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

Before the
Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party
United States House of Representatives

"Protecting American Innovation: The Federal Research Security Enterprise"

July 15, 2026

Chairman Moolenaar, Ranking Member Khanna, 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 a 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 2025 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 to stay ahead of current and evolving threats from our global adversaries, while maintaining robust and fruitful collaborations with like-minded allies. We also appreciate the Committee's engagement on emerging research security issues. Earlier this year, NSF worked closely with the Committee to review and strengthen safeguards governing access to NSF-funded computing resources through the ACCESS program. As a result, NSF implemented additional

protections to help ensure that access to high-performance computing capabilities is consistent with our research security objectives.

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 foreign 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 Council's Subcommittee on Research Security with the White House Office of Science and Technology Policy, the Department of Energy (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 legislative action.

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 (OCRSSP) 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; implement processes to assess and manage potential risks associated with foreign collaborations and data; establish and administer policies to promote transparency and guard against conflicts of interest and commitment; provide training and information on research security; and ensure effective mechanisms for compliance with organizational policies.

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's 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. NSF is currently leading an interagency effort, which includes convening a working group comprised of 14 departments and agencies, to develop a centralized certification process for the research security program requirement established by NSPM-33. Such a centralized process would allow institutions to make a single certification to satisfy harmonized agency requirements, minimizing undue burden and confusion.

NSF has continued to work with determination to build upon these earlier efforts, to implement NSPM-33 and the research security provisions of the CHIPS and Science Act, and to take proactive steps to further strengthen our approach to research security. For example, earlier this month, NSF published a Dear Colleague Letter notifying the research community of the agency's intent to implement a policy in FY 2027 to, among other things, prohibit the use of NSF funds to support research collaboration with entities named on restricted entity lists. This policy is closely aligned with that recently implemented by the Department of War. These lists identify entities that the U.S. Government has determined pose risks to national security and other foreign policy interests. Under the NSF policy, institutions will be responsible for ensuring award funds are not used to support prohibited collaborations and for maintaining appropriate oversight to identify and address potential noncompliance before NSF funds are expended. The policy establishes a clear expectation for the use of NSF funding while preserving researchers' ability to pursue a wide range of domestic and international collaborations that remain consistent with this prohibition. The policy also prohibits NSF funds to be used by senior/key personnel with active positions with, or funding from, these restricted entities. In this way, NSF will protect U.S. federal funds and safeguard U.S.-produced research from entities of concern.

This policy is the newest tool in NSF's research security toolbox, but it is not the only one. 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 researchers have complied with the prohibition. 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 thereafter. Building on these efforts, NSF has implemented additional external research security requirements. These include mandatory research security training, annual reporting of foreign gifts and contracts in excess of $50,000, and a prohibition on institutions maintaining contracts with Confucius institutes. Together, these policies strengthen NSF's ability to identify and mitigate research security risks.

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

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

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

Research/Small Business Technology Transfer (SBIR/STTR) Programs' due diligence reviews and to assess NSF proposals in key technology areas for research security issues.

The NSF Trusted Research Using Safeguards and Transparency (TRUST) framework is a key component of NSF's efforts to strengthen research security while preserving the openness that underpins the U.S. scientific enterprise. The TRUST framework provides a structured, risk-based process for assessing grant proposals for potential national security considerations through three complementary review areas: (1) evaluating active personnel appointments and affiliations – a review area strengthened by the policy announced in the aforementioned DCL, which prohibits such affiliations; (2) identifying potential noncompliance with disclosure and other applicable requirements; and (3) assessing foreseeable national security considerations associated with proposed research activities. NSF is implementing the TRUST framework through a deliberate, phased approach designed to ensure consistent, effective, and scalable implementation. The initial phase, launched in FY 2025, focused on quantum information science proposals to validate processes and inform future expansion. Building on the success of that pilot, NSF expanded the framework in FY 2026 to include numerous programs within the Directorate for Technology, Innovation and Partnerships (TIP). Beginning in late FY 2027, NSF anticipates further expanding TRUST to additional critical research programs, as resources permit, while continuing to incorporate lessons learned and operational improvements from earlier phases. This approach enables NSF to strengthen research security, protect taxpayer investments, and ensure that federally funded research advances U.S. scientific leadership in a manner that is both secure and transparent.

The NSF Safeguarding the Entire Community of the U.S. Research Ecosystem (SECURE) Program, established in response to Section 10338 of the CHIPS and Science Act, seeks to better equip 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 and research security risks, provides training, webinars, and other resources for the community, and promotes collaborative development of tools and resources to mitigate research security risks. For example, the weekly research security briefings and recently introduced webinar series each reached thousands of stakeholders from the U.S. research community. SECURE Analytics is another critical component of the SECURE Program, with a focus on providing in-depth risk landscape analyses and the development of advanced analytics tools for due diligence processes. The initial release of the due diligence tool, ARGUS, is scheduled for later this month, with follow-on releases offering enhanced features.

Programmatic oversight includes frequent NSF engagement with the principal investigators and project staff for discussion of progress against plans, demonstration of working prototypes and review of draft products, in addition to the usual tracking of project spending and performance reporting through interim and annual reports. NSF also conducts annual site visits for both projects to assess performance, provide feedback to each project on deliverables, and to advise on technical or policy issues.

NSF also established the Research on Research Security (RoRS) Program to advance the holistic understanding of the full scope, potential, challenges, and nature of the 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.

Accountability is also vital to NSF's research security efforts, and NSF works very closely with its OIG in this regard. An independent oversight office, 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 ensuring awardee proposals and project reports contain information 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.

NSF has taken, and will continue to take, swift action in response to OIG referrals. When an OIG investigation is complete, they will refer it to NSF for action. Depending on the referral, NSF may suspend an award, terminate an award, and/or suspend or debar the individual researchers on a particular award. Through these efforts, NSF has imposed 16 governmentwide debarments/voluntary exclusions, 17 governmentwide suspensions, terminated 20 awards, and suspended 72 awards. Collectively, NSF has recovered, put to better use, or protected from misuse over $20M.

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. NSF is working with the Intelligence Community and other Federal agencies to identify when US-funded researchers are being targeted through foreign talent programs, undisclosed appointments, or misleading collaboration offers. Funding agencies have a distinct advantage as disclosure data from proposals and current-and-pending support forms can be analyzed at scale to detect undisclosed affiliations and overlapping funding. NSF's analytics work in this area helps identify risks early, so cases can be addressed through outreach or corrective action rather than only after damage is done.

Cultivating a Domestic Science and Technology Workforce

NSF's research security strategy also includes proactive actions to out-innovate adversaries by cultivating a domestic STEM workforce. NSF plays a central role in expanding the pipeline of U.S. STEM talent from K-12 to Ph.D. and postdocs to early career researchers, to ensure that Americans produce the world's most consequential research. For example, the NSF Graduate Research Fellowship Program, which is focused on U.S. citizens and permanent residents, funded the largest class ever this year.

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 and continued partnership 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.