Research Security at NSF

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

March 12, 2025

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

Research Security at All Stages

Academic & Basic Research

- Safeguarding researcher ideas
- Doing due diligence on research funding sources
- Assessing potentially harmful end use
- Encouraging principled international collaboration while focusing on 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

The Office of the Chief of Research Security Strategy and Policy (OCRSSP) supports activities across the Foundation

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

About the SECURE Program

Mission:

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

Approach:

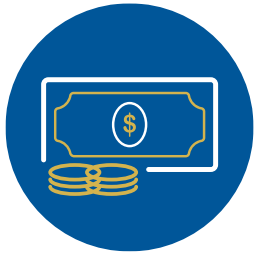
Providing information, developing tools, and providing services

Audience:

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

What SECURE Will Do

Uniform Quality of Service



Reduce Cost and Administrative Burden

Frameworks and Best Practices

Curated Syntheses

Patterns of Risk

Analytical Tools

SECURE Program Awards through Cooperative Agreements with NSF

SECURE Center University of Washington	SECURE Analytics Texas A&M University
Inform the community about evolving risks	Provide landscape risk analyses and modeling
Provide services - training, tools, best practices, case studies, etc.	Provide tailored analytics to address individual questions
Strengthen connections to build a community of practice	Protect the privacy of all users and data sources

Current Status of SECURE

- SECURE Center website: https://www.securecenter.uw.edu/
- SECURE Analytics website: https://secure-analytics.org/
- Steering Committee kickoff meeting at the end of February
  - Advise NSF on policy and operations of the SECURE Program
  - Coordinate information sharing
- Exploring potential mechanisms for international collaborations

TRUST: Trusted Research Using Safeguards and Transparency
Legislative Requirements

Section 10331 of the CHIPS and Science Act of 2022

- ***Perform risk assessments [...] of Foundation proposals and awards using analytical tools to assess nondisclosures of required information;***
- ***Establish policies and procedures for identifying, communicating, and addressing security risks*** that threaten the integrity of Foundation-supported research and development
- Conduct or facilitate ***due diligence*** with regard to applications for research and development awards [...] ***prior to making such awards***.

Section 10339 of the CHIPS and Science Act of 2022

- NSF to ***identify research areas [...] that may involve access to controlled unclassified or classified information*** and exercise due diligence in granting access to individuals working on such research

FY23 Appropriations Report

- Directs the NSF to collaborate with the Secretary of Defense and the Director of National Intelligence to ***compile and maintain a list of all NSF-funded open-source research capabilities that are known or suspected to have an impact on foreign military operations***

Our Guiding Principles

Respect the science

Get to “YES”

Focus on mitigation measures

TRUST: Trusted Research Using Safeguards and Transparency

Evaluate Three Criteria, with transparent step by step process:

1) Active appointments and positions with, or research support from U.S. proscribed parties and 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

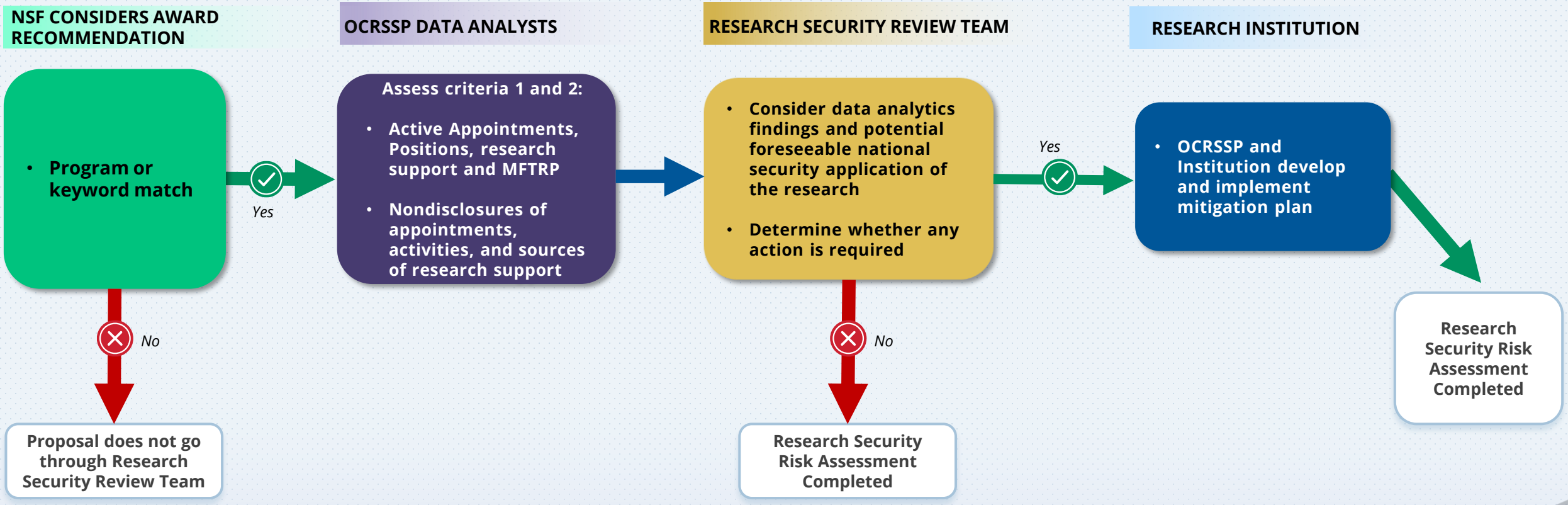
2) Nondisclosures of appointments, activities, and sources of research support (current research security policy)

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 Pilot

- A pilot of the TRUST process began in Fiscal Year 2025 focused on incoming QIS proposals
    - Informed by National Security Memorandum-10: Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems.
- Working closely with NSF PDs and OCRSSP data analysts to identify proposals for the pilot
- OCRSSP will be gathering data on resources required from NSF staff and measuring the effectiveness of the TRUST process
- Based on pilot's performance, TRUST may be expanded to other critical and emerging technology areas

TRUST Resources

- The following is a list of resources and references for learning more about TRUST

NSF TRUST Press Release

NSF TRUST Policy Memo

NSF TRUST Webinar Recording

NSF Research Security Analytics Guidelines

JASON Report: Safeguarding the Research Enterprise

Proscribed entity lists:

- 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

Contact Information:

Office of the Chief of Research Security Strategy and Policy Email:
researchsecurity@nsf.gov

NSF Research Security Website:
http://new.nsf.gov/research-security


NSF