



SUBCOMMITTEE ON INVESTIGATIONS AND OVERSIGHT

HEARING CHARTER

“Research Security: Examining the Implementation of the CHIPS and Science Act and NSPM-33”

**Thursday, December 18, 2025
10:00 a.m.
2318 Rayburn House Office Building**

Purpose

This hearing will examine the implementation process of research security directives and laws at U.S. agencies. It will also evaluate how federally funded research institutions are carrying out these requirements and whether additional changes are needed to better protect taxpayer-funded research.

Witnesses

- Dr. Rebecca Keiser, Acting Chief of Staff, National Science Foundation
- Dr. Daniel Evans, Assistant Deputy Associate Administrator for Research, National Aeronautics and Space Administration
- Dr. Patricia Valdez, Chief Extramural Research Integrity, National Institutes of Health
- Jay Tilden, Director of Office of Intelligence and Counterintelligence, Department of Energy

Overarching Questions

- How well are agencies and research institutions complying with the requirements of the National Security Presidential Memorandum 33 (NSPM-33) and the CHIPS and Science Act to protect federally funded research? What problems persist?
- What challenges do research institutions face in meeting relevant security mandates, such as managing conflicts of interest, conflicts of commitment, and implementing cybersecurity programs? How can federal guidance be made more explicit?
- How serious are the risks of foreign interference and espionage in U.S. research, particularly from malign actors and sponsored talent recruitment programs?

- How can Congress and federal agencies help research institutions improve their research security programs while still supporting scientific collaboration?

Background

In an era of increasing global competition, the United States must protect the billions of taxpayer dollars that fund its research enterprise from malign foreign interests and influence. In the past year, the House Science, Space, and Technology Committee investigated cases of malign foreign actors interfering with research at U.S. institutions. Recognizing the need to safeguard America's scientific leadership, federal agencies recently took several important steps to secure American research from foreign espionage, theft, and undue influence.

On January 14, 2021, President Trump issued National Security Presidential Memorandum 33 on National Security Strategy for United States Government-Supported Research and Development (NSPM-33).¹ The memorandum directs the development of a national strategy to safeguard the security and integrity of federally funded research and development in the United States from malign foreign actors.² Under NSPM-33, all federal agencies that fund research are required to ensure that covered recipient institutions implement standardized research security practices.³ These practices include policies addressing the disclosure of conflicts of interest and commitment, foreign affiliations, and external sources of support.⁴ Covered institutions include universities, federally funded research and development centers, and nonprofit research institutions that receive more than \$50 million in federal funding annually.⁵

NSPM-33 also mandates enhanced due diligence concerning personnel and institutional relationships with foreign entities, particularly where such relationships may pose risks of

¹ Presidential Memorandum on United States Government-Supported Research and Development National Security Policy, THE WHITE HOUSE (Jan. 14, 2021), archived at <https://trumpwhitehouse.archives.gov/presidential-actions/presidential-memorandum-united-states-government-supported-research-development-national-security-policy/> (last visited Nov. 12, 2025).

² Memorandum for the Heads of Federal Research Agencies: Guidelines for Research Security Programs at Covered Institutions, OFF. OF SCI. & TECH. POL'Y (Jul. 9, 2024), <https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/07/OSTP-RSP-Guidelines-Memo.pdf>; Guidance for Implementing National Security Presidential Memorandum 33 (NSPM-33) on National Security Strategy for United States Government-Supported Research and Development, OFF. OF SCI. & TECH. POL'Y (Jan. 4, 2022), <https://bidenwhitehouse.archives.gov/wp-content/uploads/2022/01/010422-NSPM-33-Implementation-Guidance.pdf>; President Trump Takes Bold Action to Strengthen the Security and Integrity of America's Research and Development Enterprise: Fact Sheet, THE WHITE HOUSE (Jan. 2021), <https://trumpwhitehouse.archives.gov/wp-content/uploads/2021/01/NSC-OSTP-NSPM33-Fact-Sheet-Jan2021.pdf>.

³ *Id.*

⁴ *Id.*

⁵ *Important Notice No. 149: Updates to NSF Research Security Policies*, NATIONAL SCIENCE FOUNDATION (NSF) (Jul. 10, 2025), <https://www.nsf.gov/notices/important/important-notice-no-149-updates-nsf-research-security/in149>; *Supra* at 1; Guidance for Implementing National Security Presidential Memorandum 33 (NSPM-33) on National Security Strategy for United States Government-Supported Research and Development, OFF. OF SCI. & TECH. POL'Y (Jan. 4, 2022), <https://bidenwhitehouse.archives.gov/wp-content/uploads/2022/01/010422-NSPM-33-Implementation-Guidance.pdf>

foreign interference or espionage.⁶ It requires institutions to develop mandatory research security training programs and to establish infrastructure supporting compliance, oversight, and enforcement.⁷ Additionally, the memorandum requires the development of a centralized, standardized conflicts-of-interest disclosure system to reduce administrative burdens while ensuring consistent application across federal agencies.⁸

One year after NSPM-33's issuance, the CHIPS and Science Act of 2022 (CHIPS) reinforced the federal government's commitment to research security. Specifically, CHIPS requires institutions receiving funding under the law to implement and certify compliance with several research security policies. Such policies include the disclosure of foreign affiliations and the management of conflicts of interest and commitment.⁹ Institutions must maintain internal controls to ensure data security, the responsible stewardship of federal resources, and transparency within international research collaborations.¹⁰

CHIPS authorizes over \$200 billion in new funding for federal research and development programs administered by agencies such as the National Science Foundation (NSF) and the Department of Energy (DOE).¹¹ These funds target research in emerging technologies, including artificial intelligence, quantum science, clean energy, and advanced communications.¹² The Act also mandates the development of regional innovation hubs, expands support for STEM education, and establishes mechanisms to accelerate the commercialization of federally funded research.¹³

The House Science, Space and Technology Committee has worked to monitor the implementation of these directives. In February 2024 and in March 2025, hearings were conducted on the threat of malign foreign actors on U.S. research and U.S. research

⁶ *Supra* at 1; Guidance for Implementing National Security Presidential Memorandum 33 (NSPM-33) on National Security Strategy for United States Government-Supported Research and Development, OFF. OF SCI. & TECH. POL'Y (Jan. 4, 2022), <https://bidenwhitehouse.archives.gov/wp-content/uploads/2022/01/010422-NSPM-33-Implementation-Guidance.pdf>.

⁷ *Id.*

⁸ *Id.*

⁹ CHIPS Act of 2022, Pub. L. No. 117-167, 136 Stat. 1372 <https://www.congress.gov/117/plaws/publ167/PLAW-117publ167.pdf>; *CHIPS Technology Protection Guidebook: A Resource for Implementing Applicant and Performer Research Security Requirements*, NAT'L INST. OF STANDARDS & TECH. (Mar. 11, 2024), <https://www.nist.gov/system/files/documents/2024/03/11/CHIPS%20Technology%20Protection%20Handbook%20Final.pdf>; *Research Security Provisions, The CHIPS & Science Act of 2022 (H.R. 4346)*, ASS'N OF AM. UNIVS. (Aug. 8, 2022), <https://www.aau.edu/sites/default/files/AAU-Files/Key-Issues/Science-Security/CHIPSandScienceFinalResearchSecurityProvisions.pdf>.

¹⁰ *Id.*

¹¹ *Id.*

¹² *Id.*

¹³ *Id.*

institutions.¹⁴ On June 24, 2025, our Committee requested that GAO conduct a review of federal agencies' and research institutions' implementation of research security guidelines.¹⁵ Continued oversight is necessary to ensure that these directives are implemented to their fullest extent.

Research Security Law

The framework established by NSPM-33 and the CHIPS Act forms the backbone of current U.S. research security policy. It is designed to safeguard the integrity of American scientific research from foreign interference by mandating transparency, accountability, and oversight—particularly in federally funded projects involving foreign collaboration.

The Office of Science and Technology Policy put out its initial guidance on NSPM-33 on January 4, 2022.¹⁶ In July 2024, OSTP issued a memorandum titled Guidelines for Research Security Programs at Covered Institutions, focusing on requirements of CHIPS.¹⁷ Since then, agencies have been working to create and implement relevant guidance and policies to comply with these directives.

Guidance Recently Implemented

On July 10, 2025, the NSF updated its research security policies, with the changes becoming effective on October 10, 2025.¹⁸ These updates require all U.S. research institutions, including both public and private entities, to implement formal research security programs.¹⁹

A key component of the NSF policy update requires institutions to conduct research security assessments and maintain more documentation of the disclosures mandated by NSPM-33.²⁰ These programs must include mechanisms to ensure the full disclosure of researchers' professional and financial ties to foreign institutions. These requirements include a record of employment, appointments, or participation in foreign talent recruitment programs.²¹ Institutions must additionally retain copies of contracts, grants, and agreements related to foreign

¹⁴ *Examining Federal Science Agency Actions to Secure the U.S. Science and Technology Enterprise: Hearing Before the H. Comm. on Sci., Space, and Tech.*, 118th Cong. (2024), <https://science.house.gov/2024/2/full-committee-hearing-examining-federal-science-agency-actions-to-secure-the-u-s-science-and-technology-enterprise>; *Assessing the Threat to U.S. Funded Research: Hearing Before the Subcomm. on Investigations and Oversight of the H. Comm. on Sci., Space, and Tech.*, 119th Cong. (2025), <https://science.house.gov/2025/3/assessing-the-threat-to-u-s-funded-research>.

¹⁵ Letter from Chairman Brian Babin, H. Comm. on Sci., Space, and Tech., to Honorable Gene L. Dodaro, Gov. Accountability Off. (Jun. 24, 2025), <https://republicans-science.house.gov/cache/files/b/e/bee16621-9b35-46f4-be94-ad92b96faded/5C51F3E5B022968EE8C5733D50B1F24287404263CEEB736540C2AFFE0F10E974.25.6.24--sst-letter---implementation-of-research-security-requirements-signed.pdf>.

¹⁶ *Supra* at 2.

¹⁷ *Id.*

¹⁸ *Important Notice No. 149: Updates to NSF Research Security Policies*, NSF (Jul. 10, 2025), <https://www.nsf.gov/notices/important/important-notice-no-149-updates-nsf-research-security/in149>.

¹⁹ *Id.*

²⁰ *Id.*

²¹ *Id.*

appointments, employment, and participation in foreign talent recruitment programs for all senior/key personnel.²² This documentation must be accessible to NSF upon request and reviewed for compliance with award terms.

The new guidance also mandates research security training for all personnel paid by the federal research grant.²³ Training must cover cybersecurity, foreign interference, international collaboration, proper use of research funds, and conflict-of-interest and commitment policies.²⁴ Institutions may comply by requiring completion of NSF’s Research Security Training modules or by using equivalent training.²⁵ NSF, in partnership with NIH, DOE, and DOD, provides four online training modules to offer more accessible options.²⁶

Finally, the updated policy reflects growing concerns about cybersecurity risks posed by rapidly advancing technologies and increasingly complex research environments. To safeguard research infrastructure and data, institutions must implement mandatory protections—including secure servers or cloud systems, whether built in-house or rented from another institution.²⁷ Failure to meet these requirements could jeopardize eligibility for federal research funding, making compliance both a legal obligation and a strategic necessity.²⁸ Meanwhile, adversaries seeking to exploit U.S. research do not face the same funding and compliance burdens, creating a strategic disadvantage.²⁹ Institutions must therefore take proactive steps to meet the new NSF standards while investing in long-term cybersecurity strategies to preserve the integrity of U.S.-funded research.

Research Security Failures

NSPM-33 specifically highlights concerns about foreign governments, such as the People’s Republic of China, which have not “demonstrated reciprocal commitment to open scientific exchange and have sought to exploit U.S. research environments to circumvent the risks and costs of conducting original research.”³⁰ There are documented cases of Chinese researchers

²² *Id.*

²³ *Id.*

²⁴ *Id.*

²⁵ *Id.*

²⁶ *Id.*

²⁷ National Institute of Standards & Technology, *Cybersecurity for Research: Findings and Possible Paths Forward*, NIST IR 8481 (IPD) (Aug. 31, 2023), <https://nvlpubs.nist.gov/nistpubs/ir/2023/NIST.IR.8481.ipd.pdf>.

²⁸ *Supra* at 14.

²⁹ *Supra* at 25.

³⁰ *Supra* at 1.

attempting to smuggle U.S.-funded research and hazardous materials out of the country.³¹ However, China is not the only malign actor posing risks to U.S. research security.³²

The Committee sent several oversight letters regarding research security failures at U.S. institutions, particularly universities.³³ In their responses, institutions often maintain that they are complying with current law to the best of their ability, but note the absence of clear and consistent guidance for implementing NSPM-33 and CHIPS.³⁴ This hearing will examine the causes of these inconsistencies and consider whether legislative or regulatory amendments are needed to better protect U.S.-funded research.

³¹ See e.g. Luke Barr, *2 Chinese nationals charged with smuggling 'potential agroterrorism' fungus into US: DOJ*, ABC NEWS (Jun. 3, 2025), <https://abcnews.go.com/Politics/2-chinese-nationals-charged-smuggling-potential-agroterrorism-fungus/story?id=122454213>; Ed White, *US reports the arrest of another Chinese scientist with no permit to send biological material*, ASSOCIATED PRESS (Jun. 9, 2025), <https://apnews.com/article/michigan-lab-chinese-scientist-arrested-351e3a8ea0be25c03575cf7d3090192e>; Ephrat Livni, *Researcher's Smuggling Arrest Casts Light on Dispute Over Chinese Students*, N.Y. TIMES (Nov. 21, 2025), <https://www.nytimes.com/2025/11/21/world/asia/chinese-students-us.html>; Kendall Meachum, *Former MD Anderson researcher charged with stealing cancer research to China*, THE DAILY TEXAN (Sept. 8, 2025), <https://thedailytexan.com/2025/09/08/former-md-anderson-researcher-charged-with-stealing-cancer-research-to-china/>.

³² Letters on file with Committee Staff.

³³ *Id.*

³⁴ *Id.*