BRIAN BABIN, D.D.S., Texas
CHAIRMAN

ZOE LOFGREN, California
RANKING MEMBER

Congress of the United States
House of Representatives
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
2321 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6301
(202) 225–6371
http://science.house.gov

June 24, 2025

The Honorable Gene L. Dodaro
Comptroller General of the United States
United States Government Accountability Office
441 G Street, NW
Washington, D.C. 20548

Dear Mr. Dodaro,

Since World War II, America's research enterprise has delivered profound benefits for our health, economy, and national security. This leadership is rooted in the core commitment of our shared research environment to openness, transparency, honesty, fair competition, objectivity, and democratic values. Science, technology, and innovation have been integral to U.S. leadership in the world for many decades, supported by the strength of the U.S. research community. Today, the global strategic environment is characterized by fierce military and economic competition among many actors.

Multiple foreign governments, including those of the Chinese Communist Party (CCP), Russia, and Iran, are working vigorously to acquire U.S. research and technology through both licit and illicit means. These efforts include attempts to recruit American scientists to covertly conduct research on behalf of foreign governments or to inappropriately disclose non-public results from research funded by U.S. government sources.

To address these growing risks, President Trump issued the National Security Presidential Memorandum – 33 (NSPM-33) in January 2021, establishing a national security policy for U.S. government-supported research and development. The following year, the White House Office of Science and Technology Policy (OSTP) issued broad guidance for implementing NSPM-33, aimed at protecting federally funded research from foreign threats. However, a January 2024 GAO report revealed that federal agencies' efforts to address these risks to federal research security lacked consistency. The report recommended that OSTP improve coordination and information-sharing, particularly on identifying foreign ownership among agencies, to promote a more unified and effective approach to safeguarding U.S. research.

In February 2024, on the eve of a House Science, Space, and Technology hearing titled "Examining Federal Science Agency Actions to Secure the U.S. Science and Technology Enterprise,"[1] OSTP released two new guidance documents addressing: (1) policy for the use of standardized disclosure forms,[2] and (2) guidance prohibiting federal employee participation in foreign talent recruitment plans, as well as award applicants' participation in malign foreign talent recruitment programs.[3]

Further, in July 2024, OSTP issued a memorandum on *Guidelines for Research Security Programs at Covered Institutions*,[4] outlining guidelines that require recipients of U.S. federal science and engineering support "in excess of $50 million per year" to certify to the funding agency that the institution has established and operates a research security program, including research security training as required by the *CHIPS and Science Act*, to address their unique needs, challenges, and risk profiles. The Guidelines also note four mandatory program elements necessary for a compliant research security program: (1) Cybersecurity; (2) Foreign Travel Security; (3) Research Security Training; and (4) Export Control Training.

We request that GAO conduct a review of federal agencies' and research institutions' implementation of research security guidelines that examines the following:

1. To what extent have federal agencies incorporated research security provisions as outlined by OSTP in 2024—*Guidelines for Federal Research Agencies Regarding Foreign Talent Recruitment Programs, Policy Regarding Use of Common Disclosure Forms for the "Biographical Sketch" and the "Current and Pending (Other) Support" Sections of Applications by Federal Research Funding Agencies,* and *Guidelines for Research Security Programs at Covered Institutions*—in their policies and procedures?

2. To what extent are selected covered institutions' research security programs consistent with federal guidelines?

3. To what extent do gaps exist, if any, between agencies' and selected covered institutions' research security provisions and their implementation of NSPM-33 requirements?

4. To what extent are agencies measuring the effect of these research security requirements?

5. To what extent are federal agencies monitoring covered institutions' implementation of their research security programs?

---

[1] Examining Federal Science Agency Actions to Secure the U.S. Science and Technology Enterprise: Hearing before the U.S. House Committee on Science, Space, and Technology (Feb. 15, 2024).
[2] OSTP, Memorandum for the Heads of Federal Research Agencies: Policy Regarding Use of Common Disclosure Forms for the "Biographical Sketch" and the "Current and Pending (Other) Support" Sections of Applications by Federal Research Funding Agencies (Feb. 14, 2024).
[3] OSTP, Memorandum for the Heads of Federal Research Agencies: Guidelines for Federal Research Agencies Regarding Foreign Talent Recruitment Programs (Feb. 14, 2024).
[4] OSTP, Memorandum for the Heads of Federal Research Agencies: Guidelines for Research Security Programs at Covered Institutions (July 9, 2024).

6. What metrics are agencies using to measure the impacts and effectiveness of new research security programs?

    a. If none, what data should be collected by federal agencies to assist GAO in measuring impact or for other purposes, including audits?

Thank you for your attention to this important matter. If you have any questions, please contact Victoria Rubin at Victoria.Rubin@mail.house.gov.

Sincerely,

Brian Babin

Chairman
Committee on Science, Space, and Technology

Jay Obernolte

Chairman
Subcommittee on Research and Technology

Rich McCormick

Chairman
Subcommittee on Investigations & Oversight

cc: Zoe Lofgren, Ranking Member, House Committee on Science, Space, and Technology