Research Security Training for the United States (U.S.) Research Community

Solicitation NSF 22-576

Community Webinar
Rebecca Keiser, Chief of Research Security Strategy and Policy (CRSSP)
April 20, 2022
Topics Covered

• Background on NSPM-33 and Implementation Guidance
• Solicitation Basics
• Training Module Requirements
• Module Development & Content
• Review Criteria
• Some FAQs
• Summary
Background: NSPM-33 (January 2021)

• NSPM-33 directs action to address risks to United States Government-supported Research and Development (R&D) caused by foreign government interference and exploitation.

• The memo defines roles and responsibilities of those who significantly influence U.S. R&D to address research security.
Background: NSPM-33 Implementation Guidance (January 2022)

- Published by the Subcommittee on Research Security (NSTC/JCORE)

- Key Components of the 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.
Context: Research Security Program Elements

- Cybersecurity
- Foreign Travel Security
- Research Security Training
- Export Control Training, as appropriate
NSF Solicitation 22-576: Research Security Training for the United States (U.S.) Research Community

• **Co-sponsors:** NSF, DoD, DOE, and NIH
  - Solicitation administered by NSF on behalf of the sponsors

• **Program Goals:**
  - **Finding a balanced approach to research security:** “With the goal of strengthening research security in the U.S., NSF is working in partnership with three other federal research funding agencies to find a balanced approach to research security. This effort includes the development and implementation of training—to recipients of federal research funding—in best practices to optimize research security.”
  - **Mitigating foreign government risks and threats:** “This training is an essential step toward mitigating foreign government risks and threats to U.S. government-funded research and may be used to fulfill the research security program requirement in NSPM-33.”
NSF Solicitation 22-576: Research Security Training for the United States (U.S.) Research Community (cont.)

• **What It Is:**
  • *About:* A call for proposals to develop training modules for research security (one module per proposal)
  • *Funding:* Total funding amount: $1.5 million for 1-3 awards. Funding to be administered via cooperative agreements, with substantial involvement anticipated with the collaborating federal funding agencies
  • *Proposal Deadline:* May 23, 2022

• **What It Is Not:**
  • A call for the development of general research security programs
    • Training is only one component of a research security program
  • A call for operational implementation of the training modules
NSF Solicitation 22-576: Training Module Requirements

• Requirements:
  • The training module must be internet-based and widely accessible to the end user.
  • The training module must be scalable and flexible.
  • The training module must be designed to accommodate new modules.

• Each training module proposal must address ONE of the four topical areas:
  1. Why is research security an important issue?
  2. What is a disclosure policy and how will it be used?
  3. What actions can federally funded research recipients take to manage and mitigate risk?
  4. Is international collaboration encouraged?

A proposer is authorized to submit separate proposals for more than one topical area.
NSF Solicitation 22-576: Training Module Development and Content

• **Consultation:** Recipients will be required to collaborate with a “content expert group”.
  • The “content expert group” consists of representatives from NSF, NIH, DoD, DOE, and FBI.

• **Expectations for Development of Training Modules**
  • Consultation sessions with target audience group
  • Administer system and content testing with focus groups
  • Rely on best practices and existing information on federal research security sector
  • Recipients determine training format incorporating best practices for education and training
  • On-line training must be accessible through widely available internet browsers
  • Develop and monitor success metrics
  • Each proposal shall include at ONE of the four topic modules

• **Delivery Date:** 12 months after start of cooperative agreement
Merit Review Criteria: NSF and Solicitation-specific Review Criteria

• NSF Merit Review Criteria
  • Intellectual Merit: Has the potential to advance knowledge
  • Broader Impacts: Has the potential to benefit society and contribute to the achievement of specific, desired societal outcomes

• Solicitation-specific Review Criteria
  • Innovation: Utilizes innovative approaches and latest best practices
  • Approach: Clearly states its goals, audience, and intended outcome; is based on sound rationale, educational concepts, and principles; has a sound evaluation plan; proposed modules are in a standard format and easily shareable
  • Environment: Scientific and educational environment of training will contribute to its expected goals; includes evidence of institutional commitment, collaboration among participating organizations
Some FAQs

• Should each proposal contain only one topical area?
• Can you provide more detail regarding the role of the “content expert group” and how collaboration with the recipient will work?
• Can “hosting” and “operating costs” of the modules be part of the proposal/budget?
• Is submission of separately submitted collaborative proposals permitted?
Summary

• NSPM-33 requires research security programs in all organizations receiving more than $50 million/yr. in federal research funding.

• Research security training is one component of such a program.

• NSF 22-576 is a multi-agency solicitation aimed at providing assistance to the research community in developing robust research security training capabilities.

• Federal agencies aim to partner with the research community to achieve outcomes that help the U.S. research and innovation ecosystem flourish.
Questions?
Additional Slides
Solicitation Topical Area 1: Why is research security an important issue?

Discuss the issues of research security and why research security for federally funded research is important for the U.S. government and national security.

• Seek to maintain vibrant science and engineering community for benefit of the nation

• Core principles and values: openness, transparency, reciprocity, collaboration, and integrity

• Challenge from some foreign governments seeking to misappropriate scientific research and recruit U.S. researchers through unethical means

• Some foreign talent recruitment programs disregard core principles
Solicitation Topical Area 2: What is a disclosure policy and how will it be used?

Explain federal funding agency disclosure policies; why this information is important and how it will be used.

• Emphasize and clarify information that must be disclosed
• Discuss identification of anomalies that might indicate transgressions
  • Conflicts of interest and conflicts of commitment
  • Undisclosed research duplication and researcher commitments to entities outside their U.S. employer
  • Compromises to the merit review system
  • Unauthorized use of pre-publication data and information
• Transparency and disclosure needed to assess risk and make sound funding decisions
• Potential criminal and civil ramifications for deliberate failure to make proper disclosures
Solicitation Topical Area 3: What actions can federally funded research recipients take to manage and mitigate risk?

Identify how organizations should demonstrate robust leadership and oversight; establish policies that promote transparency and guard against conflicts of interest and commitment, and more.

• Agencies alerting research community to risks to global research ecosystem
• Agencies coming together with researchers and administrators to share information and clarify requirements
• Policies to promote transparency and guard against conflicts of interest and conflicts of commitment
• Best practices
  1. Demonstrate organizational leadership and oversight
  2. Establish an expectation of openness and transparency
  3. Provide and share training, support, and information
  4. Ensure effective mechanisms for compliance with organizational policies
  5. Manage potential risks associated with collaborations and data
Solicitation Topical Area 4: Is international collaboration encouraged?

Emphasize that principled international collaboration is critical to success, but that improper foreign influence is a threat to international collaboration in the S&T enterprise. It will be important to distinguish the difference.

- Principled international collaboration:
  - Enables cutting-edge research that no nation can achieve alone
  - Trains a robust S&T workforce capable of solving global problems
  - Allows for significant contributions from international students and scholars to the U.S. research enterprise
  - Strengthens scientific and diplomatic relations
  - Leverages resources, including funding, expertise, and facilities
Additional Links and Resources

• **Program Solicitation** (Full Proposal Deadline: May 23, 2022)
  • Any proposal submitted in response to this solicitation should be submitted in accordance with the revised *NSF Proposal & Award Policies & Procedures Guide (PAPPG)* (NSF 22-1).

• **Presidential Memorandum on U.S. Government Supported Research and Development National Security Policy (NSPM-33)** (published January 2021)
  • **NSPM-33 Implementation Guidance** (published January 2022)