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/.