National Science Foundation
Office of the Director
Office of the Chief of Research Security Strategy and Policy
June 5, 2024

Trusted Research Using Safeguards and Transparency (TRUST)

For nearly 75 years, the National Science Foundation (NSF) has funded science and engineering that has had enormous benefits for society, including our economic competitiveness and national security. As we adapt to today's ever-changing landscape of threats, we remain steadfast in holding to our core identity as the only federal agency that supports fundamental research across all science disciplines and as the leading federal agency in training the next generation of top scientists and innovators.

In today's evolving geopolitical environment, a major factor in enabling U.S. science to advance apace is to ensure it is protected against efforts by foreign governments to undermine our federal proposal and award process, to gain access to early-stage prepublication information and methods, to unfairly tip the scales in the global competition for STEM talent, to coerce otherwise honest researchers to deceive their employer and funding agency, and to even outright steal and commercialize U.S. funded early-stage technology. There is no question that these efforts are harmful to American science and to NSF's ability to carry out its mission. Furthermore, while threats to any given project can compromise the integrity and reliability of those research outcomes, such threats, if left unchecked, could compromise public trust in NSF as a responsible steward of taxpayer funding and could even undermine public trust in science as a whole.

In the face of these threats, there can be an understandable impulse to turn inward. To close ourselves off from the threat, to stop collaborating with certain countries and individuals and to prevent students and researchers from certain parts of the world from visiting and contributing their talents to our innovation ecosystem. For years now, NSF has been consulting with experts to help shape NSF's posture toward mitigating risks posed by potential foreign influence. In a seminal report published in 2019, Fundamental Research Security, the JASON highlighted that for NSF to adopt a closed-off approach would be a mistake. The JASON found that foreign-born scientists and engineers in the United States make essential contributions to U.S. preeminence in science, engineering and technology, and it is imperative to continue attracting and retaining such talent if we are to maintain our global leadership.

It is with this in mind that the Office of the Chief of Research Security Strategy and Policy (OCRSSP) is proud to announce the next stage in our efforts to safeguard our research ecosystem by identifying potential undue foreign influence in NSF-funded projects. We have designed a research security risk management framework with NSF's core science mission as a guide. Our approach to mitigating risks to the integrity and security of NSF-funded research is first and foremost focused on respecting the science, on finding ways to get to "yes". This means working collaboratively with institutions to identify minimally disruptive risk mitigation measures, wherever possible, so we can allow researchers to continue to do their work and continue to collaborate internationally. This framework represents a major development in NSF's goal of fostering a culture of shared responsibility in research security, rather than one focused solely on strict compliance. In short, NSF will use information provided in proposal submissions and elsewhere to assess risk on a project-by-project basis so that NSF can work collaboratively with the community to safeguard science.

In pursuing the TRUST effort, NSF will maintain a steadfast focus on:

- Avoiding the curtailing of beneficial activities due to risk aversion or overly broad interpretation of policy;
- Protecting the core values of fairness and due process; and
- Maintaining open lines of communication with the community.

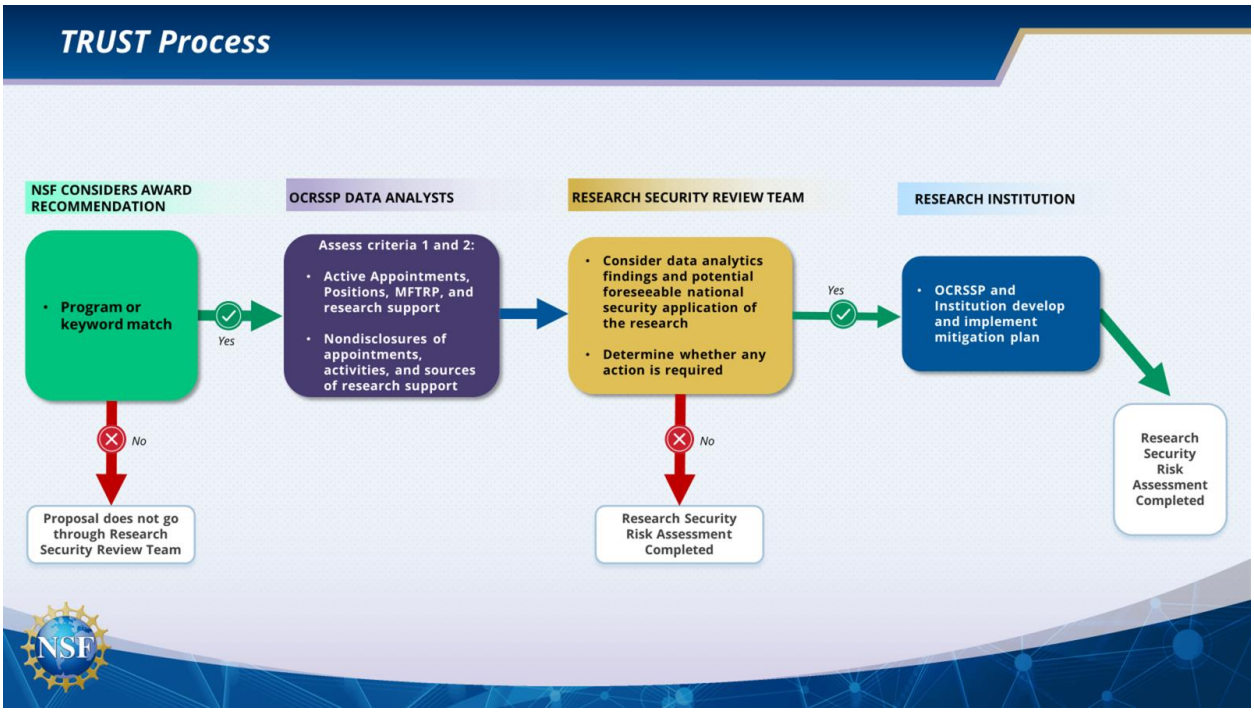
The TRUST Framework

The name of the framework we are announcing today reflects the values that will be embedded throughout its implementation. *Trusted Research Using Safeguards and Transparency (TRUST)* is a decision tree approach to assess research proposals and ongoing projects for concerning appointments and research support, non-compliance with disclosure and other requirements, and potential risks to national security.

The TRUST decision tree includes three branches, one focused on assessing active appointments, positions, and research support, and a second focused on identifying instances of nondisclosure. Projects moving through either of those branches will follow similar progressions – first the OCRSSP team will conduct an analysis using proposal submission and other data to flag areas of potential concern. The OCRSSP team will then assess whether any flagged proposals warrant engagement with the awardee institution to gather additional information and consider whether risk mitigation and management may be required.

The third branch of the TRUST decision tree represents a significant new effort for NSF, with the inclusion of national security considerations, which was congressionally mandated in the *CHIPS and Science Act of 2022* and the Fiscal Year 2023 Appropriations bill. In response to these congressional requirements, NSF commissioned a report by the JASON, Safeguarding the Research Enterprise, to provide recommendations to NSF on how to approach identifying research areas of concern that could pose potential national security risks. The findings and recommendations from this report helped inform NSF's development of the third branch of the TRUST risk management framework. NSF appreciates Congress's sustained, thoughtful engagement on these issues, and we remain eager to continue partnering on ways to approach this dynamic set of threats to U.S. research.

Thus, the third branch of the TRUST decision tree starts with the convening of a Research Security Review Team. This team, made up of 5-6 members is comprised of relevant NSF program office staff, OCRSSP staff, NSF subject matter experts, and (as needed) other U.S. Government national security experts who will serve as observers and provide guidance. The Review Team will review the results of the analyses from the first two branches and assess potential foreseeable national security concerns. If the Review Team determines that there is sufficient national security risk associated with the project, or if they confirm a concern raised in the first two criteria, OCRSSP staff and the awardee institution will work collaboratively to gather additional information that can inform the exploration of the necessity and options for mitigating those risks.



TRUST Implementation

The rollout of TRUST will take place in three phases, enabling OCRSSP to build on lessons learned as we go, including those related to institutional burden, fairness, time-to-award delays, etc. The phases will proceed as follows:

1) Beginning in fiscal year (FY) 2025, the first phase is a pilot program in which the TRUST framework will be applied to quantum-related proposals after they undergo merit review. The purpose of the phase 1 pilot is to start collecting data, assess key metrics of the program, understand the impact on NSF directorates, and build and evaluate NSF's capacity to review the potential foreseeable national security application of technology.
2) The second stage of the rollout will be focused on implementing lessons learned from the quantum pilot. OCRSSP will also explore the need for making policy updates, including to the Proposal Awards Policy and Procedures Guide (PAPPG). During this stage, the pilot will be expanded to include other *CHIPS and Science Act* key technology areas.
3) The third and final stage of the pilot will focus on scaling up and streamlining the review process as well as expanding the scope of projects to include all *CHIPS and Science Act* key technology areas.

As we progress through this pilot program, we will rely on the research community to voice their concerns to help us learn what is working and what is not. We intend to create formal opportunities for the community to engage directly with OCRSSP staff on this pilot. We will host a series of interactive webinars with a Q&A discussion with participants. The first two of these webinars will be held Tuesday, June 11 at 11am and Thursday, June 20 at 2pm. Registration information for the webinars can be found at the link here. OCRSSP staff are also more than happy to visit institutions directly to hear from administrative staff as well as faculty and students to gain a more holistic understanding of the challenges institutions face as they prepare to engage with the TRUST framework. Finally, we are establishing a dedicated email address for interested parties to submit questions or comments: trust@nsf.gov .

NSF looks forward to an open and engaging dialogue and to working closely with the research community as we strive to foster an inclusive, thoughtful, and vigilant research security culture; one that both safeguards and promotes our world-renowned research and innovation enterprise.