in academia because:1) academia is more open; and 2) work done in industry is much closer to commercialization or practical application. That is not to say that illicit activities never occur in academia, but based on prosecutions, they seem to be much more rare. It is important not to conflate illicit activities with what might be gleaned from the open publication of research, and most academic research (including in China) is, and should be openly published. This does, of course, allow some leakage of knowledge (whether from or to the U.S.) But the benefits of openness far outweigh the risks, as the studies I cited in my testimony have concluded. Openness accelerates the advance of science and enables ideas to be tested, debated and built upon. The U.S. should be doing more to capitalize on what we gain from our research, not reducing what we can gain from the research itself.

2. Rep. Harrigan's question also suggests that we should have no Chinese students at our research institutions. Chairman McCormick reiterated this idea, suggesting that educating Chinese students undermines American competitiveness. The Science Committee has been discussing these issues for many years now, so I know this is an incredibly nuanced topic, and that our competitiveness with China depends on recruiting and retaining top talent domestically and internationally. This is not a zero-sum game.

Why do Chinese nationals study and work inside our research institutions? Is educating Chinese students a detriment or a benefit to American competitiveness?

RESPONSE:

I discuss this question at greater length in the second half of my response to Chairman McCormick above. International students, including those from China, come to the U.S. because we are home to most of the world's top research universities. (That stature is now under threat from a variety of federal policies that will weaken our universities and their reputations, whether that is the intention behind the policy or not.) Like Americans, international students want to engage with other top researchers, and they want to improve their prospects for a better, more productive and more prosperous future. It seems incontrovertible that attracting all this talent from around the world is a vast net benefit for the U.S.

3. Democrats on the Science Committee have longstanding concerns about racial profiling of scientists with Chinese and East Asian heritage. If xenophobia dominates, how would this impact our research security posture?

RESPONSE:

Anything that discourages top students or scholars from coming to the U.S. is detrimental to the U.S. Programs that target individuals of particular ethnicities – or that make them feel unduly targeted – are not only ethically wrong, they are counter-productive. The U.S. should of course arrest and prosecute any person who is reasonably suspected of illegal activity, including espionage and intellectual property theft. But the China Initiative was counter-productive. It put individuals who turned out to be guilty of nothing through the wringer, while making even U.S. citizens of Asian origin think twice about conducting research for the U.S. government. It was a propaganda win for China that also discouraged Chinese talent of goodwill from coming to the U.S. It also sought criminal prosecution for unacceptable deficiencies that could have been handled through traditional agency processes. The U.S. should rigorously guard against inappropriate efforts to take advantage of U.S. science and the openness of our system. It should not do so by casting what is clearly too wide, or too biased a net. More effective and productive means of protecting the U.S. are available.

Appendix II

Additional Material for the Record

ARTICLE SUBMITTED BY REPRESENTATIVE EMILIA SYKES

Exclusive: US intel shows Russia and China are attempting to recruit disgruntled federal employees, sources say

By Natasha Bertrand, Katie Bo Lillis and Zachary Cohen, CNN

5 minute read · Updated 9:36 AM EST, Sat March 1, 2025

Russian servicemen stand with the Kremlin's Spasskaya tower and Saint Basil's cathedral before the Victory Day military parade rehearsal in central Moscow, on April 27, 2023. Kirill Kudryavtsev/AFP via Getty Images

(CNN) — Foreign adversaries including Russia and China have recently directed their intelligence services to ramp up recruiting of US federal employees working in national security, targeting those who have been fired or feel they could be soon, according to four people familiar with recent US intelligence on the issue and a document reviewed by CNN.

The intelligence indicates that foreign adversaries are eager to exploit the Trump administration's efforts to conduct mass layoffs across the federal workforce – a plan laid out

by the Office of Personnel Management earlier this week.

Russia and China are focusing their efforts on recently fired employees with security clearances and probationary employees at risk of being terminated, who may have valuable information about US critical infrastructure and vital government bureaucracy, two of the sources said. At least two countries have already set up recruitment websites and begun aggressively targeting federal employees on LinkedIn, two of the sources said.

A document produced by the Naval Criminal Investigative Service said the intelligence community assessed with "high confidence" that foreign adversaries were trying to recruit federal employees and "capitalize" on the Trump administration's plans for mass layoffs, according to a partly redacted copy reviewed by CNN.

It added that foreign intelligence officers were being directed to look for potential sources on LinkedIn, TikTok, RedNote and Reddit.

At least one foreign intelligence officer directed an asset to create a company profile on Linkedin and post a job advertisement, and to actively pursue federal employees who indicate they are "open to work," the NCIS document says.

The adversaries think the employees "are at their most vulnerable right now," another of the sources said. "Out of a job, bitter about being fired, etc."

"It doesn't take a lot of imagination to see that these cast aside federal workers with a wealth of institutional knowledge represent staggeringly attractive targets to the intelligence services of our competitors and adversaries," a third source familiar with the recent US assessments told CNN.

The intelligence seems to confirm what was previously a hypothetical fear for current and US officials: that the mass firings could offer a rich recruitment opportunity for foreign intelligence services that might seek to exploit financially vulnerable or resentful former employees. The Justice Department has charged multiple former military and intelligence officials for providing US intelligence to China in recent years.

"China has always been committed to developing relations with the United States on the basis of mutual respect and non-interference in each other's internal affairs," said Chinese embassy spokesperson Liu Pengyu. "We oppose groundless speculation on China without factual basis."

CNN has reached out to the Office of the Director of National Intelligence as well as the embassy of Russia in Washington for comment.

Officials have been discussing the risk

Career officials at the CIA have been quietly discussing that risk and how to mitigate it in the recent weeks, current and former intelligence officials previously told CNN. Director of National Intelligence Tulsi Gabbard earlier this week suggested that those discussions represented a "threat" made by disloyal government employees — rather than a clinical warning of the potential risks posed by President Donald Trump's aggressive cost-cutting strategy — and that those involved should be penalized.

"I am curious about how they think this is a good tactic to keep their job," Gabbard told Fox News' Jesse Watters on Tuesday. "They're exposing themselves essentially by making this indirect threat using their propaganda arm through CNN that they've used over and over and over again to reveal their hand, that their loyalty is not at all to America. It is not to the American people or the Constitution. It is to themselves.

"And these are exactly the kind of people that we need to root out, get rid of so that the patriots who do work in this area, who are committed to our core mission can actually focus on that," she said.

Multiple current officials across national security agencies who spoke to CNN on the condition of anonymity expressed frustration at the administration's response to what they see as very real warnings — not partisan swiping.

"Employees that feel they have been mistreated by an employer have historically been much more likely to disclose sensitive information," said Holden Triplett, who served as director of counterintelligence at the National Security Council in the first Trump administration and is a former FBI attaché at the US embassies in Moscow and Beijing. "We may be creating, albeit somewhat unintentionally, the perfect recruitment environment."

'This isn't reality TV'

"This isn't reality TV," said another former intelligence official. "There are consequences."

The CIA and Defense Department are weighing significant staff cuts. The Pentagon said in a memo last week that over 5,000 probationary employees, who in most cases have been in their job a year or less, could be fired in the short term. And the CIA has already fired more than 20 officers for their work on diversity issues, many of whom are now challenging their dismissal in court.

The CIA also aggressively seeks to recruit disaffected government employees in adversarial countries "all the time," noted a former intelligence official — using similar tactics. The agency

has released a series of public recruitment videos aimed at persuading disgruntled Russian government employees to spy for the United States, videos that detailed ways to securely contact the agency.

"'Domestic political turbulence in your country? Sign up with us to help us help your country!'" the former official paraphrased the US efforts, adding that those efforts deeply aggravate foreign governments.

The CIA may have already inadvertently put some American secrets within the grasp of foreign spies and hackers. In an effort to comply with the executive order to downsize the federal workforce, the CIA earlier this month sent the White House an extraordinarily unusual email listing all new hires that have been with the agency for two years or less — a list that included CIA officers who were preparing to operate under cover — over an unclassified email server.

Some of those officers, who have had access to classified information about the agency's operations and tradecraft, may now be terminated as part of the layoffs.

This story has been updated with new reporting.

CNN's Sean Lyngaas contributed reporting.

MORE FROM CNN

US suspends offensive cyber operations against Russia, senior US ...

Trump administration announces review of Columbia's ...

How a CIA informant stopped Taiwan from developing ...

NEWS & BUZZ

China and Canada immediately

Science News
@scinews.bsky.social

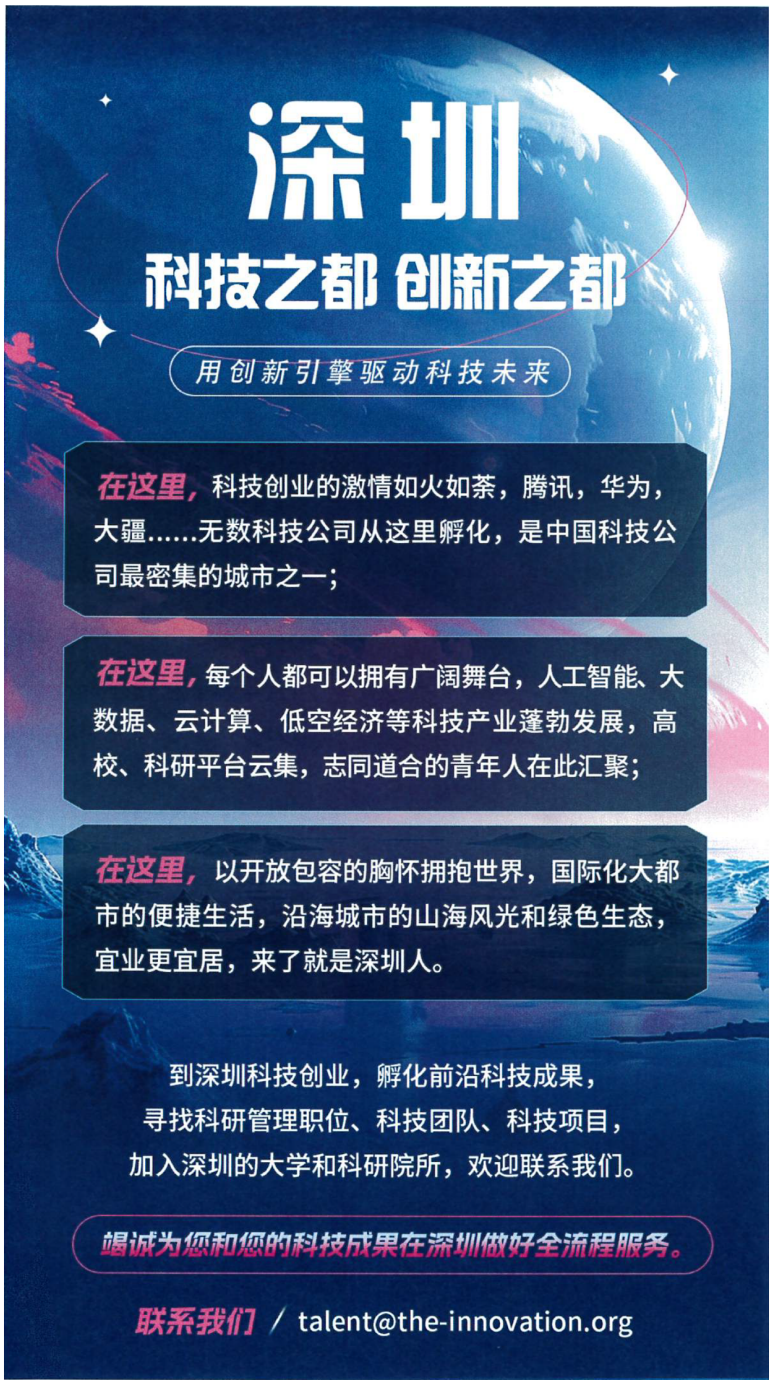
+ Follow

Welcome global talents to pursue career development and entrepreneurship in Shenzhen, China. Especially for talents who have been dismissed by the U.S. NIH or other universities/institutes.

> **The Innovation** @theinnovation.bsky.social · 8d
> Welcome global talents to pursue career development and entrepreneurship in Shenzhen, China.
>
> Email: talent@the-innovation.org

February 18, 2025 at 12:59 AM · Everybody can reply

SHENZHEN
A City of Technology
A Metropolis of the Future
Propelled by the engine of innovation,
Shenzhen drives technological advancement into tomorrow.
Here, the passion for tech entrepreneurship burns bright. Tencent, Huawei, DJI, and countless technology enterprises have been nurtured in this fertile ground, making Shenzhen one of China' s most concentrated hubs for technological innovation.
Here, boundless opportunities await. Thriving industries such as artificial intelligence, big data, cloud computing, and the low-altitude economy flourish alongside world-class universities and research platforms, weaving a tapestry of technological aspirations where like-minded talents converge.
Here, an open and inclusive spirit embraces the world. As an international coastal metropolis, Shenzhen harmonizes urban convenience with lush mountain-sea landscapes and sustainable ecosystems, crafting a future that is both professionally vibrant and eminently livable—once you come, you are a Shenzhener .
Join us in Shenzhen to pioneer cutting-edge innovations, explore roles in scientific research management, collaborate with tech teams, or initiate transformative projects. Partner with leading universities and research institutions to turn visions into reality.
Contact us today for comprehensive, end-to-end support to realize your technological ambitions in Shenzhen.
Email: / talent@the-innovation.org
Full-cycle services for you and your scientific achievements.


深圳
科技之都 创新之都
用创新引擎驱动科技未来
在这里，科技创业的激情如火如荼，腾讯，华为，大疆……无数科技公司从这里孵化，是中国科技公司最密集的城市之一；
在这里，每个人都可以拥有广阔舞台，人工智能、大数据、云计算、低空经济等科技产业蓬勃发展，高校、科研平台云集，志同道合的青年人在此汇聚；
在这里，以开放包容的胸怀拥抱世界，国际化大都市的便捷生活，沿海城市的山海风光和绿色生态，宜业更宜居，来了就是深圳人。
到深圳科技创业，孵化前沿科技成果，
寻找科研管理职位、科技团队、科技项目，
加入深圳的大学和科研院所，欢迎联系我们。
竭诚为您和您的科技成果在深圳做好全流程服务。
联系我们 / talent@the-innovation.org