The Path Forward for Research Security and Integrity

***Sarah Stalker-Lehoux**, Deputy Chief of Research Security Strategy and Policy, National Science Foundation*

Presentation to the Society of Research Administrators International Annual Meeting

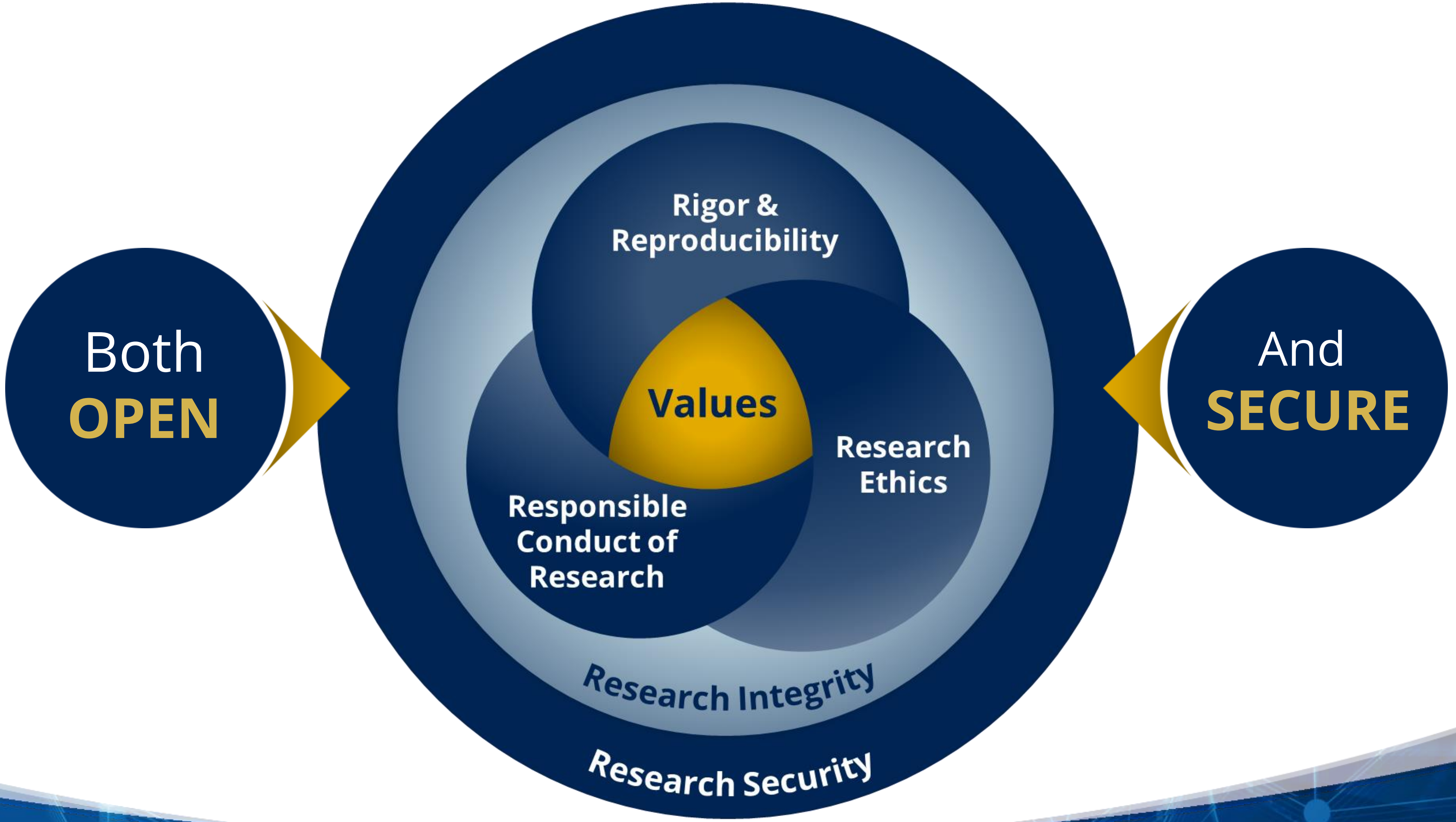
October 16, 2023

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.

Values are the Heart of Research Security



Both
OPEN

Rigor & Reproducibility

Values

Research Ethics

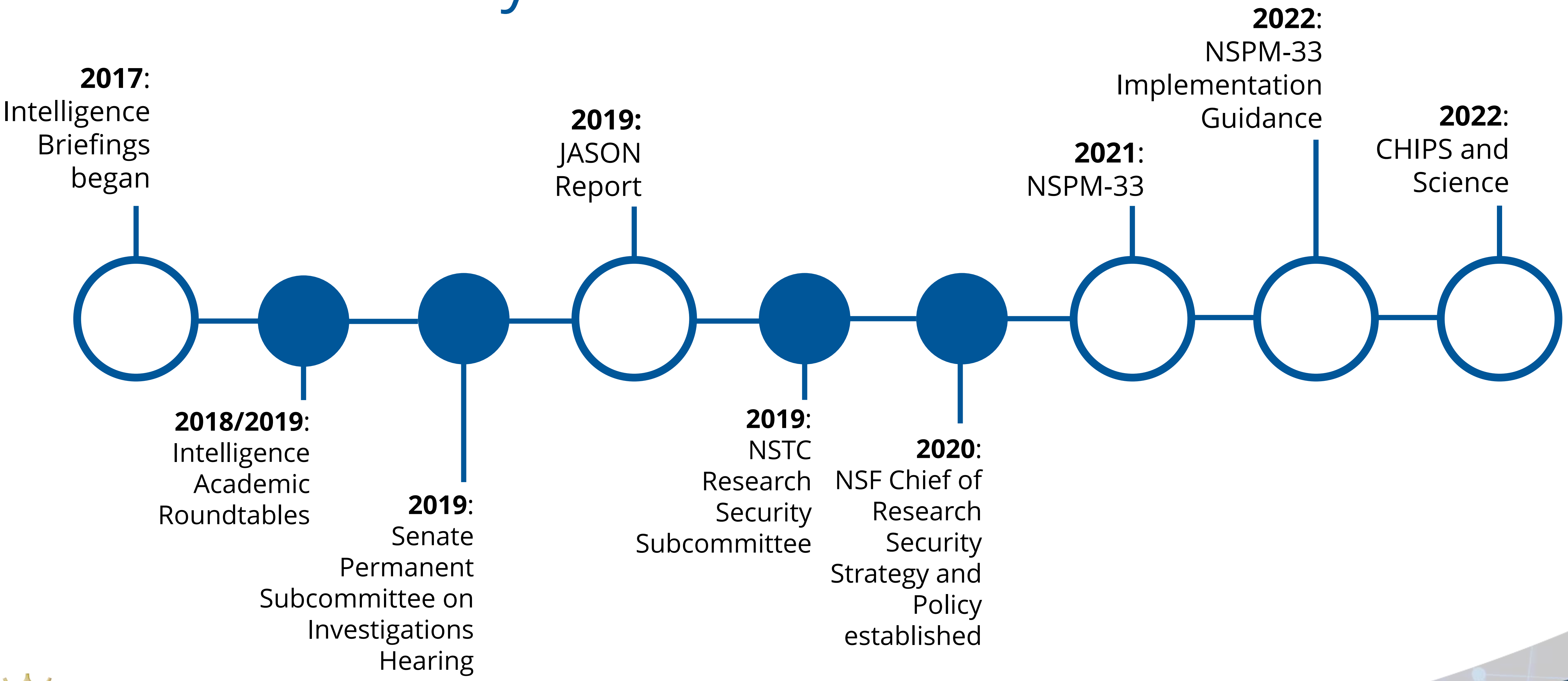
Responsible Conduct of Research

Research Integrity

Research Security

And
SECURE

Research Security Timeline



2017: Intelligence Briefings began

2018/2019: Intelligence Academic Roundtables

2019: Senate Permanent Subcommittee on Investigations Hearing

2019: JASON Report

2019: NSTC Research Security Subcommittee

2020: NSF Chief of Research Security Strategy and Policy established

2021: NSPM-33

2022: NSPM-33 Implementation Guidance

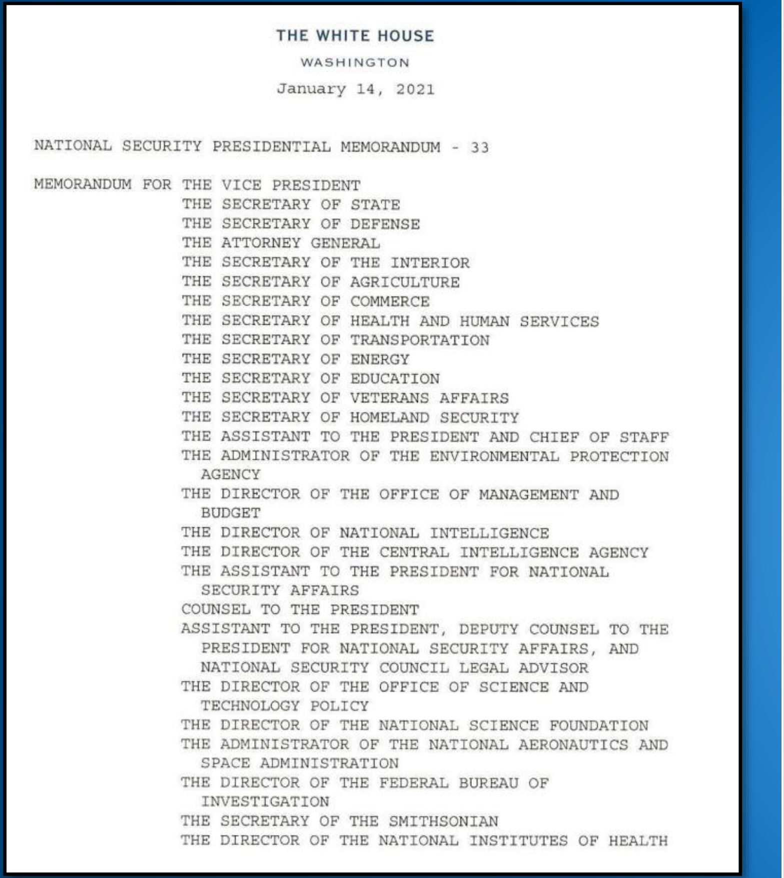
2022: CHIPS and Science

2019 JASON report "Fundamental Research Security“ Findings:

- **Foreign-born scientists and engineers in the United States make essential contributions to U.S. preeminence in science, engineering and technology today. Continuing to attract and retain such talent is essential for maintaining that leading position.**
- The United States upholds values of ethics in science, including objectivity, honesty, accountability, fairness and stewardship. These values protect research integrity.
- Actions of the PRC government and its institutions that are not in accord with U.S. values of science ethics have raised concerns about foreign influence in the U.S. academic sector.
- **The scale and scope of the problem remain poorly defined. Academic leadership, faculty and front-line government agencies lack a common understanding of foreign influence in U.S. fundamental research, possible risks and the possible detrimental effects of restrictions that might be enacted in response.**
- Conflicts of interest and commitment in the research enterprise can be broader than those that are strictly financial.
- There are many stakeholders with responsibility for the integrity of fundamental research, from U.S. government agencies to individual scholars. Universities and research funding agencies have policies and guidelines regarding some of these responsibilities, but these are often insufficient for individuals to assess risk and take appropriate actions.

2019 JASON report "Fundamental Research Security" Recommendations:

1. **Expand the scope of expectations under the umbrella of research integrity to include full disclosure of commitments and actual or potential conflicts of interest.**
2. Failures to disclose commitments and actual or potential conflicts of interest should be investigated and adjudicated by the relevant office of NSF and by universities as presumptive violations of research integrity, with consequences similar to those currently in place for scientific misconduct.
3. **NSF should take a lead in working with NSF-funded universities and other entities, as well as professional societies and publishers to ensure that the responsibilities of all stakeholders in maintaining research integrity are clearly stated, acknowledged and adopted. Harmonization of these responsibilities with those of other federal research-funding agencies is encouraged.**
4. Education and training in scientific ethics at universities and other institutions performing fundamental research should be expanded beyond traditional research integrity issues to include information and examples covering conflicts of interest and commitment.
5. NSF should further engage with the community of foreign researchers in the United States to enlist them in the effort to foster openness and transparency in fundamental research, nationally and globally, as well as to benefit from their connections to identify, recruit and retain the best scientific talent to the United States.



THE WHITE HOUSE

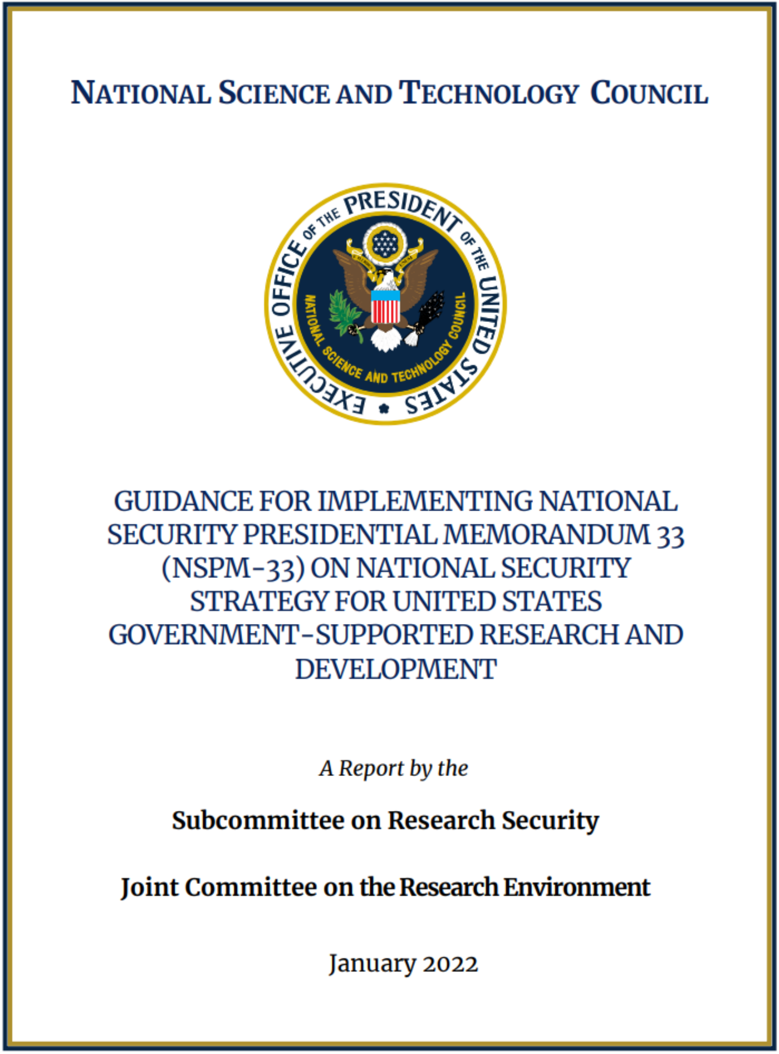
WASHINGTON

January 14, 2021

NATIONAL SECURITY PRESIDENTIAL MEMORANDUM - 33

MEMORANDUM FOR THE VICE PRESIDENT
THE SECRETARY OF STATE
THE SECRETARY OF DEFENSE
THE ATTORNEY GENERAL
THE SECRETARY OF THE INTERIOR
THE SECRETARY OF AGRICULTURE
THE SECRETARY OF COMMERCE
THE SECRETARY OF HEALTH AND HUMAN SERVICES
THE SECRETARY OF TRANSPORTATION
THE SECRETARY OF ENERGY
THE SECRETARY OF EDUCATION
THE SECRETARY OF VETERANS AFFAIRS
THE SECRETARY OF HOMELAND SECURITY
THE ASSISTANT TO THE PRESIDENT AND CHIEF OF STAFF
THE ADMINISTRATOR OF THE ENVIRONMENTAL PROTECTION AGENCY
THE DIRECTOR OF THE OFFICE OF MANAGEMENT AND BUDGET
THE DIRECTOR OF NATIONAL INTELLIGENCE
THE DIRECTOR OF THE CENTRAL INTELLIGENCE AGENCY
THE ASSISTANT TO THE PRESIDENT FOR NATIONAL SECURITY AFFAIRS
COUNSEL TO THE PRESIDENT
ASSISTANT TO THE PRESIDENT, DEPUTY COUNSEL TO THE PRESIDENT FOR NATIONAL SECURITY AFFAIRS, AND NATIONAL SECURITY COUNCIL LEGAL ADVISOR
THE DIRECTOR OF THE OFFICE OF SCIENCE AND TECHNOLOGY POLICY
THE DIRECTOR OF THE NATIONAL SCIENCE FOUNDATION
THE ADMINISTRATOR OF THE NATIONAL AERONAUTICS AND SPACE ADMINISTRATION
THE DIRECTOR OF THE FEDERAL BUREAU OF INVESTIGATION
THE SECRETARY OF THE SMITHSONIAN
THE DIRECTOR OF THE NATIONAL INSTITUTES OF HEALTH

NSPM-33



NATIONAL SCIENCE AND TECHNOLOGY COUNCIL

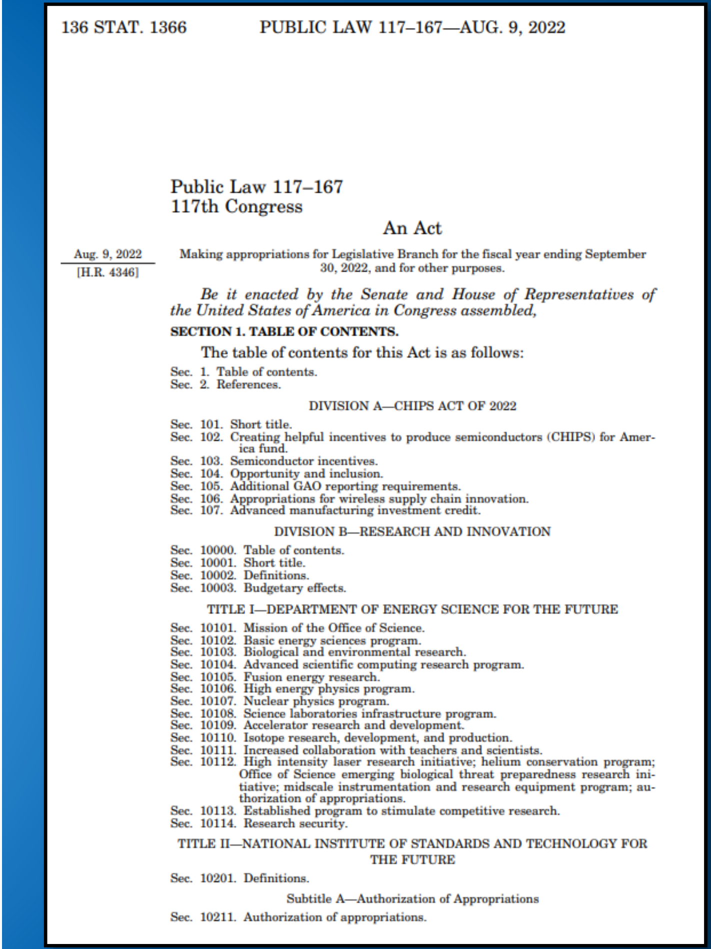
GUIDANCE FOR IMPLEMENTING NATIONAL SECURITY PRESIDENTIAL MEMORANDUM 33 (NSPM-33) ON NATIONAL SECURITY STRATEGY FOR UNITED STATES GOVERNMENT-SUPPORTED RESEARCH AND DEVELOPMENT

A Report by the

Subcommittee on Research Security

Joint Committee on the Research Environment

January 2022



136 STAT. 1366 PUBLIC LAW 117–167—AUG. 9, 2022

Public Law 117–167
117th Congress

An Act

Aug. 9, 2022
[H.R. 4346]

Making appropriations for Legislative Branch for the fiscal year ending September 30, 2022, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. TABLE OF CONTENTS.

The table of contents for this Act is as follows:

Sec. 1. Table of contents.
Sec. 2. References.

DIVISION A—CHIPS ACT OF 2022

Sec. 101. Short title.
Sec. 102. Creating helpful incentives to produce semiconductors (CHIPS) for America fund.
Sec. 103. Semiconductor incentives.
Sec. 104. Opportunity and inclusion.
Sec. 105. Additional GAO reporting requirements.
Sec. 106. Appropriations for wireless supply chain innovation.
Sec. 107. Advanced manufacturing investment credit.

DIVISION B—RESEARCH AND INNOVATION

Sec. 10000. Table of contents.
Sec. 10001. Short title.
Sec. 10002. Definitions.
Sec. 10003. Budgetary effects.

TITLE I—DEPARTMENT OF ENERGY SCIENCE FOR THE FUTURE

Sec. 10101. Mission of the Office of Science.
Sec. 10102. Basic energy sciences program.
Sec. 10103. Biological and environmental research.
Sec. 10104. Advanced scientific computing research program.
Sec. 10105. Fusion energy research.
Sec. 10106. High energy physics program.
Sec. 10107. Nuclear physics program.
Sec. 10108. Science laboratories infrastructure program.
Sec. 10109. Accelerator research and development.
Sec. 10110. Isotope research, development, and production.
Sec. 10111. Increased collaboration with teachers and scientists.
Sec. 10112. High intensity laser research initiative; helium conservation program; Office of Science emerging biological threat preparedness research initiative; midscale instrumentation and research equipment program; authorization of appropriations.
Sec. 10113. Established program to stimulate competitive research.
Sec. 10114. Research security.

TITLE II—NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY FOR THE FUTURE

Sec. 10201. Definitions.

Subtitle A—Authorization of Appropriations

Sec. 10211. Authorization of appropriations.

CHIPS And Science Act

Office of the Chief of Research Security Strategy and Policy’s Research Security Activities

- Implementing Research Security Policies
- Research Security Training Modules
- Data Analytics Program
- Research on Research Security Program
- SECURE Center

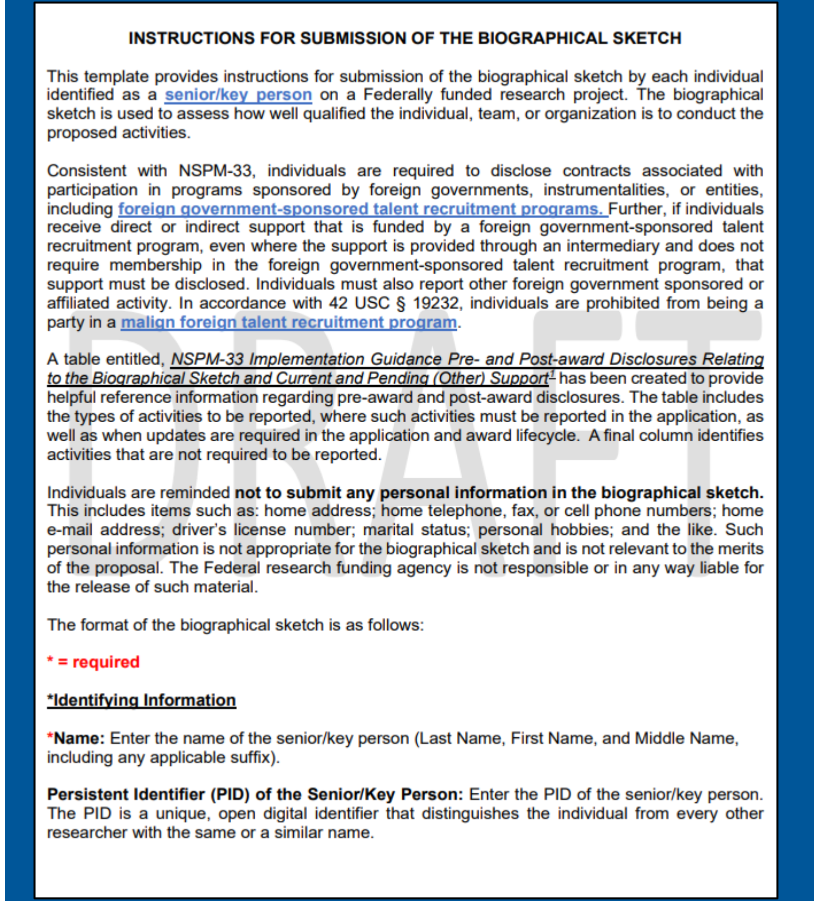
NSPM Implementation Guidance, issued January 2022

- **Disclosure Policy** — ensuring that federally-funded researchers provide to their funding agencies and research organizations the 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.

Harmonized Disclosures

Common Disclosure Forms

Biographical Sketch



INSTRUCTIONS FOR SUBMISSION OF THE BIOGRAPHICAL SKETCH

This template provides instructions for submission of the biographical sketch by each individual identified as a senior/key person on a Federally funded research project. The biographical sketch is used to assess how well qualified the individual, team, or organization is to conduct the proposed activities.

Consistent with NSPM-33, individuals are required to disclose contracts associated with participation in programs sponsored by foreign governments, instrumentalities, or entities, including foreign government-sponsored talent recruitment programs. Further, if individuals receive direct or indirect support that is funded by a foreign government-sponsored talent recruitment program, even where the support is provided through an intermediary and does not require membership in the foreign government-sponsored talent recruitment program, that support must be disclosed. Individuals must also report other foreign government sponsored or affiliated activity. In accordance with 42 USC § 19232, individuals are prohibited from being a party in a malign foreign talent recruitment program.

A table entitled, *NSPM-33 Implementation Guidance Pre- and Post-award Disclosures Relating to the Biographical Sketch and Current and Pending (Other) Support*[1] has been created to provide helpful reference information regarding pre-award and post-award disclosures. The table includes the types of activities to be reported, where such activities must be reported in the application, as well as when updates are required in the application and award lifecycle. A final column identifies activities that are not required to be reported.

Individuals are reminded **not to submit any personal information in the biographical sketch.** This includes items such as: home address; home telephone, fax, or cell phone numbers; home e-mail address; driver's license number; marital status; personal hobbies; and the like. Such personal information is not appropriate for the biographical sketch and is not relevant to the merits of the proposal. The Federal research funding agency is not responsible or in any way liable for the release of such material.

The format of the biographical sketch is as follows:

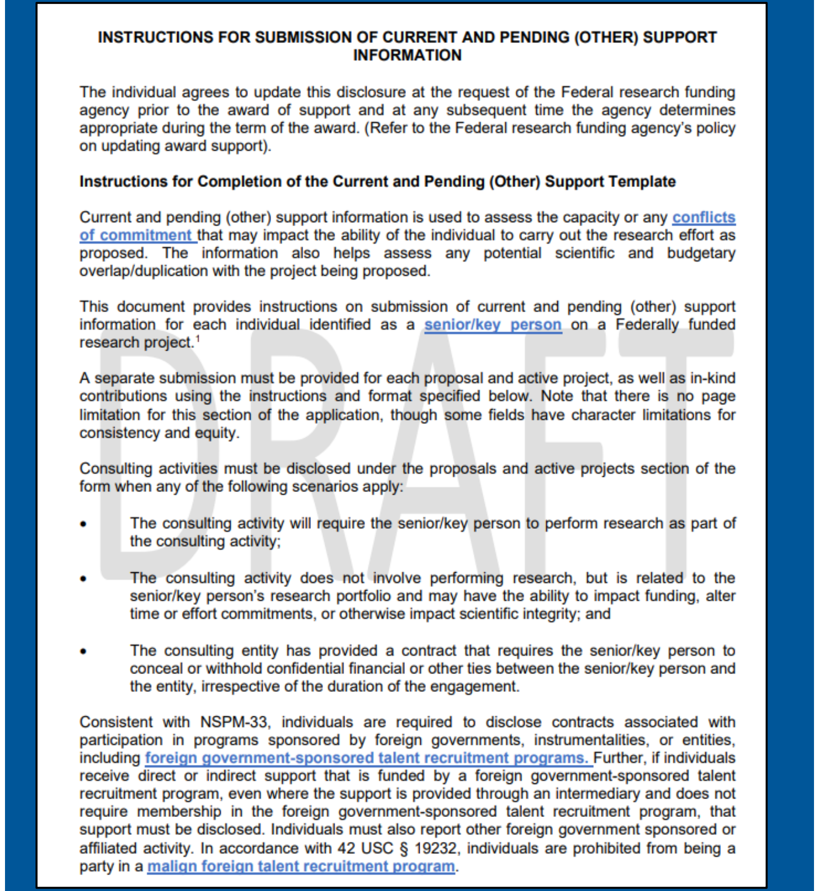
*** = required**

***Identifying Information**

***Name:** Enter the name of the senior/key person (Last Name, First Name, and Middle Name, including any applicable suffix).

Persistent Identifier (PID) of the Senior/Key Person: Enter the PID of the senior/key person. The PID is a unique, open digital identifier that distinguishes the individual from every other researcher with the same or a similar name.

Current & Pending Support



INSTRUCTIONS FOR SUBMISSION OF CURRENT AND PENDING (OTHER) SUPPORT INFORMATION

The individual agrees to update this disclosure at the request of the Federal research funding agency prior to the award of support and at any subsequent time the agency determines appropriate during the term of the award. (Refer to the Federal research funding agency's policy on updating award support).

Instructions for Completion of the Current and Pending (Other) Support Template

Current and pending (other) support information is used to assess the capacity or any conflicts of commitment that may impact the ability of the individual to carry out the research effort as proposed. The information also helps assess any potential scientific and budgetary overlap/duplication with the project being proposed.

This document provides instructions on submission of current and pending (other) support information for each individual identified as a senior/key person on a Federally funded research project.[1]

A separate submission must be provided for each proposal and active project, as well as in-kind contributions using the instructions and format specified below. Note that there is no page limitation for this section of the application, though some fields have character limitations for consistency and equity.

Consulting activities must be disclosed under the proposals and active projects section of the form when any of the following scenarios apply:

- The consulting activity will require the senior/key person to perform research as part of the consulting activity;
- The consulting activity does not involve performing research, but is related to the senior/key person's research portfolio and may have the ability to impact funding, alter time or effort commitments, or otherwise impact scientific integrity; and
- The consulting entity has provided a contract that requires the senior/key person to conceal or withhold confidential financial or other ties between the senior/key person and the entity, irrespective of the duration of the engagement.

Consistent with NSPM-33, individuals are required to disclose contracts associated with participation in programs sponsored by foreign governments, instrumentalities, or entities, including foreign government-sponsored talent recruitment programs. Further, if individuals receive direct or indirect support that is funded by a foreign government-sponsored talent recruitment program, even where the support is provided through an intermediary and does not require membership in the foreign government-sponsored talent recruitment program, that support must be disclosed. Individuals must also report other foreign government sponsored or affiliated activity. In accordance with 42 USC § 19232, individuals are prohibited from being a party in a malign foreign talent recruitment program.

Importance of Disclosure

EVALUATING RISKS

Transparency and full disclosure are essential to properly identify and assess risks.

AVOIDING CONFLICTS

Disclosed information is used to identify potential conflicts of interest and commitment in some instances and potential issues related to capacity, overlap, and duplication in others.

ASSESSING QUALIFICATIONS

Disclosed information is used to assess the qualifications of the individual or team to perform the proposed project.

Enables a system that is fair to those who apply for grants and a system where grant decisions are made based on complete and accurate information

Research Security Program Requirements

NSPM-33: Research Security Program Requirements

Cybersecurity

Foreign Travel Security

Research Security Training

Export Control Training

The Chips and Science Act of 2022

- Prohibition of malign foreign government talent recruitment programs
- Requirement to establish a Research Security and Integrity Information Sharing and Analysis Organization (SECURE Center)
- 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

President Biden sits at a table with the recently signed 'CHIPS and Science Act,' surrounded by legislators and Vice President Kamala Harris.

CHIPS +: Malign Foreign Talent Program Definition

- Unauthorized transfer of intellectual property or other nonpublic information;
- Recruit trainees or researchers to enroll in such program;
- Establishing a laboratory/employment/appointment in a foreign country in violation of terms and conditions of a Federal research award;
- Inability to terminate;
- Overcapacity/overlap/duplication;
- Mandatory to obtain research funding from the foreign government's entities;
- Omitting acknowledgement of U.S. home institution/funding agency;
- Not disclosing program participation; or
- Conflict of interest/commitment.

And also sponsored by a country of concern

SECURE

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

Today's Geopolitical Environment is Challenging for Research

Researchers & Institutions

SECURE is the bridge

US Government

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

Duties of SECURE under CHIPS

1. **Serve as a clearinghouse for information** to help enable the members and other entities in the research community to understand the context of their research and identify improper or illegal efforts by foreign entities to obtain research results, know how, materials, and intellectual property;

2. **Develop a standard set of frameworks and best practices**, relevant to the research community, to assess research security risks in different contexts;

3. **Share information concerning security threats** and lessons learned from protection and response efforts through forums and other forms of communication;

4. **Provide timely reports** on research security risks to provide situational awareness tailored to the research and STEM education community;

5. **Provide training and support**, including through webinars, for relevant faculty and staff employed by institutions of higher education on topics relevant to research security risks and response;

6. **Enable standardized information gathering** and data compilation, storage, and analysis for compiled incident reports;

7. **Support analysis of patterns of risk and identification** of bad actors and enhance the ability of members to prevent and respond to research security risks;

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

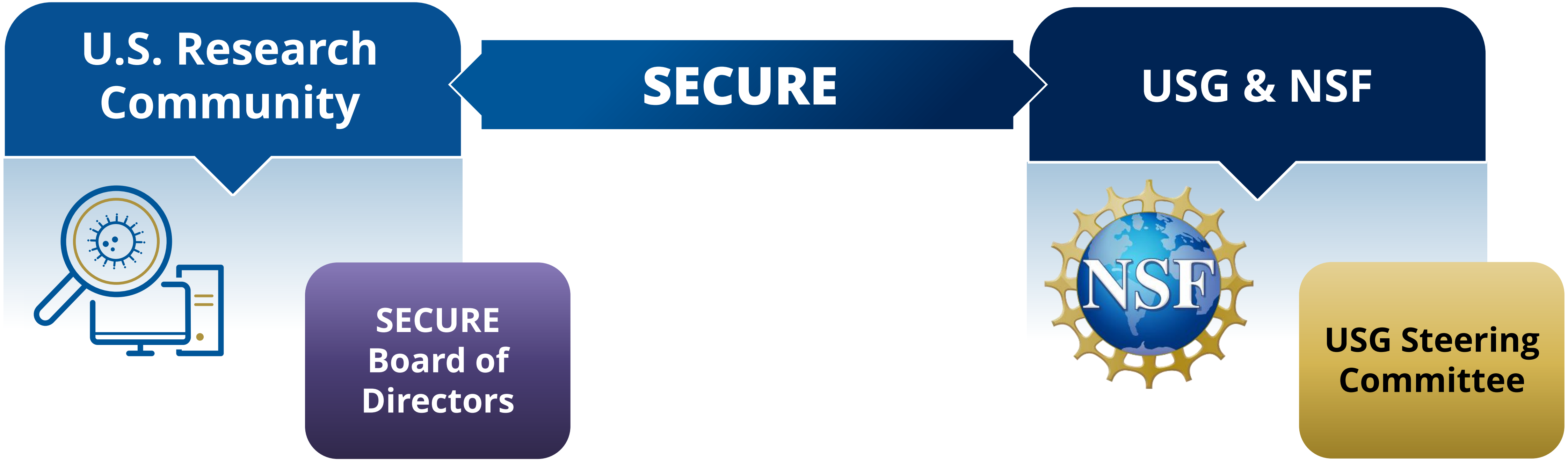
Analytical Tools

Advice, Decisions, Investigations, Policy

Functional Domains

- Tools & Training
- Community Engagement & Inquiries
- Data Analysis & Reporting

Governance Structure of SECURE



U.S. Research Community

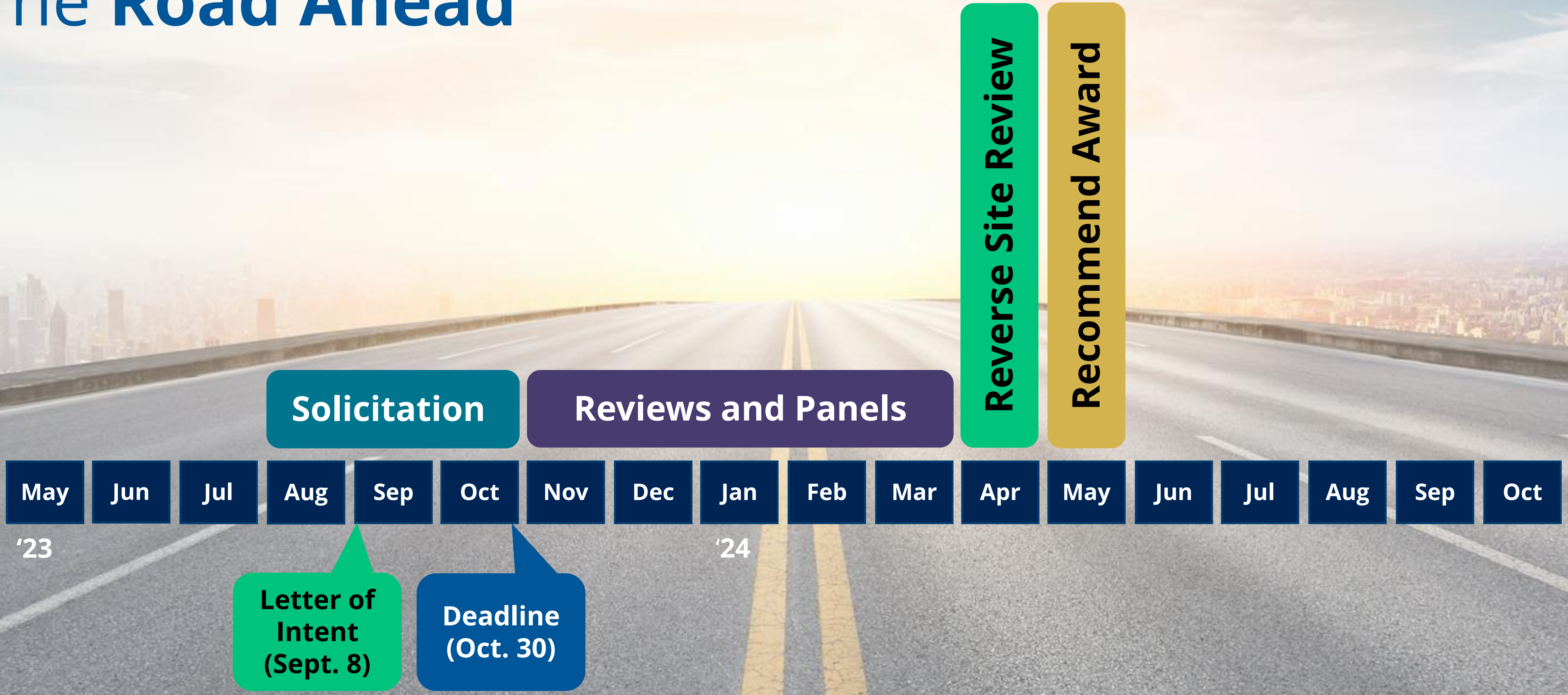
SECURE

USG & NSF

SECURE Board of Directors

USG Steering Committee

The **Road Ahead**



Solicitation

Reviews and Panels

Reverse Site Review

Recommend Award

May Jun Jul Aug Sep Oct Nov Dec Jan Feb Mar Apr May Jun Jul Aug Sep Oct

‘23

‘24

Letter of Intent (Sept. 8)

Deadline (Oct. 30)

Research Security Training Modules

Research Security Training for the U.S. Research Community

- Four teams developing 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

Research Security Training Module Topics

1 What is Research Security

2 Disclosure

3 Manage and Mitigate Risk

4 International Collaboration

Foreign Financial Disclosure Requirements

CHIPS+: Foreign financial transactions and gifts

Sec. 10999b of CHIPS+

- Requires NSF “recipient institution of higher education... a foundation of the institution, and related entities such as any educational, cultural, or language entity…. to report all “current financial support, the value of which is $50,000 or more, including gifts and contracts, received directly or indirectly from a foreign source” which is “associated with a foreign country of concern.

CHIPS+: Prohibition of Confucius Institutes

Sec. 10339(a)

- The term “Confucius Institute” means a cultural institute established as a partnership between a United States institution of higher education and a Chinese institution of higher education to promote and teach Chinese language and culture that is funded, directly or indirectly, by the PRC Government.
- NSF funds may not be obligated or expended to an institution of higher education that maintains a contract or agreement between the institution and a Confucius Institute, unless the Director, after consultation with the National Academies, determines such a waiver is appropriate in accordance with subsection (c).

Research on Research Security Program (RRSP)

JASON report - Research Program on Research Security Findings:

1. ***The issue of research security is real.*** The fruits of US STEM research and their benefits to US interests across many arenas have been challenged by inappropriate practices in the international arena.
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.

JASON report - Research Program on Research Security Recommendations:

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.*** In a research program on research security, NSF and proposers must consider the ability to access confidential data at universities and private companies. NSF should assist Principal Investigators with data access and in the use of methods for anonymization of data.
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.

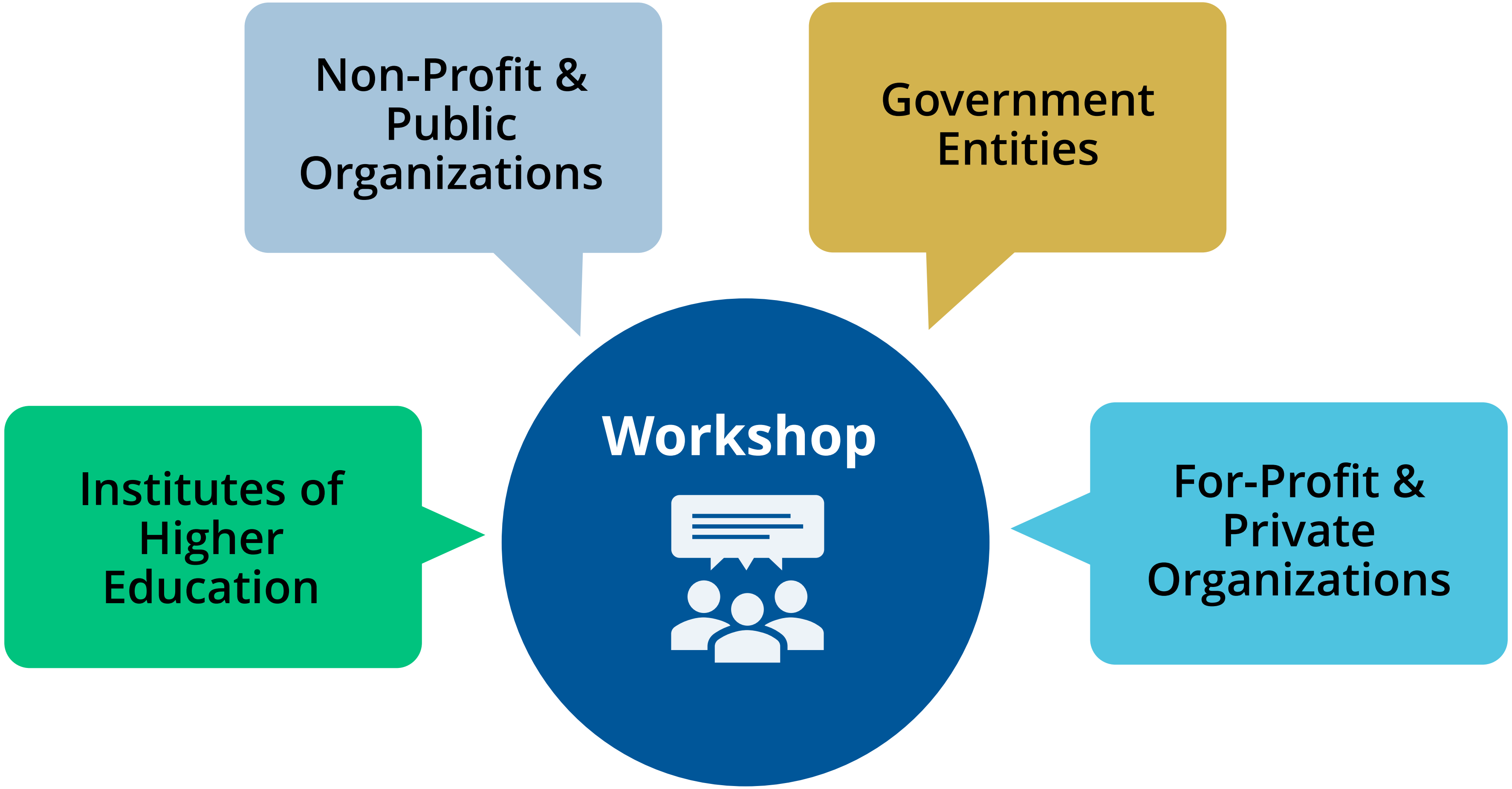
Report posted on CRSSP website: https://new.nsf.gov/research-security

Research on Research Security Program (RRSP)

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

First Step: Creating a Community of Practice



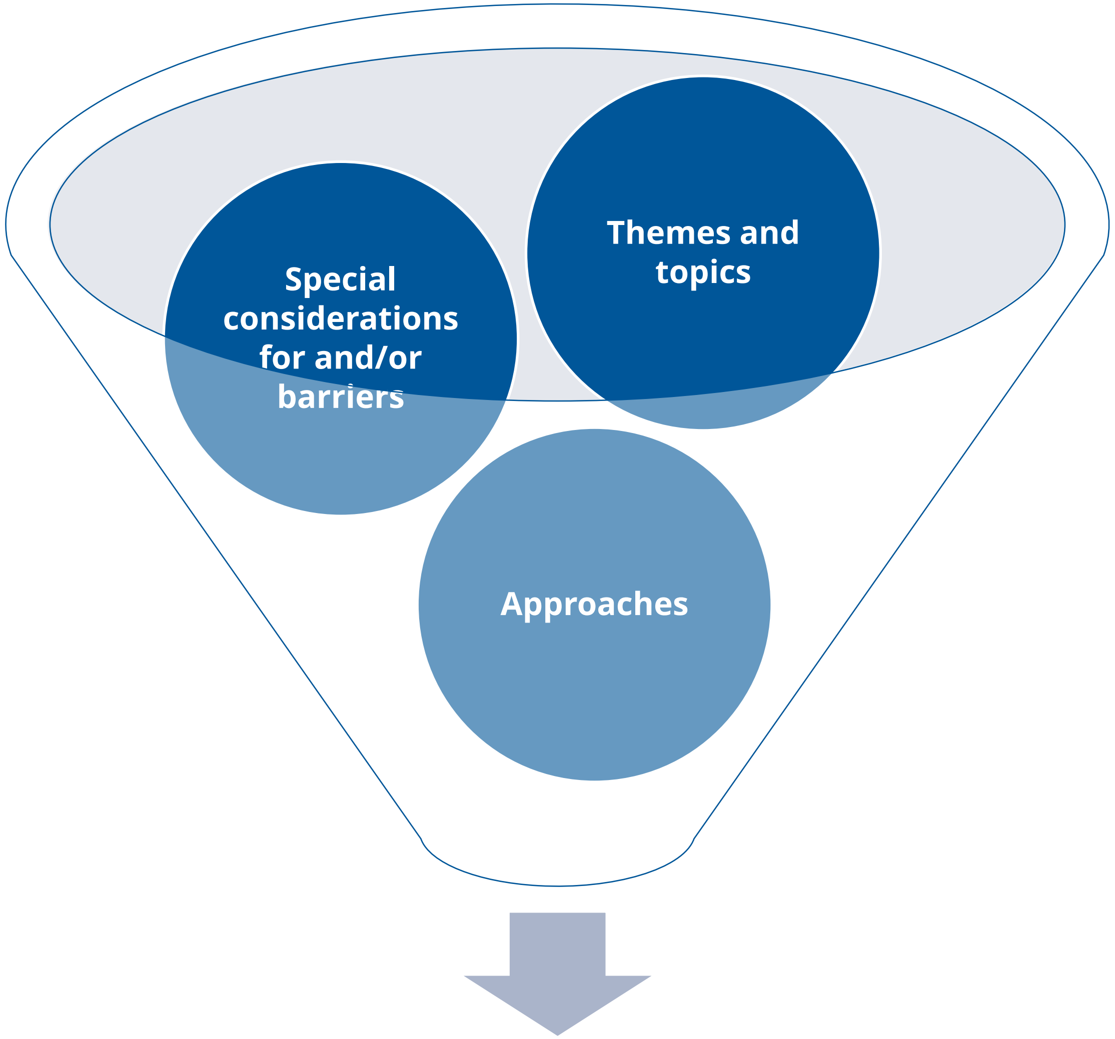
Non-Profit & Public Organizations

Government Entities

Workshop

Institutes of Higher Education

For-Profit & Private Organizations

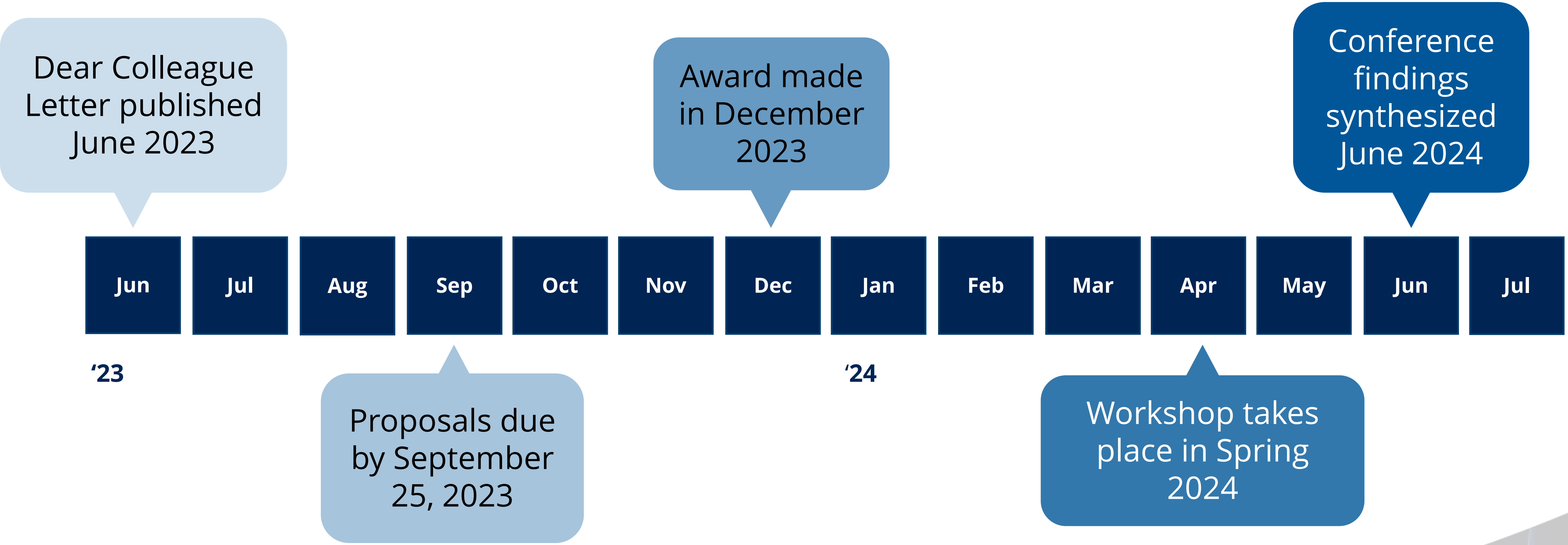


Research on Research Security Workshop

Potential Themes & Topics

- Nature & Pervasiveness of Research Security Threats
- Research Security Threat Identification, Mitigation, and Prevention
- International Dimensions of Research Security
- & others as identified by workshop organizers

Workshop Timeline



Dear Colleague Letter published June 2023

Proposals due by September 25, 2023

Award made in December 2023

Workshop takes place in Spring 2024

Conference findings synthesized June 2024

Research Security Analytics Tools

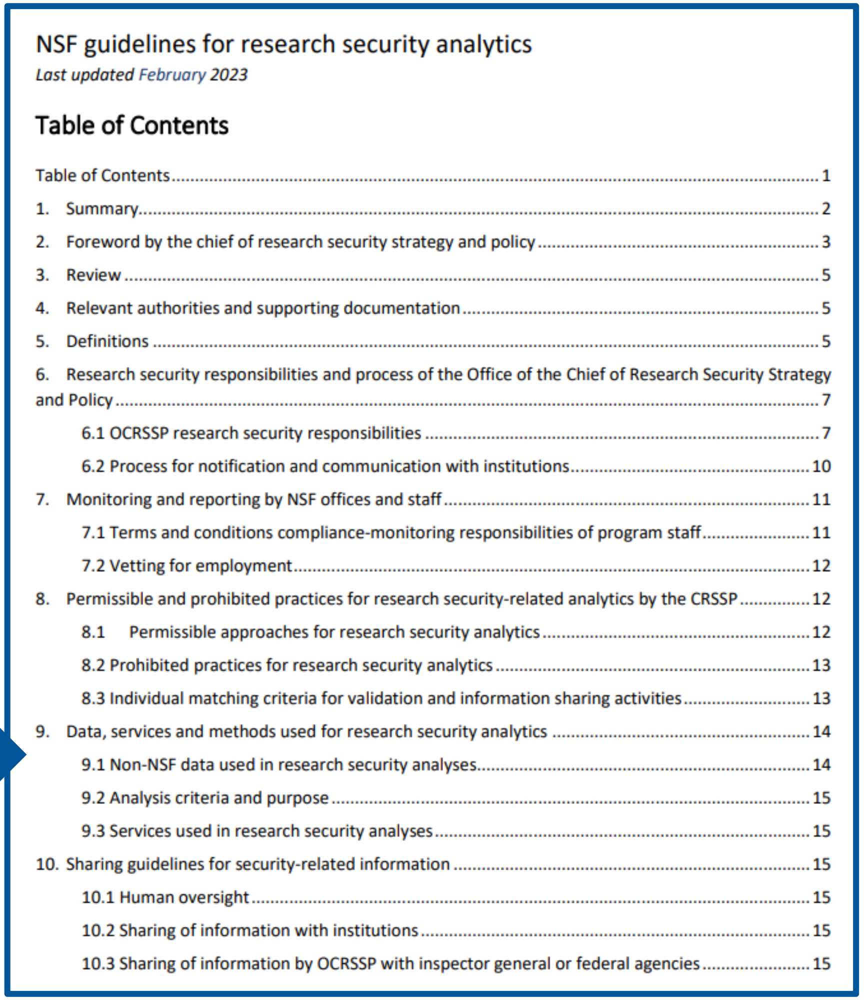
The NSF Research Security Analytics Guidelines

is a public document describing NSF's internal guidance for research security data-related practices

Uses for the data-related practices include:

- Compliance-monitoring responsibilities of program staff
- Vetting for employment

Available online



NSF guidelines for research security analytics

Last updated February 2023

Table of Contents

NSF Guidelines for Research Security Analytics – **Key Principles**

1. Program staff are not permitted to use research security concerns as a determining factor in the merit review process.

2. All research security analytics activities at NSF will be conducted solely by the Office of the Chief of Research Security Strategy and Policy, or OCRSSP.

3. Program staff are not permitted to conduct intentional information querying activities related to research security. Concerns encountered during routine merit review activities (see "routine assessment" in definitions) are to be reported to OCRSSP

Research Security Analytics Summary

Routine Assessment

- Guardrails established to ensure unbiased monitoring techniques
- Research security related analytics restricted to OCRSSP staff only

Validation

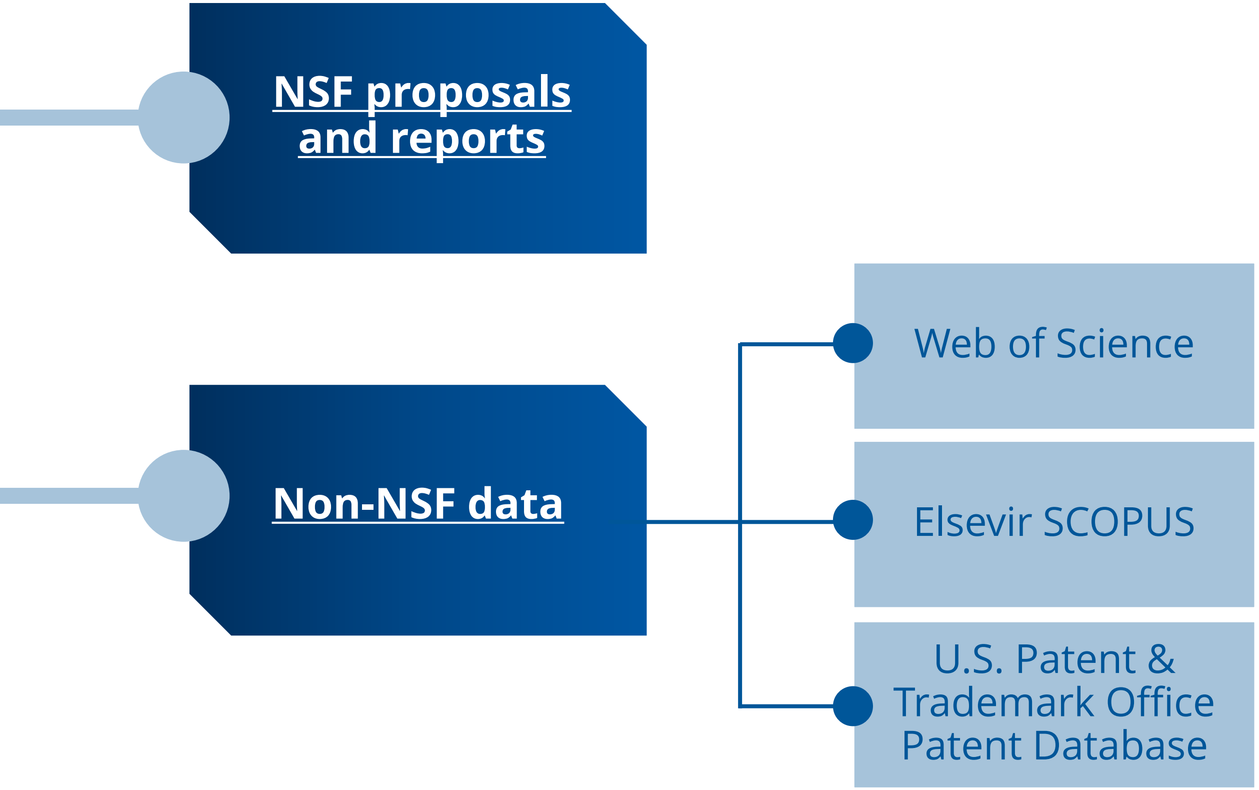
- Human oversight is a critical part of the validation process
- Process in place to ensure open-source information is accurate and represents the activies of the attributed individuals

Reporting

- Reporting requirements to OIG & other federal agencies outlined in guidelines
- What information may be shared detailed in the guidelines

Research Security Analytics

Data Used in Research Security Analyses



NSF proposals and reports

Non-NSF data

- Web of Science
- Elsevir SCOPUS
- U.S. Patent & Trademark Office Patent Database

Analysis Criteria & Purpose

- Mismatches between institutional affiliations in published papers and disclosed within proposals to NSF
- Mismatches between funding sources in published papers and disclosed Current and Pending within proposals to NSF
- Mismatches between filed patents in the USPTO and self-reported in NSF annual reports

Questions?

Contact Information:
Sarah Stalker-Lehoux
Deputy Chief of Research Security Strategy and Policy
sstalker@nsf.gov

Office of the Chief of Research Security Strategy and Policy:
research-protection@nsf.gov

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

NSF