Overview of Research Security

Dr. Rebecca Keiser, *Chief of Research Security Strategy and Policy*

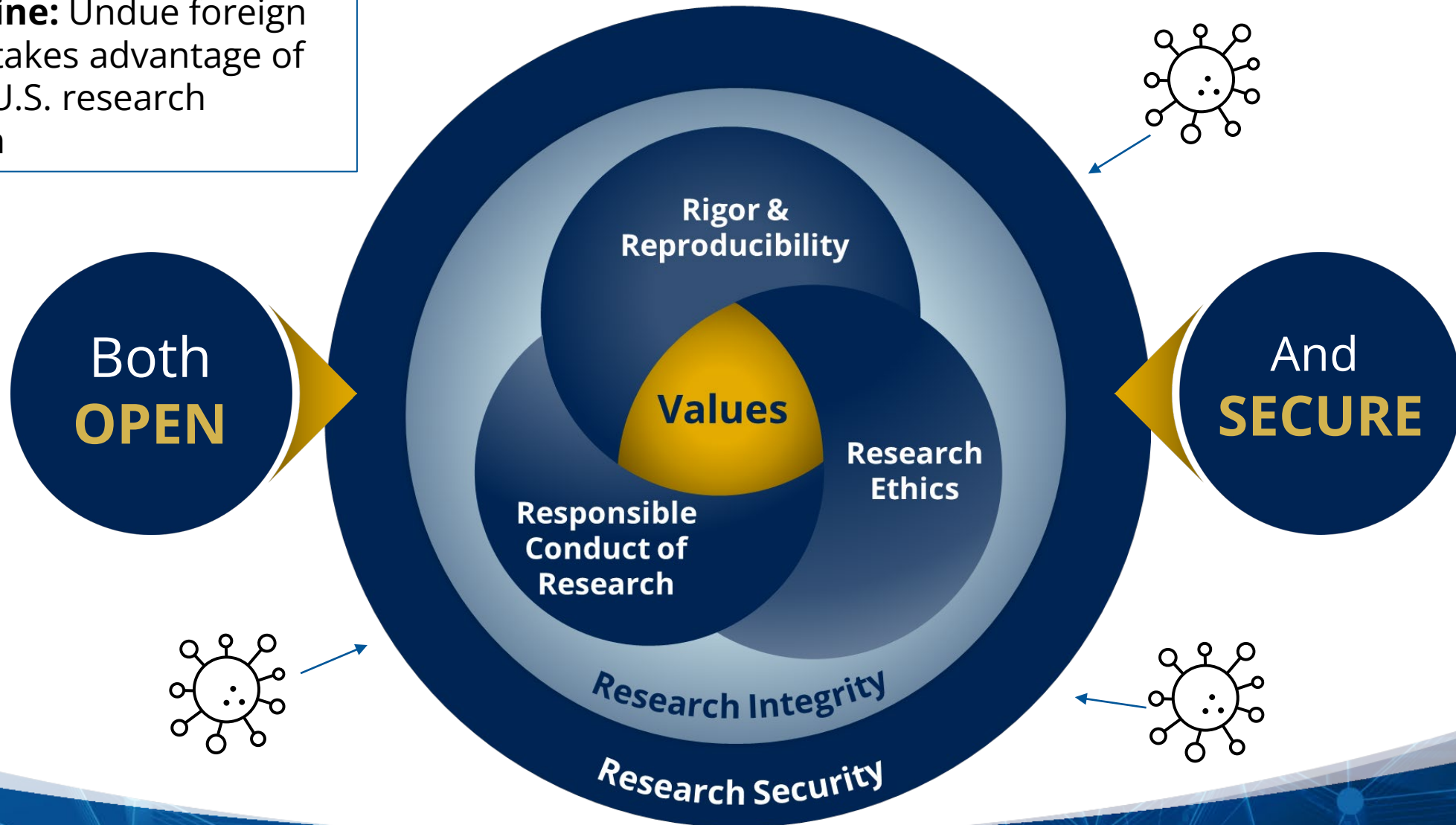# What is Research Security?

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.
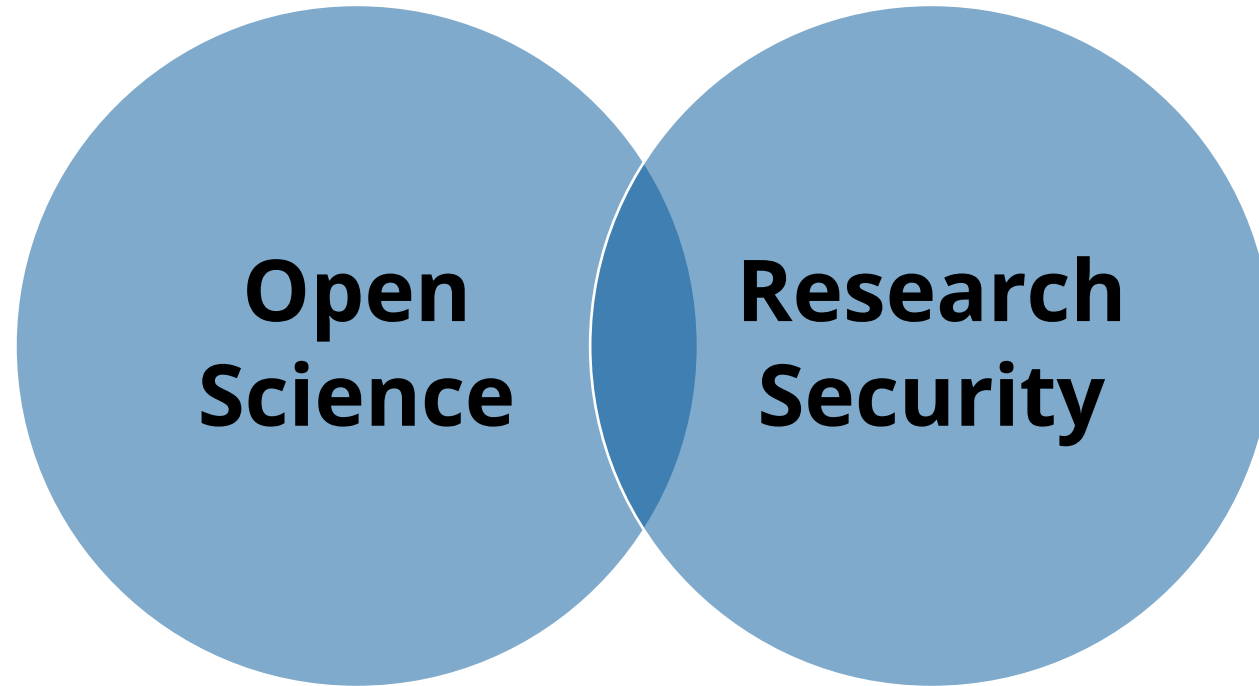
Source: OSTP/NSPM-33

Cell Diagram of Research Security

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

Open Science

Research Security

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

Research Security Program Standards (RSPS)

Research Security Program Standards (RSPS)
Key Components

Cybersecurity

Foreign Travel Security

Research Security Training

Export Control Training

Research Security Training (RST)

Research Security Training for the Research Community

- Four teams developed research security training frameworks and training modules

- 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)
   o U.S. Bureau of Industry and Security Entity List
   o Annex of Executive Order (EO) 14032 or superseding EOs
   o 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

NSF CONSIDERS AWARD RECOMMENDATION

OCRSSP DATA ANALYSTS

RESEARCH SECURITY REVIEW TEAM

RESEARCH INSTITUTION

- **Program or keyword match**

Yes →

Assess criteria 1 and 2:

- **Active Appointments, Positions, MFTRP, and research support**
- **Nondisclosures of appointments, activities, and sources of research support**

- **Consider data analytics findings and potential foreseeable national security application of the research**
- **Determine whether any action is required**

Yes →

- **OCRSSP and Institution develop and implement mitigation plan**

No ↓

Proposal does not go through Research Security Review Team

No ↓

Research Security Risk Assessment Completed

Research Security Risk Assessment Completed