NSPM-33, CHIPS, and Research Security

FDP Fall Meeting (Remote)
September 19, 2023

FDP Foreign Influence Working Group (FIWG)
Foreign Influence Working Group; Science & Security Updates Description:

Representatives from NIH, NSF, DOD, and DOE will provide updates related to NSPM-33 and CHIPS Act initiatives, including the most recent iteration of the Common Forms for Current and Pending/Other Support and Biosketch. FDP updates from Listening Sessions held since the last meeting will also be covered, as will thoughts on upcoming activities.

Speakers: Rebecca Keiser and Jean Feldman, NSF, Michelle Bulls, NIH, Jason Day, DOD & Jeremy Ison, DOE
Ongoing Areas of Interest

- TikTok/ByteDance Ban of Federal Contracts
- Harmonization of Forms
- NIH Notice - International Subawards
- DoD – Countering Unwanted Influence in Department Funded-Research at Institutions of Higher Education
- NSF SECURE Proposal
- Research Security Program Security Requirements
- Research Security Program – FDP Priorities *(To be discussed)*
Values are the Heart of Research Security

Both OPEN And SECURE

- Rigor & Reproducibility
- Research Ethics
- Responsible Conduct of Research
- Research Integrity
- Research Security
The Chips and Science Act of 2022: Research Security

- The Chips and Science Act includes 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 (RSI-ISAO)
  - 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
Today's Geopolitical Environment is Challenging for Research
About SECURE

**Mission:**
Empower the research community to make security-informed decisions about research security concerns

**Approach:**
Providing information, developing tools, and providing services

**Audience:**
IHEs, non-profit research institutions, and small and medium-sized businesses
What SECURE will do... and won’t do

- Uniform Quality of Service
- Reduce Cost and Administrative Burden
- Frameworks and Best Practices
- Curated Syntheses
- Patterns of Risk
- Analytical Tools

Decisions, Investigations, Policy
Research on Research Security Program

JASON Findings

1. The issue of research security is real.

2. US researchers often feel threatened, frightened, and/or burdened by past and current actions to deal with problems of research security and integrity. Survey data indicate that these concerns are widespread and deep.

3. The consequences and appropriate actions related to breaches of research security differ among STEM fields.

4. The definition of research integrity differs across national interests and cultures.

5. The NSF internal project on the identification of potential breaches of research integrity and security through analysis of open-source data could lead to a useful product for dissemination to other federal, academic, and commercial organizations.

6. STEM Principal Investigators best understand the customs and practices of their discipline, and they can be important partners in a research program on research security. They should have the ability to decide when the products of research are ready for publication and public dissemination.

7. The success of an NSF program on research security will depend on NSF working with universities and private companies to make available their data on issues of research security in a protected manner that allows access to approved research programs on this topic and provides protection of the privacy of the sources.
1. The products of a research program on research security must not be used to disadvantage anyone based on their ethnic background or country of origin.

2. The NSF program should emphasize research on effective methods for informing and training Principal Investigators about potential risks in international collaborations by country and, where appropriate, by institution.

3. The NSF research program should encourage research projects in collaboration with international organizations that share our concerns for research security.

4. As part of the proposed research program, NSF should encourage collaborations between social scientists and other STEM researchers, for example, via cross-disciplinary workshops before and during research performance.

5. The NSF should work closely with US STEM professional societies to maximize access of research program awardees to STEM researchers and to disseminate educational and training materials.

6. NSF should work with other Federal agencies that have a major stake in unclassified basic and applied research to create a protected database of matters of breaches of research security at universities, private companies, and government laboratories, which can be accessed by approved researchers in the NSF research program on research security while maintaining the privacy of the sources.
FDP Session on NSPM-33, CHIPS, and Research Security

Jean Feldman, Head, Policy Office
Presentation to Federal Demonstration Partnership
September 19, 2023
NIH Update for Federal Demonstration Partnership (FDP) on Research Security

Michelle Bulls
National Institutes of Health (NIH)
Director, NIH Office of Extramural Research

FDP Session on NSPM-33, CHIPS, and Research Security
September 19, 2023
Policy for Risk-Based Security
Reviews of Fundamental Research

Federal Demonstration Partnership Meeting

Jason Day
Research Policy Director
OUSD(R&E)

9/19/2023
Outline

• Fundamental research and the open research enterprise
• Policy on risk-based security review processes pursuant to National Security Presidential Memorandum-33
  - New risk-based security review policy
  - DoD Component risk-based security reviews
  - Mitigation or rejection decisions
  - Oversight by the Office of the Under Secretary of Defense for Research and Engineering
  - Decision matrix
  - 1286 lists
• This brief is focused solely on proposals for fundamental research conducted by academic institutions. This means:
  - Research that is largely free from restrictions such as publication reviews or restrictions on foreign nationals.

• Fundamental research and open international collaborations are invaluable for scientific creativity that enables the DoD to maintain a competitive research advantage.

• The Department is enacting risk-based security reviews of fundamental research projects to comply with National Security Presidential Memorandum - 33
• The Deputy Secretary of Defense signed a memorandum on 14 Dec 2022 on National Security Presidential Memorandum – 33 Implementation

• The Office of the Under Secretary of Defense for Research and Engineering (OUSD(R&E)) is directed to ensure a consistent implementation of NSPM-33 across the Department and to ensure the Department’s policies are aligned with the interagency and OSTP
The Countering Unwanted Foreign Influence in Department-Funded Research Institutions of Higher Education policy and enclosures was publicly released June 30, 2023.

Policy for risk-based security reviews of fundamental research
- Intent is to ensure consistent application of risk-based security reviews for fundamental research project proposals across the DoD.

DoD Component Decision Matrix to Inform Fundamental Research Proposal Mitigation Decisions
- A guide to assist program managers and DoD components in reviewing fundamental research proposals for potential conflicts of interest and conflicts of commitment.

FY22 Lists Published in Response to Section 1286 of NDAA 2019
- The 1286 List includes foreign institutions that have been confirmed as engaging in problematic activity as described in Section 1286(c)(8)(A) of the NDAA for FY 2019, as amended. It also identifies the foreign talent programs that have been confirmed as posing a threat to the national security interests of the United States as described in Section 1286(c)(9)(A) of the NDAA for FY 2019, as amended. Per the Decision Matrix, certain engagements with these institutions will require mitigation before a proposal can be funded.


The Department is committed to preserving open science, international collaboration, and involvement of talented foreign students and researchers in DoD-funded fundamental research.

The Department’s policy is to mitigate potential conflicts of interest listed in the Decision Matrix to the maximum extent possible.

Policy implementation will be transparent and consistent across the Department.

The Department will not discriminate on the basis of race or national origin.

The Department will not penalize researchers for activities believed acceptable prior to the USD(R&E) Griffin Letter to Academia, dated 10 October 2019.

The Department is interested in collecting feedback from the academic community as it implements its policy. The decision matrix may be updated to incorporate changes in law and policy, account for lessons learned, and ensure consistency with other Federal agencies.
Every fundamental research proposal selected for award based on technical merit will undergo a risk-based review

Component policies must:

• Ensure a proposal is fundamental research
• Use the Decision Matrix
• Use the disclosures and Standard Form 424 submitted by the proposing institution for all covered individuals listed in fundamental research project proposals selected for award to identify potential research security risks and employ relevant publicly available information, at a minimum, to verify the information submitted in the disclosures and Standard Form 424
• Conduct annual reviews of funded research projects using the Research Performance Progress Report
• Not discourage international research collaboration
• Not impact time to award if no mitigation is necessary.
  - Working with the institution to mitigate conflicts of interest may result in additional time to award
• Define the level of research security risk mitigation determination that is appropriate for the components to follow their customary process to recommend and make funding decisions and when a decision by component leadership (or designee) is required
Mitigating potential risks

• Mitigation is the preferred option for Components to take concerning any risks uncovered

• Mitigation measure examples:
  - Require the covered individual(s) to complete insider risk awareness training;
  - Require increased frequency of reporting by the covered individual(s) through the Research Performance and Progress Report (RPPR);
  - Replace individuals listed in the fundamental research project proposal who are deemed a research security risk;
  - Provide DoD the covered individual's(s') contracts for review and clarity relationships, affiliations, and/or associations considered risky; and
  - Require the covered individual(s) to resign from positions deemed problematic by the risk-based security review.
• Denials shall only occur when risks are unable to be mitigated or if required by law

• Denials must be explained in writing to proposing institutions, including unclassified rationale

• Institutions may challenge a denial and OUSD(R&E) will mediate
OUSD(R&E) Oversight

• Denials must be reported to OUSD(R&E) and other Components

• Components shall provide OUSD(R&E) with a summary of risk-based security reviews including number of reviews, denials, and description of denials on an ongoing basis

• OUSD(R&E) may also conduct periodic spot checks independent of the Component process

• OUSD(R&E) must ensure that Components’ policies and implementation are in line with other Components’ and Federal agencies’ policies
Decision Matrix
• **Foreign talent recruitment programs** – is a way a Foreign Country of Concern (FCOC) corrupts the open research enterprise by conducting secretive dealings between recipients and the FCOC, including transfer of knowledge and personnel outside of norms
  - Malign foreign talent recruitment program – defined in CHIPS

• **Funding sources** – accepting funding from FCOCs may create a conflicting obligation to that FCOC

• **Patents** – patents arising from US–funded research filed in a foreign country before being filed in the U.S. can be an indicator of undisclosed agreements with a foreign country

• **Entity lists** – problematic actors that affiliation or association with could create a conflict of interest or conflict of commitment
  - Affiliation = Academic (not including undergraduate or graduate students), professional, or institutional appointments or positions with a foreign government or a foreign government-connected entity, whether full-time, part-time, or voluntary (including adjunct, visiting, post-doctoral appointment, or honorary), where monetary reward, non-monetary reward, or other quid-pro-quo obligation is involved.
  - Association = Academic (not including undergraduate or graduate students), professional, or institutional appointments or positions (including adjunct, visiting, voluntary, post-doctoral appointment, or honorary) with a foreign government or a foreign government-connected entity where no monetary reward, non-monetary reward, or other quid-pro-quo is involved.
1286 Lists

FY22 Lists Published in Response to Section 1286 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115-232), as amended
• The 1286 List includes foreign institutions that have been confirmed as engaging in problematic activity as described in Section 1286(c)(8)(A) of the NDAA for FY 2019, as amended. It also identifies the foreign talent programs that have been confirmed as posing a threat to the national security interests of the United States as described in Section 1286(c)(9)(A) of the NDAA for FY 2019, as amended.

- Table 1: List of Institutions of the People’s Republic of China, Russian Federation, and other Countries with Specific Characteristics
- Table 2: Foreign Talent Programs that Pose a Threat to National Security Interests of the United States

• Documentation on problematic behaviors engaged in by the institutions on the 1286 list can be found in USG published sources
  - Entities List
  - Justice Department Court Cases
• Contact the **Academic Liaison** for any questions / concerns / issues pertaining to research security at institutions of higher education at:

  osd.mc-alex.ousd-r-e.mbx.academic-liaison@mail.mil

• DoD research security information:
  - **Academic research security pertaining to fundamental research**
    Basic Research Office website at:
    https://basicresearch.defense.gov/Programs/Academic-Research-Security/
  - **Efforts to balance the promotion and protection of critical and emerging technology through the technology development cycle**
    Science and Technology Program Protection Office’s Maintaining Technology Advantage website at: https://rt.cto.mil/stpp/mta/#
  - **DoD’s public release of the Policy for Risk-Based Security Reviews**
    including the decision matrix and 1286 lists: Defense.gov:
DOE Office of Science: Research Security Policy Update

Virtual FDP Meeting - Science and Security Session

Jeremy Ison
Senior Policy Advisor at U.S. Department of Energy (DOE)
September 19, 2023
How can FDP help?

FIWG has spent the summer exploring this:

• Listening Session #1
• Listening Session #2
• Demo of MART with FBI representatives (upcoming)
• Identification of potential FDP demonstrations and early-stage prioritization (with RSS)

See FIWG Web Page for slides, videos, and documents:

https://thefdp.org/default/committees/research-administration/foreign-influence-working-group/
Our Suggestion (from Listening Session)

• **Use FDP to implement a Pilot** that would support:
  
  • Development, Demonstration, & **Sharing of Effective Practices**
  
  • **Multi-directional feedback throughout implementation from/to** federal partners and a variety of research institutions (large/small, public/private, higher education/research institutes, ERIs and HBCUs)
  
  • Ability to get direct feedback from **Faculty**.
  
  • **Evaluate the implementation & enforcement timeline** to ensure that the traditional institutional cycles (budget, technology development, training, hiring, culture change, etc.) have adequate time to develop the necessary resource support mechanisms.
<table>
<thead>
<tr>
<th>Demonstration Item (Top Impact Ranked listed first)</th>
<th>Impact</th>
<th>Feasibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>4. Create a glossary of federally defined terms with definitions adequate to guide institutional users in their implementation process.</td>
<td>86%</td>
<td>73%</td>
</tr>
<tr>
<td>9. Implement Research Security Training.</td>
<td>86%</td>
<td>55%</td>
</tr>
<tr>
<td>8. Define appropriate practices for identifying and addressing research security breaches and insider threats.</td>
<td>82%</td>
<td>41%</td>
</tr>
<tr>
<td>11. Matrix for the Assessment of Risk and Transparency (MART).</td>
<td>77%</td>
<td>68%</td>
</tr>
<tr>
<td>Demonstration Item (Top Impact Ranked listed first)</td>
<td>Impact</td>
<td>Feasibility</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------------------------------------------------</td>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>3. Determine mutually acceptable and feasible implementation timetables.</td>
<td>77%</td>
<td>64%</td>
</tr>
<tr>
<td>10. Identify effective practices for implementing flexible international travel options to meet the intent of the final standards.</td>
<td>77%</td>
<td>64%</td>
</tr>
<tr>
<td>5. Draft model research security program descriptions.</td>
<td>76%</td>
<td>81%</td>
</tr>
<tr>
<td>1. Work with federal agencies on the certification requirements and how to best implement them.</td>
<td>73%</td>
<td>77%</td>
</tr>
<tr>
<td>13. SciENCv (Assessment and Quantification of Researcher Use and Management of SciENCv for Biosketch and Current and Pending (Other) Support Forms).</td>
<td>73%</td>
<td>77%</td>
</tr>
</tbody>
</table>
# FDP Sci and Security Demonstration Possibilities (internal survey with FIWG and RSS)

<table>
<thead>
<tr>
<th>Demonstration Item (Top Impact Ranked listed first)</th>
<th>Impact</th>
<th>Feasibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>6. Create a directory of key publicly advisable databases used to identify malefactors or mechanisms to gain information from non-public databases deemed essential by the federal government.</td>
<td>68%</td>
<td>36%</td>
</tr>
<tr>
<td>7. Work with federal agencies to also create a mechanism to identify good actors, such as foreign entities with research security programs or that incorporate research security requirements into their research integrity programs.</td>
<td>50%</td>
<td>36%</td>
</tr>
<tr>
<td>2. Articulate how organizations that do not meet the $50M threshold should effectively and reasonably comply with the standards.</td>
<td>41%</td>
<td>59%</td>
</tr>
</tbody>
</table>
• Date and time
  • 11:00-12:30 EST on Wednesday 20th, 2023

• Description:
  • This session will explore, and provide a forum for discussion on, institutional engagement in the assessment of international agreements and funding opportunities, including outside activities, funding proposals, and non-monetary agreements, and associated processes and tools. The session will also include discussion on broader needs and tools for assessing, managing and mitigating research security risks and include administrative, federal and faculty perspectives.

• Speakers:
  • Greg Moffat, Chief Research Security Officer, MIT, Sarah Stalker-LeHoux, Deputy Chief Research Security and Policy, NSF and RSS Co-chair and Faculty Member (TBD)
Thanks