Association of Public & Land-grant Universities

Demystifying Research Security Regulations: A Conversation with NSF

Overview of Research Security

***Dr. Sara Barber**, Science Policy Advisor, Office of the Chief of Research Security, Strategy, and Policy (OCRSSP), National Science Foundation*

APLU Commission on International Initiatives

June 17, 2024

What is Research Security?

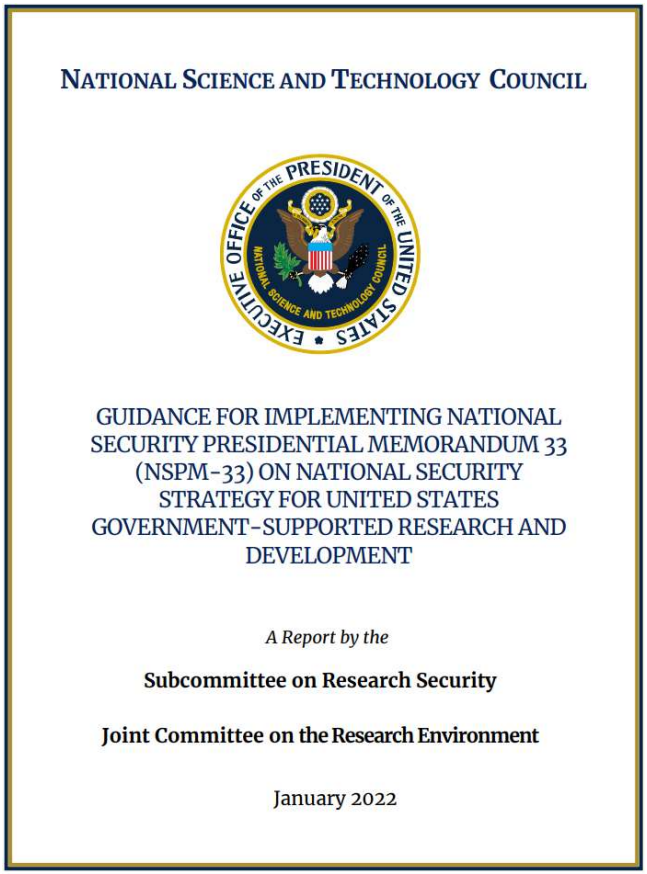
Research security –

Safeguarding the research enterprise against the misappropriation of research and development to the detriment of national or economic security, related violations of research integrity, and foreign government interference.

Source: OSTP/NSPM-33

NSPM-33 Implementation Updates

- **Harmonized Disclosure Policy**
  - OSTP released final forms – February 2024
  - NSF's policy – effective May 2024
- **Research Security Program Standards**
  - *In progress:* DRAFT RSPS Guidance - February 2023
- **Community Resources**
  - Research Security Training Modules – available now
  - *In progress* - SECURE Center – Summer 2024
- **Oversight and Enforcement**
  - *In progress* – Research on Research Security
  - *In progress* - TRUST Framework



NATIONAL SCIENCE AND TECHNOLOGY COUNCIL

GUIDANCE FOR IMPLEMENTING NATIONAL SECURITY PRESIDENTIAL MEMORANDUM 33 (NSPM-33) ON NATIONAL SECURITY STRATEGY FOR UNITED STATES GOVERNMENT-SUPPORTED RESEARCH AND DEVELOPMENT

A Report by the

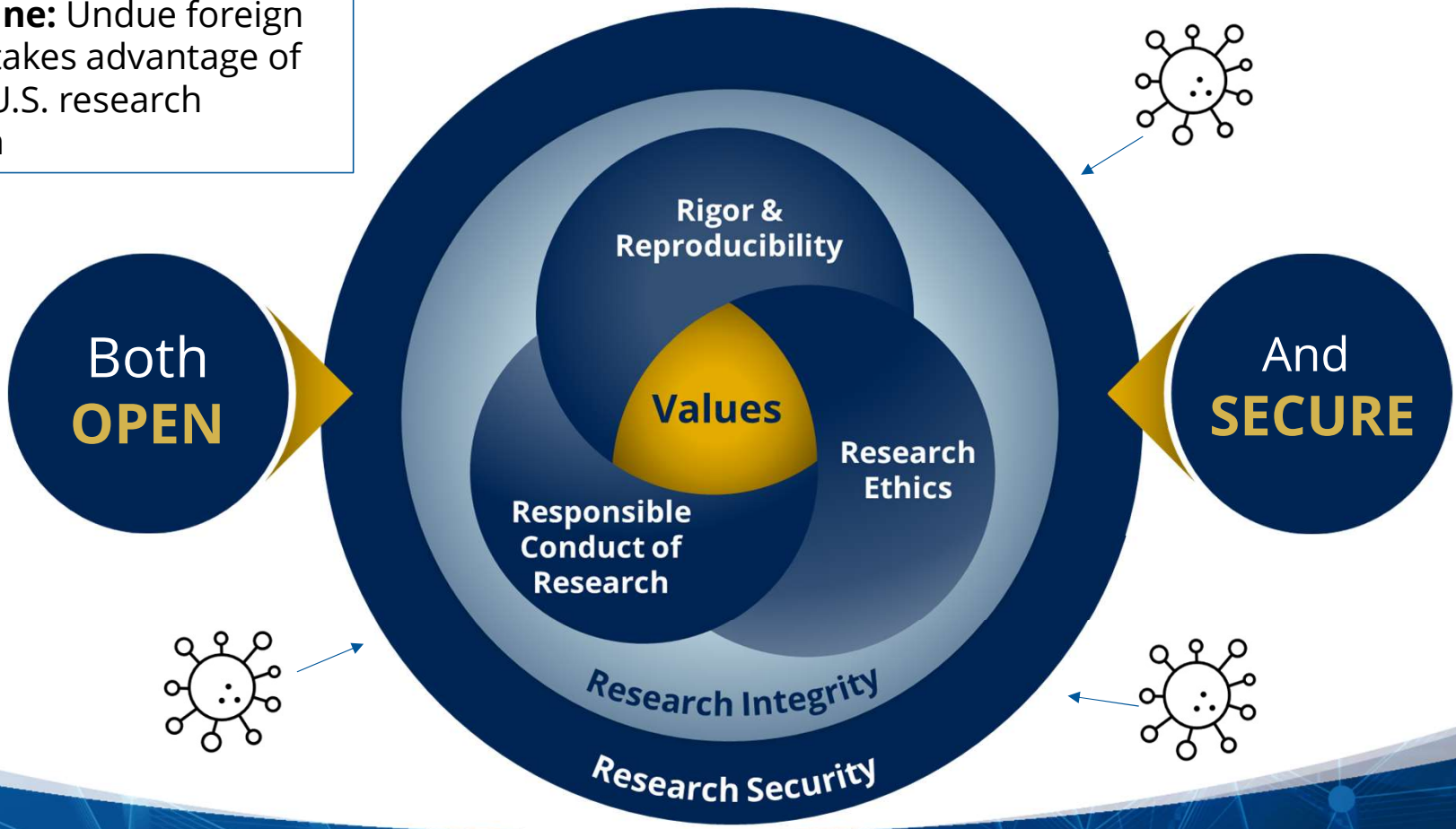
Subcommittee on Research Security

Joint Committee on the Research Environment

January 2022

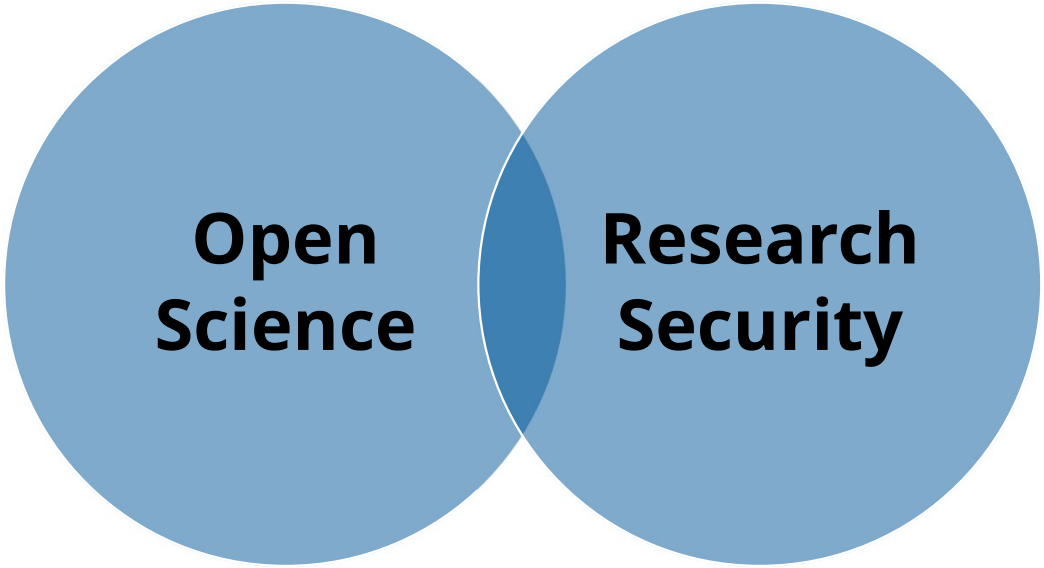
Cell Diagram of Research Security

Bottom Line: Undue foreign influence takes advantage of the open U.S. research ecosystem



Openness and security are not contradictory but complementary and mutually reinforcing.

-G7 Best Practices for Secure and Open Research



International partners are pursuing same policies…. balancing research openness and security aspects

Research Security at All Stages

Academic & Fundamental Research

- Safeguarding researcher ideas
- Doing due diligence on research funding sources
- Assessing potentially harmful end use
- Differentiating international collaboration from research security

Applied Research

- Safeguarding intellectual property
- Doing due diligence on sources of venture capital and investment
- Assessing potentially harmful end use
- Vetting international transactions

Research Security by All Actors

Funders

- Collecting appropriate disclosures
- Assessing research proposals for risk
- Working to mitigate risk to “get to yes”

Research Institutions

- Ensuring disclosures are complete
- Overseeing use of research funding
- Reviewing potential international interactions
- Creating a “research security safety culture”

Researchers

- Understanding terms of any proposed affiliation or funding source
- Communicating with home institution and funding agency
- Promoting a “research security safety culture” in the lab

Common Disclosure Forms

Common Disclosure Forms

- The objective of the *Disclosure Requirements and Standardization* section of NSPM-33 Implementation Guidance is to, "**Provide clarity regarding disclosure requirements** (e.g., who discloses what, relevant limitations and exclusions), **disclosure process** (e.g., updates, corrections, certification, and provision of supporting documentation), and **expected degree of cross-agency uniformity.**"

- NSTC Research Security Subcommittee has worked to develop consistent disclosure requirements for use by senior personnel, as well as to develop proposed common disclosure forms for the **Biographical Sketch and Current and Pending (Other) Support** sections of an application for Federal R&D grants or cooperative agreements.

- On **February 14 of this year, OSTP released guidance** requiring federal research funding agencies to use harmonized common disclosure forms for the Bio Sketch and the Current and Pending (Other) Support portions of funding application packages for grants and cooperative agreements. NSF requirement effective **May 2024**.

Research Security Program Standards (RSPS)

Research Security Program Standards (RSPS)
Key Components

Research Security Training (RST)

Research Security Training for the U.S. Research Community

- Four teams developed research security training frameworks and training modules
- Co-funded with National Institutes of Health (NIH), Department of Energy (DOE), and Department of Defense (DOD)
- Available for all appropriate researchers, stakeholders, students, academics, research security experts and leaders, government agencies and national laboratories

Module Topics

1. What is Research Security 
2. Disclosure 
3. Manage and Mitigate Risk 
4. International Collaboration 

SECURE

Safeguarding the Entire Community in the U.S. Research Ecosystem

Mission:

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

Approach:

Providing information, developing tools, and providing services

Audience:

Universities, non-profit research institutions, and small and medium-sized businesses

Research on Research Security program (RoRS)

Research on Research Security Program (RoRS)

NSF seeks to fund research that will…

Identify and characterize attributes that distinguish research security from research integrity

Improve understanding of the nature, scale, and scope of research security risks

Provide insight into methods for identifying, mitigating, and preventing research security violations

Develop methodologies to assess the potential impact of research security threats on the U.S. economy, national security, and research enterprise

TRUST

Trusted Research Using Safeguards and Transparency

Our Guiding Principles

Respect the science

Get to “YES”

Focus on mitigation measures

Practicing Thoughtful Vigilance…

TRUST

Avoid curtailing beneficial activities due to risk aversion or overly broad interpretation of policy.

Avoid the targeting of individuals based on nationality or country of origin. Protect core values of fairness and due process throughout.

Maintain open lines of communication with the community. We want to hear from institutions before situations become a major concern.

TRUST: Trusted Research Using Safeguards and Transparency

Evaluate Three Criteria, with transparent step by step process:

1) Active appointments and positions w/ or research support from U.S. proscribed parties and active party to a malign foreign government talent recruitment program (MFTRP)
   - U.S. Bureau of Industry and Security Entity List
   - Annex of Executive Order (EO) 14032 or superseding EOs
   - Sec. 1260H of the *National Defense Authorization Act* (NDAA) for FY2021 and Sec. 1286 of the NDAA for FY2019, as amended

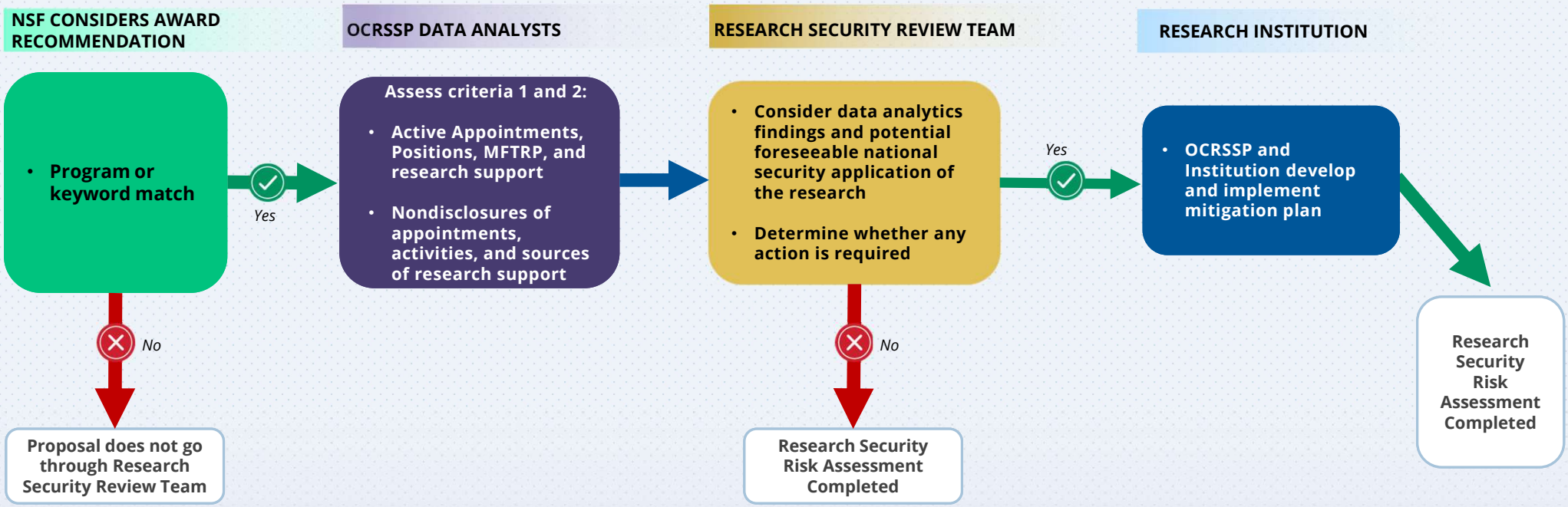
2) Nondisclosures of appointments, activities, and sources of research support (current research security policy)

3) Potential foreseeable national security applications of the research

OCRSSP will confirm that senior personnel have no ***active appointments and positions with U.S. proscribed parties,*** and that they are not **currently a party to a malign foreign talent recruitment program**

Undisclosed information will be examined from the time NSPM-33 Implementation Plan was released (Jan 2022)

TRUST Process



TRUST Implementation

- **Phase 1 – Quantum Proposals – beginning FY25**
  - Pilot program will assess:
    - Implementation of new Research Security Review Team process
    - Timeline of process, bandwidth and resources required from NSF staff
    - NSF's ability to assess potential national security application of the research
    - How often NSF needs other USG expert consultation
    - Whether we want to review classified information

- **Phase 2 – PAPPG Changes & Expand to additional CHIPS+ Key Tech Areas**
  - Information to assess certain criteria are not currently in solicitations
  - Consider expansion to Microelectronics, AI, and Biotechnology.

- **Phase 3 – Scale up Review for all CHIPS+ Key Tech/TIP Priorities**
  - NSF POs will have taken training to feel more assured in the process
  - Mitigations will be more streamlined, expediting the review process


NSF