NSPM-33 Implementation Guidance and CHIPS+Science Research Security Provisions

Presentation to COGR

Rebecca Keiser

Chief of Research Security Strategy and Policy

National Science Foundation

October 20, 2022

NSF Research Security Efforts

- Make disclosure requirements as clear and understandable as possible
- Use data analytics to understand the scale and scope of the issues
- Encourage international collaboration as distinguished from improper foreign government influence
- Partner with the research community and the U.S. government interagency community to address risks

Summary of NSF-77: Data Analytics Application Suite

The System of Records Notice (SORN) NSF-77 “Data Analytics Application Suite” expands the allowed uses of NSF’s internal data. It enables the aggregation, linkage, and analysis of information reported by individuals and organizations participating in NSF-supported activities along with published information related to the research enterprise. This is the process under the Privacy Act.

NSF-77 enables NSF to address top priorities by:

- Connecting funding outcomes and understanding of the scientific enterprise.
- Improving NSF’s understanding of diversity equity and inclusion activities and programs.
- Improving research security coordination and assuring accuracy and fairness.
- Empowering strategic planning, collaborations, and program development.

Potential International Collaboration Questions-1

- Describe the engagement succinctly and without jargon. Is it fundamental research? If not, what are the institution’s policies around creating the engagement?
- Are the terms of the engagement made clear in writing? Have all the participants been identified? Are all participants known to the PI and the PI’s institution?
- Are all the participants’ conflicts of interest and commitment documented? Are there any aspects of the engagement that are not to be disclosed to any of the participants? If so, what is the reason?
- Is there any aspect of the engagement that seems unusual, unnecessary or poorly specified?
- Where does the funding and other resources needed for the activity come from? Is it clear what each party is providing?

Potential International Collaboration Questions-2

- Are all the tangible assets of the engagement, existing or to be generated (e.g., data, metadata, profits, equipment, etc.), known? How will they be shared? Who decides how they are allocated?
- How does a participant end their engagement?
- Are scholars expected to reside away from their home institutions as a part of the engagement? If so, how are they chosen for participation in the engagement?
- What are the reporting requirements back to home institutions or organizations?
- Who will control the dissemination of the resulting fundamental research?

[i] Report | NSF-Commissioned JASON Report JSR-19-21 | "Fundamental Research" | 6 December 2019 |pp. 34-36 | https://www.nsf.gov/news/special_reports/jasonsecurity/JSR-19-2IFundamentalResearchSecurity_12062019FINAL.pdf |accessed 14 May 2020 | JASON is an independent group of scientists which advises the US Government on matters of science and technology and is administratively managed by the MITRE Corporation.

NSPM-33 Implementation Guidance

- **Disclosure Policy** — ensuring that federally-funded researchers provide their funding agencies and research organizations with appropriate information concerning external involvements that may bear on potential conflicts of interest and commitment;
- **Oversight and Enforcement** — ensuring that federal agencies have clear and appropriate policies concerning consequences for violations of disclosure requirements and interagency sharing of information about such violations; and,
- **Research Security Programs** — ensuring that research organizations that receive substantial federal R&D funding (greater than $50 million annually) maintain appropriate research security programs.

Status of NSPM-33 Efforts

- Federal Register notice for standardized disclosure requirements and formats out for public comment
- Standards and certification process for research security programs: in work, out for public comment by end of year
- Awards for research security training modules: announcement November 1

CHIPS + Science Research Security Provisions

Several research security provisions including:

- Prohibition of malign foreign government talent recruitment programs
- Requirement to establish a Research Security and Integrity Information Sharing and Analysis Organization
- Research security training requirement for all covered personnel
- Inclusion of research security training as part of Responsible and Ethical Conduct of Research training
- Reporting on foreign financial transactions and gifts
- Prohibition of Confucius Institutes

Malign Foreign Talent Recruitment Program Definition in CHIPS + Science

Program, position or activity that requires an individual to take on the following:

- Unauthorized transfer of intellectual property or other nonpublic information;
- Recruit trainees or researchers to enroll in such program;
- Establishing a laboratory/employment/appointment in a foreign country in violation of terms and conditions of a Federal research award;
- Inability to terminate;
- Overcapacity/overlap/duplication;
- Mandatory to obtain research funding from the foreign government’s entities;
- Omitting acknowledgement of U.S. home institution/funding agency;
- Not disclosing program participation;
- Conflict of interest/commitment; or
- Sponsored by a country of concern

Helpful Links

Federal Register notice for the standardized disclosure instructions and formats: NSTC Research Security Subcommittee NSPM-33 Implementation Guidance Requirements & Standardization (nsf.gov)

OSTP blog post providing the research community with an update on OSTP research security efforts: An Update on Research Security: Streamlining Disclosure Standards to Enhance Clarity, Transparency, and Equity - The White House

ODNI Safeguarding Science resource: Safeguarding Science (dni.gov).