Dr. Rebecca Keiser

Chief of Research Security, Strategy, and Policy

U.S. National Science Foundation

Before the

Committee on Science, Space, and Technology

United States House of Representatives

"Examining Federal Science Agency Actions to

Secure the U.S. Science and Technology Enterprise"

February 15, 2024

Chairman Lucas, Ranking Member Lofgren, and Members of the Committee, my name is Dr. Rebecca Keiser, and I am the Chief Officer for Research Security, Strategy, and Policy at the U.S. National Science Foundation. It is a privilege to appear before you today to discuss how the National Science Foundation is working to secure the nation's research enterprise and protect the taxpayer investments that are critical to advancements in science, technology, engineering, and mathematics (STEM), and STEM education research while promoting principled international research collaborations.

Established by the National Science Foundation Act of 1950 (P.L. 81-507), the U.S. National Science Foundation (NSF) is an independent federal agency 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." NSF is unique in carrying out its mission by supporting research across all fields of STEM, and at all levels and settings of STEM education.

At this time of intense global competition, securing the nation's research enterprise is an essential part of meeting the agency's mission, and it is essential to our nation's economic and national security. NSF works closely on this effort with our agency counterparts, including the Departments of Energy and Defense, the National Institutes of Health (NIH), and the federal law enforcement and intelligence communities. The agency does so while emphasizing the importance of balancing research security with international collaboration and the nation's ability to attract and retain global talent. NSF has worked quickly to address an age of new threats and challenges, dedicating considerable effort and resources to raise awareness of these threats and to implement needed

requirements, training, and oversight. NSF's efforts have led to ongoing initiatives aimed at clarifying proposal preparation and award administration requirements, as well as the issuance of new policies and directives in the proposal and award process. The agency has also focused on providing tools and assistance to the U.S. research community as we have a shared responsibility to safeguard our research enterprise. The agency has developed training modules for both federal and academic personnel and built new analytic capabilities to help us monitor vulnerabilities.

NSF appreciates the leadership of Congress and this Committee in addressing this challenge, and the agency has moved swiftly to implement applicable requirements of the CHIPS and Science Act of 2022 (P.L. 117-167,), and the FY 2020 and FY 2021 National Defense Authorization Acts.

Overview of Research Security

In 2019, NSF commissioned a report by the JASONs, a group of U.S. scientists who are uniquely qualified to conduct studies in security matters for the federal government and who possess a strong connection to the research enterprise. The findings of that report and its recommendations have been invaluable to NSF's approach to research security. The JASON report underscored the contributions and critical role that foreign-born scientists and engineers training and working in the United States have made to the nation's preeminence in science, engineering, and technology today. Their recommendations left no ambiguity that the U.S. should maintain a leading position to attract and retain the best global science and engineering talent. However, the JASON report also found that a small 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.

In 2019, the United States Government acted by standing up the National Science and Technology Council (NSTC) Research Security Subcommittee. The purpose of the Subcommittee is to coordinate Federal Government efforts to enhance the security and integrity of America's science and technology research enterprise without compromising American values or the openness, transparency, and reciprocity, which must be upheld for the research and innovation ecosystem to flourish. The Subcommittee includes subject matter experts from 18 departments, agencies, and offices in the Executive Office of the President. These experts identified critical emerging technology subfields, which their home organizations determined may be critical to U.S. national security. NSF co-chairs this Subcommittee with the White House Office of Science and Technology Policy (OSTP), the Department of Energy (DOE), and the NIH. In that role, NSF has helped lead the implementation of National Security Presidential Memorandum 33 (NSPM-33), which put in place new standards and requirement to uphold U.S. values in the research enterprise.

In 2020, NSF created a Chief of Research Security, Strategy and Policy (CRSSP) position – the position I currently hold. This position was codified in the CHIPS and Science Act of 2022, which also called on NSF to create an Office of the Chief of Research Security, Strategy and Policy (OCRSSP). The OCRSSP leads NSF's efforts to safeguard the research enterprise, developing policies and guardrails that balance the security of federally funded research with initiatives that maintain an open and collaborative international research environment; 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.

Federally funded organizations also have a role as stewards of that research. Organizations receiving federal funding 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. Ultimately, research security is about protecting American competitiveness. Ethical behavior is foundational to the conduct of research, and it can only be achieved when everyone can collaborate in an open environment, shielded from the threats of dishonest and unethical behavior that can be caused by undue foreign influence.

Safeguarding Taxpayer Investments

The future of U.S. competitiveness requires that we safeguard critical investments and take steps to address research security while also cultivating vibrant international partnerships that are critical to success. NSF plays a leading 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 already 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 in the process of becoming a citizen; barring NSF staff from participating in foreign talent recruitment programs; and, requiring an annual "Science and Security Training" for all NSF employees.

In January 2022, the National Science and Technology Council's Research Security Subcommittee issued implementation guidance for NSPM-33. A key effort in the Implementation Guidance was the harmonization of disclosure requirements across the Federal government for those applying for research and development funding. NSF and NIH stewarded these harmonized disclosure forms and they have been approved by OMB and are now in effect, adding transparency and consistency in the federal funding process.

Over the past year, with the increased funding the agency received in the FY 2023 Omnibus Appropriations Act, NSF has moved swiftly and made significant progress in implementing Research Security provisions contained in the CHIPS and Science Act. NSF implemented the prohibition on funding for researchers that participate in a malign foreign talent program, as defined in the CHIPS and Science Act. 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, the 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.

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

Consistent with the agency's published System of Records Notice[2] NSF has also established new analytic capabilities to proactively identify conflicts of commitment, vulnerabilities of pre-publication research, and risks to the merit review system. In 2023, NSF published[3] how it approaches these practices. The guidelines include a breakdown of which agency personnel may conduct research security-related activities; what activities to monitor proposal and award disclosures are allowed and with what resources they are conducted; how information will be validated to ensure accuracy; and how information may be shared within NSF and externally. As directed by the CHIPS and Science Act, NSF will scale up the use of these analytics and contribute to NSF's Small Business Innovation Research due diligence process in FY 2024.

NSF is in the process of establishing the Research Security and Integrity Information Sharing and Analysis Organization called for in the CHIPS and Science Act. Called SECURE, this center will provide needed information and tools to the research community. Full proposals for SECURE were due at the end of October 2023, and NSF is currently reviewing those proposals and we expect to make an award this summer. NSF is confident that we will be able to establish an innovative center that will build the capacity of the research community to make risk-informed decisions and create a trusted partnership on research security between research-awarding agencies and the research community, thus strengthening the security of our national research enterprise as envisioned by the law.

NSF, in partnership with the interagency community, including the Departments of Defense and Energy, and the NIH, developed research security training modules for the research community. On January 30th, NSF launched four interactive online research security training modules, now available to researchers and institutions across the U.S. These modules are designed to facilitate principled international collaboration in an open, transparent and secure environment that safeguards the nation's research ecosystem. These training modules signify a major first step in reconciling the needs of the research, law enforcement, and intelligence communities to pursue trusted relationships in the global research community while minimizing economic and security risks. They provide researchers with clear guidelines and effective strategies to protect against existing and emerging research security threats.

Furthermore, NSF has launched a new program specifically designed to study the field of research security, following the federal requirements outlined in NSPM-33 and its accompanying implementation guidelines. The Research on Research Security Program will help us understand the full nature, scope, challenges, and potential of this important field and its critical areas, including cybersecurity, foreign travel security, research security training, and export control training. The program will specifically fund projects that assess the methods for identifying research security risks and the strategies for preventing and mitigating them. Along with raising awareness for the field, this research will inform the development of best practices for research communities, offering guidance to researchers on how to protect their work, enhance transparency and collaboration, and responsibly disclose research findings and other proactive steps to ensure the integrity of our nation's research model. There is significant international partner interest in this research program and NSF will hold a workshop this spring.

[2] https://www.federalregister.gov/documents/2021/11/09/2021-24487/privacy-act-of-1974-system-of-records
[3] https://new.nsf.gov/research-security/guidelines

NSF coordinates its activities with OSTP, DOE, NIH, and other departments and agencies, including the Department of Justice and members of the Intelligence Community. In addition, NSF works very closely with its Office of the Inspector General (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. NSF partnered with the Office of the Director of National Intelligence to develop the Safeguarding Science Toolkit[4], an online resource for the community with information about research security and sensitive technology areas. And NSF is a member of the National Counterintelligence Task Force (NCITF) so that our agency can coordinate with both other civilian and DoD science agency partners and the intelligence community through NCITF on research security issues.

Conclusion

Safeguarding taxpayer investments in research and innovation is central to the nation's global leadership in STEM. NSF welcomes and encourages international collaboration with like-minded partners and views it as essential to pursuing the frontiers of science. 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. This partnership must strike a balance that safeguards the security and integrity of current and future independent and collaborative scientific efforts; conducts appropriate risk assessments that ensure the research enterprise continues to operate with the highest integrity; and ensures U.S.-based researchers and research organizations have the tools and support they need to continue the world-class innovation that has made the American research enterprise a leading contributor to our nation's economic and national security.

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 necessary authorities and tools to identify and mitigate risks and to put strong requirements in place. As good stewards of American taxpayer funds, we stand ready to take immediate action to safeguard these investments

[4] https://www.dni.gov/index.php/safeguarding-science

when we see new threats arise and we look forward to continuing to work with you on this vitally important issue.

Thank you for the opportunity to testify before you today. I look forward to answering any questions you may have.