Dr. Rebecca Keiser
Chief of Research Security, Strategy, and Policy and acting Chief of Staff
U.S. National Science Foundation

Before the
Subcommittee on Investigations and Oversight
Committee on Science, Space, and Technology
United States House of Representatives

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

December 18, 2025

Chairman McCormick, Ranking Member Sykes, and Members of the Subcommittee, my name is Dr. Rebecca Keiser, Chief of Research Security, Strategy, and Policy and acting Chief of Staff at the U.S. National Science Foundation (NSF). It is an honor to be with you today to discuss how NSF is working to protect critical U.S. taxpayer investments in research and development and in our domestic science, technology, engineering, and mathematics (STEM) talent from malign foreign actors.

Established by the National Science Foundation Act of 1950 (P.L. 81-507), NSF is an independent federal agency that supports research across all fields of STEM and at all levels of STEM education, charged with the mission "to promote the progress of science; to advance the national health, prosperity, and welfare; to secure the national defense; and for other purposes." Research security is a vital part of our mission and is essential to U.S. economic and national security.

To this end, NSF works closely with partners in federal law enforcement, including the NSF Office of Inspector General (OIG), and the intelligence community, as well as other federal R&D funders, some of whom are also represented here today. For example, NSF was pleased to be among the federal agencies that partnered with the Office of the Director of National Intelligence (ODNI) on the recent release of the ODNI bulletin, *Safeguarding Academia: Protecting Fundamental Research, Intellectual Property, Critical Technologies, and the U.S. Research Enterprise*. NSF also counts Congress as an important partner in this work, and we remain committed to working with you to continue to bolster U.S. research security efforts in response to current and evolving threats from our global adversaries, while maintaining robust and fruitful collaborations with like-minded allies.

Overview of Research Security

Under the first Trump Administration in 2019, NSF commissioned a report by the JASON, a group of U.S. scientists who are uniquely qualified to conduct studies in security matters for the federal government. The findings of that report and its recommendations have helped to inform NSF's approach to research security. It found that a group of governments – notably the People's Republic of China – were attempting to benefit from the global research ecosystem without upholding the core values of openness, transparency, and reciprocal collaboration.

As co-chair of the National Science and Technology Committee's Subcommittee on Research Security with the White House Office of Science and Technology Policy, DOE, and the National Institutes of Health (NIH), NSF collaborated on the development of National Security Presidential Memorandum (NSPM)-33. Released in January 2021, NSPM-33 was written to provide clear direction to the research community on research security. Indeed, many of the NSF efforts I am excited to speak with you about today have either been bolstered by or are in direct response to NSPM-33 and legislation this Committee had a leadership role in authoring.

In 2020, NSF created the position of Chief of Research Security, Strategy and Policy (CRSSP). This position was subsequently established in the CHIPS and Science Act of 2022, which also required NSF to maintain a Research Security and Policy Office. The Office of the Chief of Research Security, Strategy and Policy (CRSP) leads NSF's efforts to safeguard the research enterprise, developing policies and guardrails that ensure the security of federally funded research while maintaining an international research environment that supports collaboration with likeminded partners; collaborates with federal partners and the White House to coordinate efforts aimed at improving research security and integrity at the federal level; and engages with international partners to ensure current and future international collaborations continue to abide by our core values.

Recipients of federal research dollars also have a responsibility as stewards of that research. They must demonstrate robust leadership and oversight; establish and administer policies to promote transparency and guard against conflicts of interest and commitment; provide training and information on research security; ensure effective mechanisms for compliance with organizational policies; and implement processes to assess and manage potential risks associated with foreign collaborations and data.

The security of the U.S. research ecosystem is the responsibility of the federal government as well as the recipients of federal research dollars. It is a matter of protecting American competitiveness and national security and requires continued vigilance, culture change, and accountability.

Securing the U.S. Research Ecosystem

NSF plays an important role in federal efforts to address research security and is expanding capabilities and competencies to protect the U.S. science and engineering enterprise. Prior to NSPM-33 and the CHIPS and Science Act, NSF was working diligently to put measures in place that strengthen research security and integrity for the NSF-funded research community and for NSF staff. In 2019 and 2020, NSF actions included emphasizing compliance with disclosure requirements in

NSF's Proposal and Award Policies and Procedures Guide[1] for NSF staff and NSF-funded institutions and researchers; requiring all NSF personnel to be a U.S. citizen or be in the process of becoming a citizen; barring NSF staff from participating in foreign talent recruitment programs; and requiring annual "Science and Security Training" for all NSF employees. Following NSPM-33, NSF played a key role in harmonizing required disclosure forms across government to bring greater transparency and consistency to the federal funding process. Currently, NSF is leading an interagency effort to develop a centralized certification process for the research security program requirement established in NSPM-33. This centralized process will allow institutions to make a single certification to satisfy harmonized agency requirements, minimizing undue burden and confusion. In October 2024, NSF convened a working group comprised of 14 departments and agencies to craft an interagency memorandum of agreement to set this coordinated process in motion. The working group is in active deliberations and anticipates reaching final agreement in early 2026.

NSF has continued to work with speed and determination to build upon these earlier efforts and to implement NSPM-33 and the research security provisions of the CHIPS and Science Act. NSF implemented the prohibition on funding for researchers that participate in a malign foreign talent recruitment program, as defined by law. Research institutions must certify to NSF that they have a program to identify malign foreign talent recruitment program members through the proposal and annual reporting process. In addition, senior personnel on an NSF proposal who are responsible for the design and conduct of the research must certify they are not part of such a program, and they must do so annually during the term of an NSF award. Malign foreign talent recruitment programs include any program in a country of concern.

NSF has established analytic capabilities to proactively identify conflicts of commitment, vulnerabilities of pre- publication research, and risks to the merit review system. NSF published[2] related guidelines to help the community of federally funded researchers understand how the agency approaches these practices. NSF uses these capabilities for its Small Business Innovation Research/Small Business Technology Transfer (SBIR/STTR) Programs’ due diligence reviews and to assess NSF proposals in key technology areas for research security issues.

NSF, in partnership with DOW, DOE, the NIH, and the broader interagency community, developed research security training modules for the research community. The training modules provide researchers with clear guidelines and effective strategies to protect against existing and emerging research security threats. NSF has implemented statutory requirements for researchers to certify they have taken research security training to qualify to apply for NSF funding to ensure there is an understanding of research security risks.

In addition, NSF established the Safeguarding the Entire Community of the U.S. Research Ecosystem (SECURE) Program to empower the research community to identify and mitigate foreign interference that poses risks to the U.S.-funded research enterprise. The program includes the SECURE Center, which tracks emerging trends research security risks. For example, the SECURE Center produces biweekly SECURE Center Research Security Briefings, provides up-to-date training, and will launch the SECURE Virtual Environment once beta testing is complete. The SECURE Virtual Environment will serve as a user-driven resource for sharing best practices and technical know-how and promoting

[1] https://new.nsf.gov/policies/pappg/23-1/summary-changes

[2] https://new.nsf.gov/research-security/guidelines

meaningful dialogue throughout the research security community. SECURE Analytics is another critical component of the SECURE Program, providing expertise in the form of advisory reports and in-depth risk landscape analyses, risk modeling, and real-time risk data reporting. SECURE Analytics will launch a cutting-edge due diligence software platform once beta testing is complete.

The NSF Trusted Research Using Safeguards and Transparency (TRUST) framework guides NSF in assessing grant proposals for potential national security risks. The TRUST framework includes three branches: The first focuses on assessing active personnel appointments and positions; the second focuses on identifying instances of noncompliance with disclosure and other requirements; and the third focuses on potential foreseeable national security considerations. NSF is implementing the TRUST framework in three phases: The first, which began in FY 2025, involved piloting the process on quantum-related proposals. With this pilot, NSF is collecting data and assessing key metrics, monitoring the impact on NSF Directorates and building and evaluating NSF's ability to review the potential national security applications of NSF-funded technology. In the second phase, expected to begin later in FY 2026 or FY 2027, will incorporate lessons learned from the pilot phase and will expand the review process to include other critical technology areas, as resources allow. In phase three, NSF will scale up the review process to include all key technology areas and/or the priorities of the NSF Technology, Innovation and Partnerships (TIP) Directorate.

NSF also established the Research on Research Security (RoRS) Program to advance the understanding of the full scope, potential, challenges, and nature of the research on research security field through scholarly evidence. This includes assessment of the characteristics that distinguish research security from research integrity, improving the quantitative understanding of the scale and scope of research security risks, developing methodologies to assess the potential impact of research security threats, and assessing the additional research security risks in an innovation system that includes more use-inspired research rather than staying well within the bounds of fundamental research. For example, through this program, researchers in Illinois are exploring ways to leverage AI to rapidly discover and mitigate vulnerabilities in advanced cyberinfrastructure to prevent the theft of sensitive data and other research security breaches. In Virginia, another team is developing the first comprehensive threat assessment framework to assure research security in the novel and fast-evolving domain of AI research. This is just some of what is funded by the first ever set of RoRS awards which were made this year. We’re excited by their potential contributions to both our understanding of the research security challenge and how those challenges can be addressed. NSF has also established an international RoRS working group to collaborate with like-minded partners to build this evidence base.

Furthermore, NSF works very closely with its OIG, an independent oversight office that reports directly to the National Science Board and Congress. The OIG is responsible for conducting audits, reviews, and investigations of NSF programs, and of organizations and individuals that apply for or receive NSF funding. This responsibility includes auditing awardees to ensure that they maintain an appropriate conflict of interest policy for employees consistent with NSF requirements. The OIG also conducts financial audits and investigations to determine whether awardees are misusing taxpayer funds; failing to report financial support; duplicating research; and violating rules, regulations, or policy, including allegations of research misconduct (e.g., falsification, fabrication, and plagiarism). NSF has taken, and will continue to take, swift action, such as terminating grants and debarring researchers when the OIG reports incidents to NSF and such action is appropriate.

In several recent cases handled by the Department of Justice and NSF-OIG, institutions were required to develop research security corrective action plans. NSF OCRSSP is responsible for overseeing these corrective action plans, demonstrating NSF's focus on ensuring it is an appropriate steward of taxpayer funding to safeguard federally-funded research.

NSF also works with the Intelligence Community and other Federal agencies through its partnership with the National Counterintelligence Task Force to identify and analyze research security-related issues. NSF's research security analytics tools have significantly contributed to these efforts.

Conclusion

Safeguarding taxpayer investments in research and innovation is central to U.S. national security and international competitiveness. NSF welcomes international collaboration and understands that, when grounded in shared values of openness, transparency, and reciprocity, such collaborations with like-minded partners can advance the frontiers of science for the benefit of the American people.

Along with our federal partners, NSF has engaged in robust discussions with international colleagues bilaterally, as well as through groups like the G7, to develop common frameworks for understanding and addressing research security. The research community, industry, individual researchers, and the U.S. government must work together to identify, understand, and address the risks posed to the research ecosystem by foreign actors that do not share those values; improve awareness of these risks through increased communication and information sharing; and promote practices that further the principled conduct of research.

NSF's collaborative, well-established relationships with our federal partners, the law enforcement and Intelligence Communities, and with the NSF OIG have been critical to our response to threats to NSF-funded research from foreign interference. In addition, Congress's actions, including through the CHIPS and Science Act, have provided the agency with important authorities and tools to identify and mitigate risks and to put strong requirements in place. As good stewards of American taxpayer funds, we remain committed to the security of the U.S. research ecosystem and we look forward to continuing to work with you on this vitally important issue.

Thank you for the opportunity to appear before you today. I look forward to answering your questions.