Stony Brook University

# Research Security Program

Dear Researchers,

The Research Security Program would like to bring some recent U.S. government and federal sponsor agency actions to your attention. Many of these actions span across multiple federal sponsor agencies and may require additional action on your part.

## National Science Foundation (NSF) Enhances Research Security with New TRUST Proposal Assessment Process

NSF News, June 5, 2004

The U.S. National Science Foundation has announced a new risk mitigation process, the Trusted Research Using Safeguards and Transparency (TRUST) framework, which will guide the agency in assessing grant proposals for potential national security risks. The revised procedures will help safeguard U.S. taxpayer investments in research and innovation while strengthening international collaboration.

Developed by the NSF Office of the Chief of Research Security Strategy and Policy (OCRSSP), the TRUST framework includes three branches.

- First branch focuses on assessing active personnel appointments and positions;
- Second branch focuses on identifying instances of noncompliance with disclosure and other requirements; and
- Third branch is the inclusion of a review for potential foreseeable national security considerations.

The framework is designed to avoid curtailing beneficial research activities due to institutions or individuals in the community being overly cautious, protect the agency's core values of fairness and due process and maintain open lines of communication with the research community. Read the full NSF article here

TRUST will have a three phase roll-out:

- 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 second stage of the rollout will be focused on implementing lessons learned from the quantum pilot.
- 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.

## Reminder - Other Federal Agency Risk Reviews

Department of Defense (DOD), Risk-based security reviews of Fundamental Research

"Countering Unwanted Foreign Influence in Department-Funded Research at Institutions of Higher Education" provides for risk-based security reviews of Fundamental Research that

assesses four factors for prinicipal investigators and other key personnel:

- Participation in foreign talent recruitment programs;
- Current or prior funding from “foreign countries of concern” (FCOCs). FCOCs are currently defined as China, Russia, North Korea, and Iran per section 10612 of the CHIPS Act of 2022;
- Filing a patent in an FCOC or on behalf of an FCOC-connected entity, or in a non-FCOC country without disclosure; and
- Associations or affiliations with organizations on U.S. Entity (trade restriction) and other indicated lists (see SBU page Restricted Party Screening)

### National Institutes of Health (NIH), Foreign Component

NIH requires prior approval for a foreign component (NOT-OD-19-114), A foreign component is the existence of any “significant scientific element or segment of a project” outside of the United States, in other words:

- Performance of work by a researcher or recipient in a foreign location, whether or not NIH grant funds are expended; and/or
- Performance of work by a researcher in a foreign location employed or paid for by a foreign organization, whether or not NIH grant funds are expended.

Activities that would meet this definition include, but are not limited to, (1) the involvement of human subjects or animals, (2) extensive foreign travel by recipient project staff for the purpose of data collection, surveying, sampling, and similar activities, or (3) any activity of the recipient that may have an impact on U.S. foreign policy through involvement in the affairs or environment of a foreign country.

Examples of other grant-related activities that may be significant are:

- Collaborations with investigators at a foreign site anticipated to result in co-authorship;
- Use of facilities or instrumentation at a foreign site; or
- Receipt of financial support or resources from a foreign entity.

## U.S. Government Lists: Restricted Parties

On May 9, 2024 the U.S. Department of Commerce, Bureau of Industry and Security announced that new institutions and organizations were added to the Entity List.

- 22 institutes (universities and institutes)  and firms were added for participation in China’s quantum technology advancements and for acquiring or attempting to acquire U.S.-origin items to enhance China’s quantum capabilities.
- Four entities were added for acquiring or attempting to acquire U.S.-origin items to be used by China’s military for its unmanned aerial systems (UAS).
- 11 entities were added for involvement in China's High Altitude Balloon program.

Reminder that international collaborators (including potential co-authors) should be screened against the U.S. Government’s Lists for parties of concern. Individuals may use the tools available on the Export Controls website to identify parties on these lists.

Learn more about the U.S. Government Restricted Parties Lists

## Remember to contact the Research Security Program if:

- You are, or think you may be, involved in a Malign Foreign Talent Recruitment Program.
- You are approached by a Malign Foreign Talent Recruitment Program.

- You have an award from, or have submitted/or plan to submit a proposal to, a federal sponsor agency and have collaborated on publications/projects with an 1286 List entity/program (pages 18-21 of the "Countering Unwanted Foreign Influence in Department-Funded Research at Institutions of Higher Education" document) or on a U.S. Government Restricted Party List.
- Your research involves a critical and emerging technology and you have accepted a restriction on publications/dissemination or foreign national involvement, verbally or in writiing.

**Questions**

Contact the Research Security Program

Visit the Research Security Program website

Thank you,

Susan Gasparo

Director of Research Security Office of the Vice-President for Research