

#COGROct2023

# Multi-Agency Panel on Research Security Risk Assessment & Analysis

*October 26, 2023*



# COGR

---



[www.cogr.edu](http://www.cogr.edu)

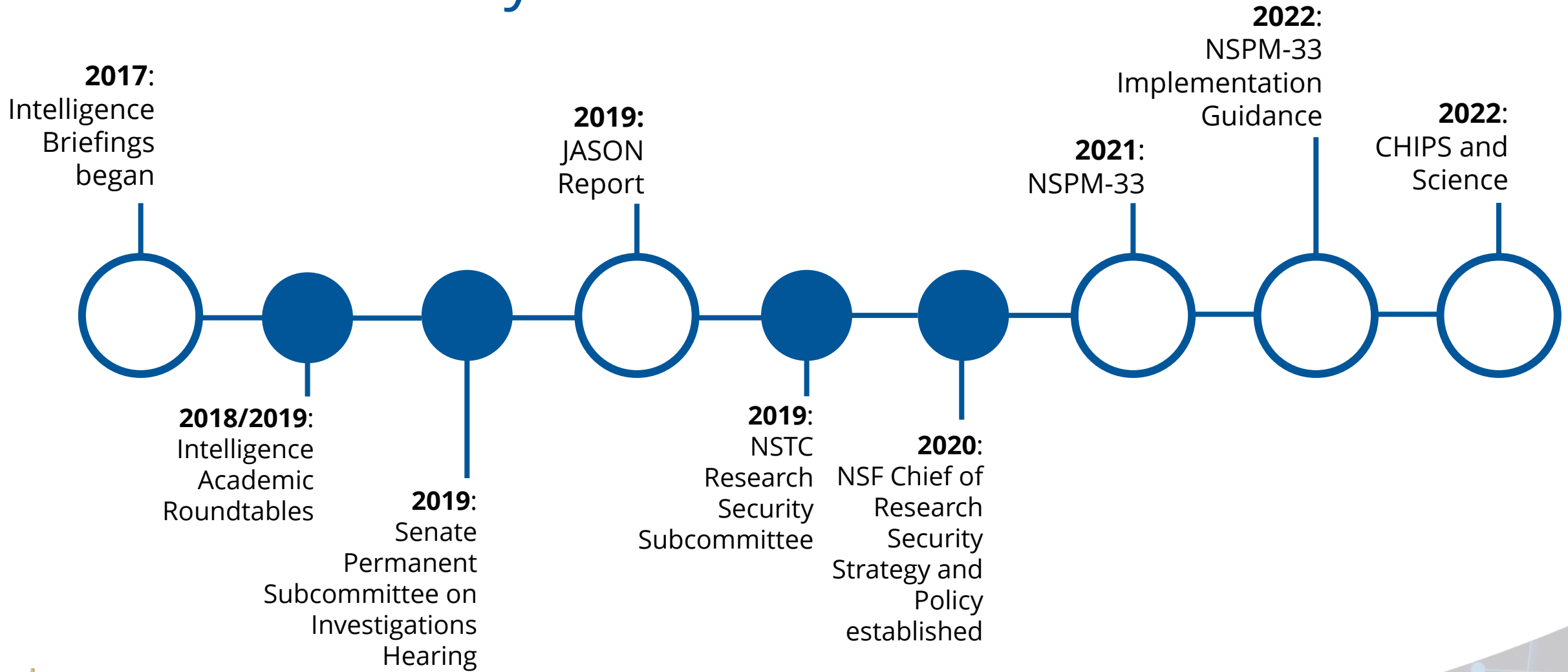


# Overview of Research Security Initiatives at NSF

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

*October 2023*

# Research Security Timeline





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



# The Chips and Science Act of 2022

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 (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

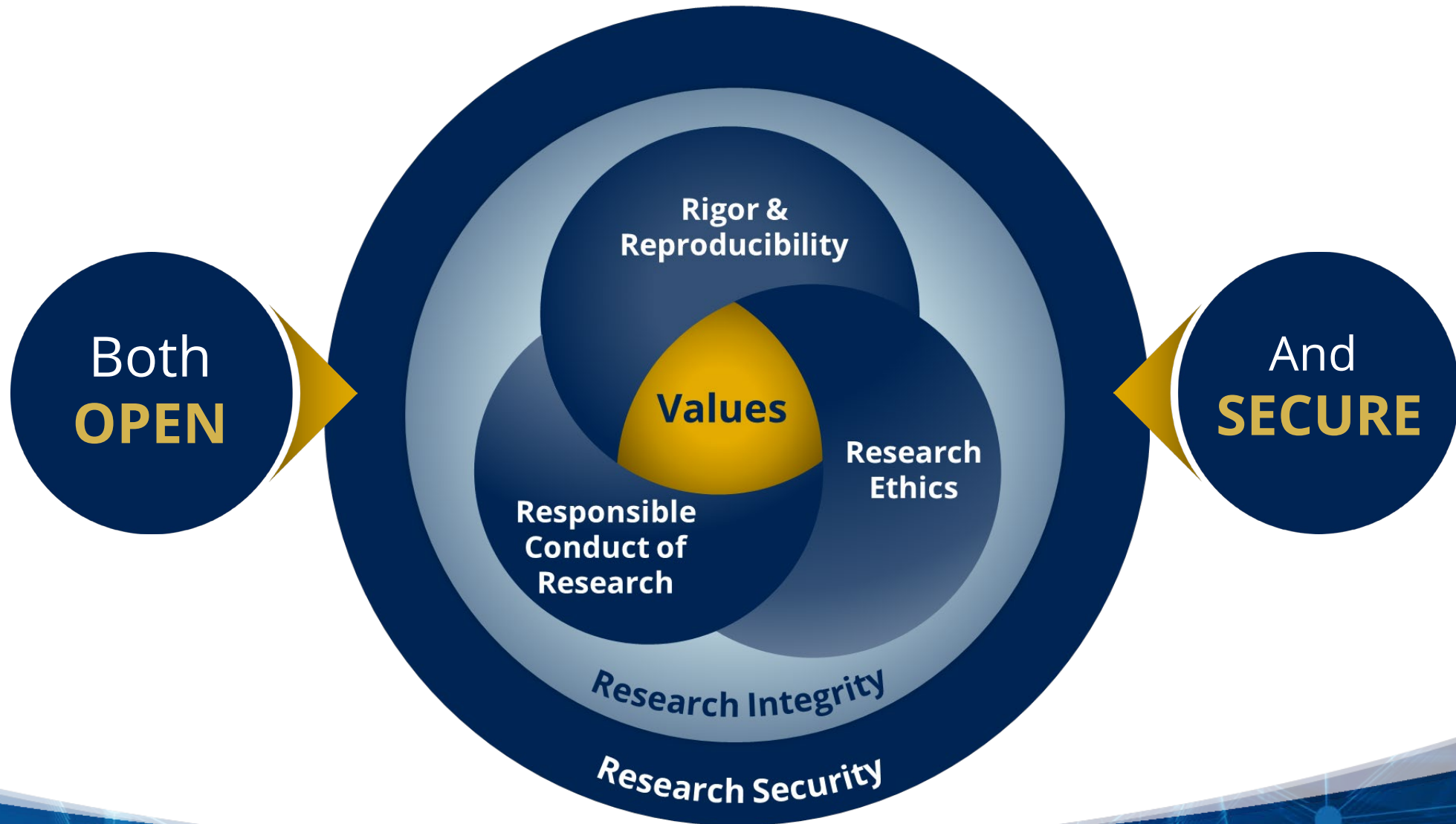
A photograph of President Joe Biden sitting at a wooden table outdoors, signing a document. He is wearing a blue suit and sunglasses. He is surrounded by a group of people, including Vice President Kamala Harris, who is clapping. Other people in the background are also clapping and smiling. The table has a seal of the President of the United States on it.

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





# Values are the Heart of Research Security



# SECURE

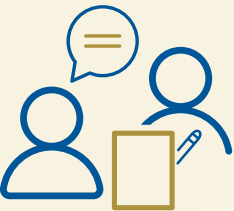
Safeguarding the Entire Community in  
the U.S. Research Ecosystem



# 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



# Research on Research Security Program (RRSP)



# 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





# 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



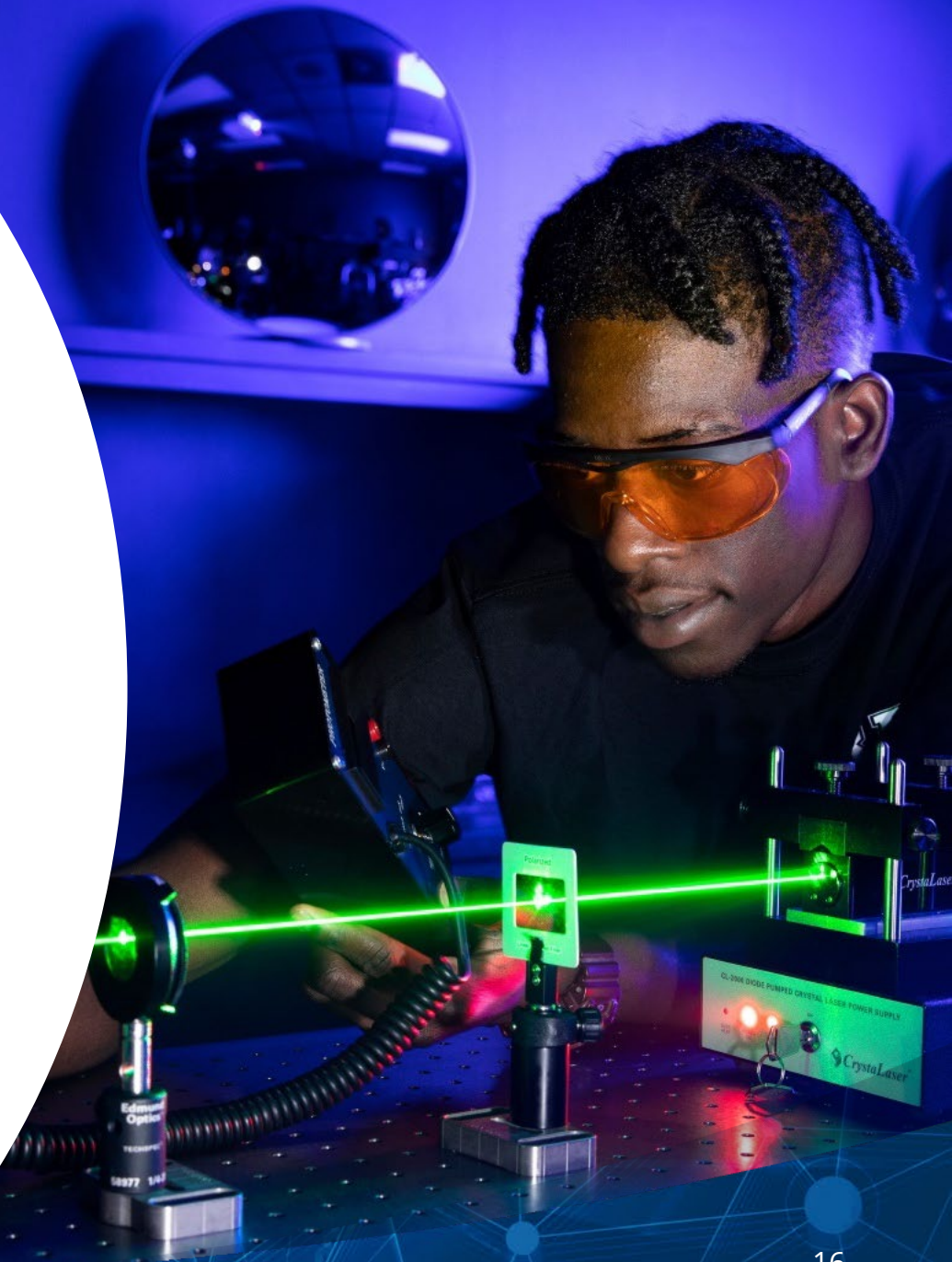


# Research Security Training Modules



# 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



# Module Topics

1

What is  
Research  
Security



2

Disclosure



3

Manage and  
Mitigate Risk



4

International  
Collaboration





# Standardized Disclosure Forms



# Standard 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**"
- National Science and Technology Council (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 research and development (R&D) grants or cooperative agreements
- The National Science Foundation (NSF) has agreed to serve as steward for these common forms as well as for posting and maintenance of the table entitled, *NSPM-33 Implementation Guidance Pre- and Post-award Disclosures Relating to the Biographical Sketch and Current and Pending (Other) Support*



# Drafts of these forms are currently available on NSF website

## 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*<sup>1</sup> 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.<sup>1</sup>

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](#).





# 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



## NSF guidelines for research security analytics

*Last updated February 2023*

### Table of Contents

Table of Contents.....	1
1. Summary.....	2
2. Foreword by the chief of research security strategy and policy .....	3
3. Review .....	5
4. Relevant authorities and supporting documentation.....	5
5. Definitions .....	5
6. Research security responsibilities and process of the Office of the Chief of Research Security Strategy and Policy.....	7
6.1 OCRSSP research security responsibilities .....	7
6.2 Process for notification and communication with institutions.....	10
7. Monitoring and reporting by NSF offices and staff.....	11
7.1 Terms and conditions compliance-monitoring responsibilities of program staff.....	11
7.2 Vetting for employment.....	12
8. Permissible and prohibited practices for research security-related analytics by the CRSSP .....	12
8.1 Permissible approaches for research security analytics.....	12
8.2 Prohibited practices for research security analytics .....	13
8.3 Individual matching criteria for validation and information sharing activities .....	13
9. Data, services and methods used for research security analytics .....	14
9.1 Non-NSF data used in research security analyses.....	14
9.2 Analysis criteria and purpose .....	15
9.3 Services used in research security analyses.....	15
10. Sharing guidelines for security-related information .....	15
10.1 Human oversight .....	15
10.2 Sharing of information with institutions .....	15
10.3 Sharing of information by OCRSSP with inspector general or federal agencies.....	15

# 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 activities of the attributed individuals



## Reporting

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







# Office of Research, Technology, and Economic Security (RTES)

## RTES Vetting Center

---

Julie K. Anderson, Director  
October 2023



# Why is RTES Vetting Needed?

Examples of Threats



Foreign ownership, control and influence of an entity



Improper foreign influence of an individual or project



Conflicts of Interest/Commitment



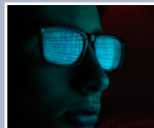
Intellectual Property (IP) Theft



Supply Chain



Equipment that could have questionable components

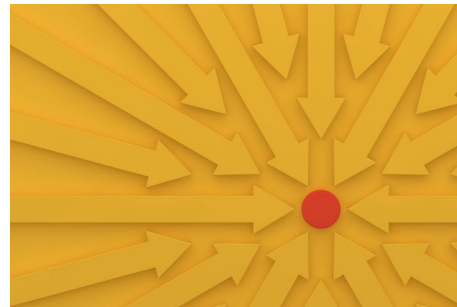


Physical threats

The U.S. and our allies continue to face serious research, technology, and economic security (RTES) threats as some foreign governments work aggressively to acquire our most advanced technologies and dominate strategic supply chains.

## Why is it important to the Department of Energy?

Much of DOE's portfolio concerns critical and emerging (C&E) technology areas, which are of particular importance for U.S. technological competitiveness and national security strategies. C&E technologies are frequently the target of theft, espionage, and illegal export by adversaries.



Examples of Targets: Advanced Batteries; Advanced Computing; Advanced Engineering Materials; Advanced Manufacturing; Artificial Intelligence/machine learning; Autonomous systems and Robotics; Biotechnologies; Quantum Information Technologies; Next Generation Renewable Energy Generation and Storage; Semiconductors and microelectronics.





# Primary RTES Office Functions

## Due Diligence, Liaison & Assessment

- Conduct or facilitate due diligence reviews, in coordination with other internal reviews
- Develop comprehensive risk assessment frameworks
- Review FOAs and awards to ensure the appropriate RTES measures are in place

## Information Sharing (Internal)

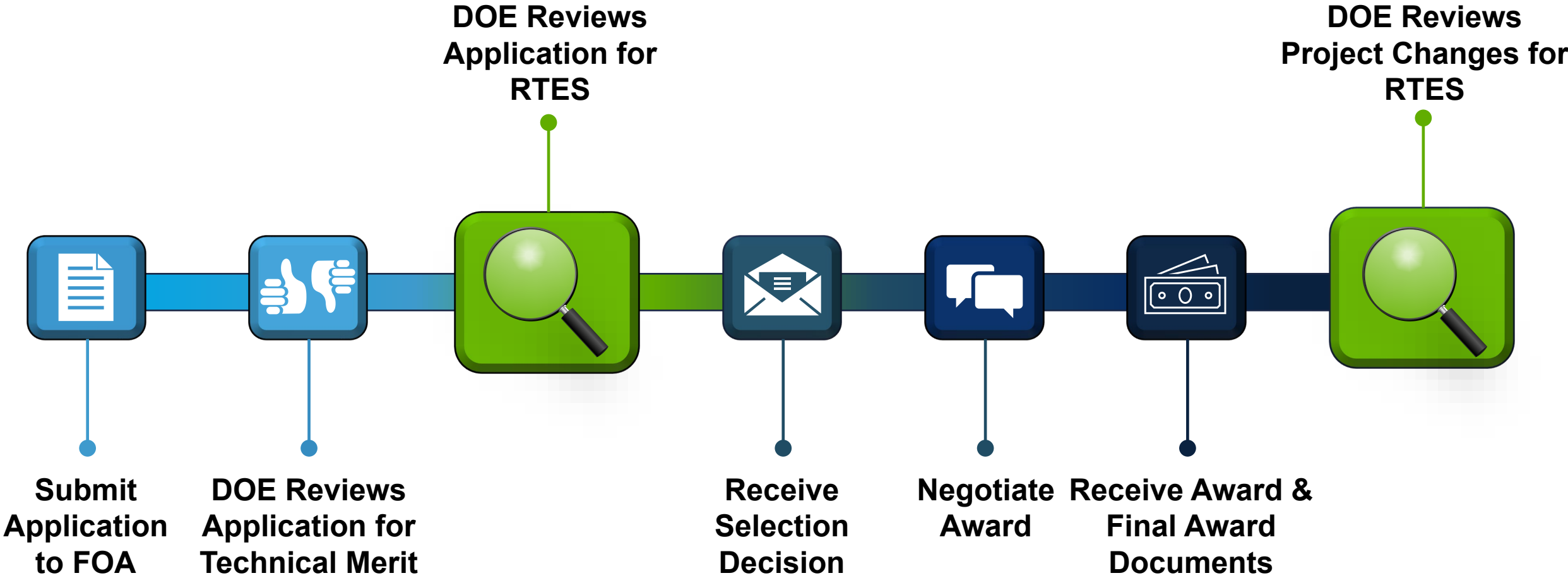
- Resource to program offices on RTES
- Foster cross-office information sharing through program RTES POCs
- Train offices on how to identify, communicate, and mitigate security risks

## Communications & Outreach (External)

Conduct outreach with the broader scientific community on RTES topics



# DOE RTES Due Diligence Reviews



# RTES-Related Application Disclosures

## For Individuals

-  CV/Resume/Biosketch
-  Current and Pending Support Disclosure
-  Ties to a Foreign Government Talent Recruitment Program
-  Conflicts of Interest

## For Organizations

-  % of foreign ownership/control, including whole or partial ownership by an entity in a country of risk (COR)
-  List of all directors (and board observers)
-  Ties to Foreign Government Talent Recruitment Programs sponsored by COR
-  Venture capital/institutional investors with ties to a COR; contractual/financial obligations with foreign enterprises
-  Technology licensing or IP sales to a COR in the last 5 years
-  Waiver requests for foreign work or foreign entity participation
-  Joint ventures or subsidiaries affiliated with a country of risk





# Clarifications & Due Process

**If more  
information is  
needed during  
DOE's RTES  
review**

## DOE is committed to:



Ensuring more consistency, transparency, and due process.



Allowing individuals and entities to provide clarifying information, where appropriate, and doing so prior to reaching a decision.



Providing more discretion and privacy.



Alignment with Section 10633 of the CHIPS and Science Act.



# Update for COGR on Research, Technology and Economic Security

Jeremy Ison

Senior Policy Advisor for Research Security

Office of the Under Secretary for Science and Innovation  
U.S. Department of Energy



U.S. DEPARTMENT OF  
**ENERGY**

Office of  
Science

[Energy/gov/science](https://www.energy.gov/science)

# DOE Mission Space

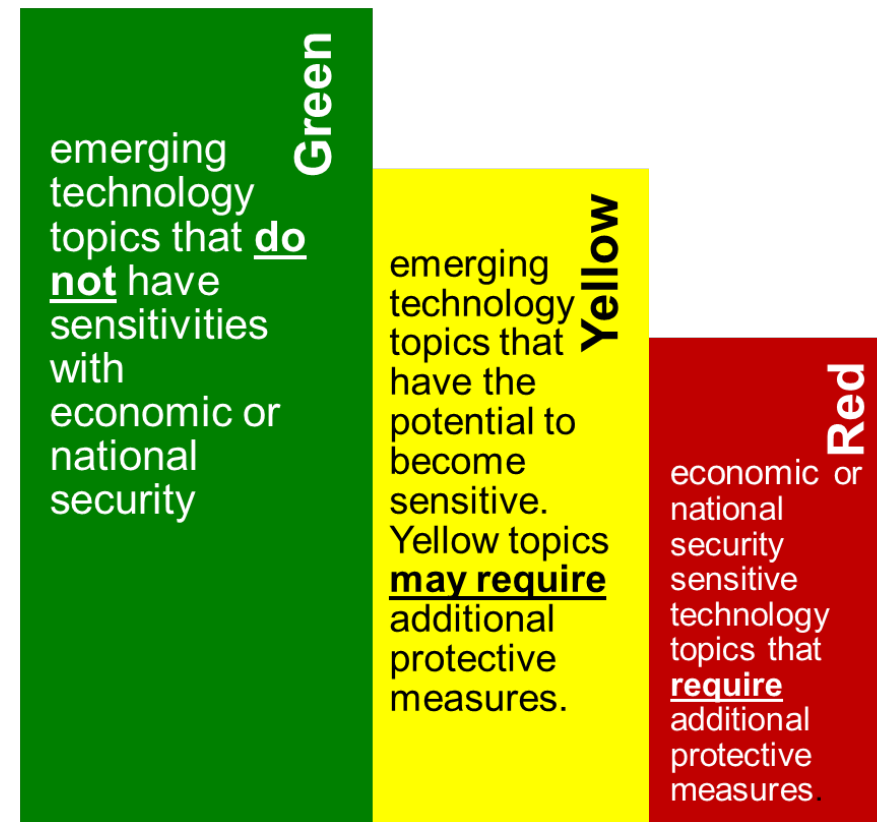
- DOE mission is broad: ranging from “quarks to quagmires and from weapons to windmills”
  - Types of Research: Discovery science to applied research to demonstration to deployment
  - Topics: Particle physics to the power grid
- Agency policies must be broad enough to cover a wide range of risks and equities, ranging from low-risk basic research to demonstration projects with national security implications.
- DOE and the National Labs must **BOTH**:
  - Balance protection of research results and IP in certain areas in order to bolster economic and national security interests
  - Promote international collaboration to maintain U.S. S&T competitiveness and leadership capabilities





# Update: DOE Laboratory Policy

- ◆ DOE uses its Science and Technology Risk Matrix to manage risks at the National Laboratories associated with critical and emerging technologies that do not otherwise have control mechanisms.
- ◆ Applies only to:
  - Countries of Concern (China, Russia, Iran, North Korea)
  - Guidance and management of certain activities at the national laboratories (e.g. foreign engagements, CRADAs/SPPs, official travel, foreign national access)
- ◆ Recent Developments:
  - DOE plans to update the S&T Risk Matrix annually with flexibility to edit on a rolling basis.
  - DOE plans to more broadly disseminate the Matrix to Laboratory staff to assist with implementation and to facilitate awareness/training on Matrix use.



# Foreign Government Sponsored or Affiliated Activities Order

- The Order's purpose is to continue the flow of scientific and technical information consistent with the Department of Energy's broad scientific mission, while also:
  - ensuring protection of U.S. competitive and national security interests and DOE program objectives
  - preventing potential conflicts of interest, e.g., financial interests, conflicts of commitment, and outside employment, which may undermine the DOE research enterprise
  - limiting unauthorized transfers of scientific and technical information
- The Order was expanded in September 2020 to include "Other Foreign Government Sponsored or Affiliated activities" managed by countries of risk
- These other activities include, employment, other support, grants/contracts, appointments to positions, etc.
- The Order prohibits participation in foreign talent recruitment programs from a country of risk and restricts participation in other foreign government sponsored or affiliated activities of a country of risk.
- The Order provides an option to seek an exemption for certain reported other activities, which will in turn be evaluated by risk and threat
- The Order requires disclosure of participation in country of risk talents programs and other sponsored activities and taking actions necessary to comply with the policy

# Update: Office of Science Financial Assistance

- ◆ The Office of Science (SC):
  - Continues to recommend universal disclosure (sources of support, positions and appointments)
  - Continues to recommend the use of SciENcv to reduce administrative burden by allowing the use of digital persistent identifiers
- ◆ SC is supportive of recent actions emerging from its interagency partners:
  - DoD Decision Matrix and Policy for Risk-based Reviews of Fundamental Research
  - NIST report on Safeguarding International Science
  - Continued development of NSF RSI-ISAO (Risk Assessment Center)
- ◆ Will look to these achievements and related policies as we continue to consider our approach to financial assistance.



# Update: Interagency and Community Engagement

- ◆ It is essential that DOE coordinates its research, technology and economic security policy with the interagency, and it is a priority to increase engagement with the research community.
  - Continuing to participate as co-chair on the National Science and Technology Council (NSTC) Subcommittee on Research Security.
  - Continuing to engage with allies and partners through State Department-led efforts.
  - Increasing public-facing engagements with leaders and membership of organizations such as COGR and others.

# Today's Discussion

- ◆ As we continue to evaluate our policies, we are here today to listen and learn from your experiences, perspectives, and recommended best practices.
- ◆ In particular, we are interested in hearing your thoughts and experiences:
  - How would you describe your community's experiences with DOE in the context of research security? How could those interactions be improved, and how do they compare with other funding agency interactions?

# Policy for Risk-Based Security Reviews of Fundamental Research

Bindu R. Nair  
Director, Basic Research  
OUSD(R&E)

10/26/2023

Controlled by: OUSD(R&E)  
Controlled by: Basic Research Office  
Category: Unclassified  
Distribution: A  
POC: Bindu Nair, (571) 372-6418







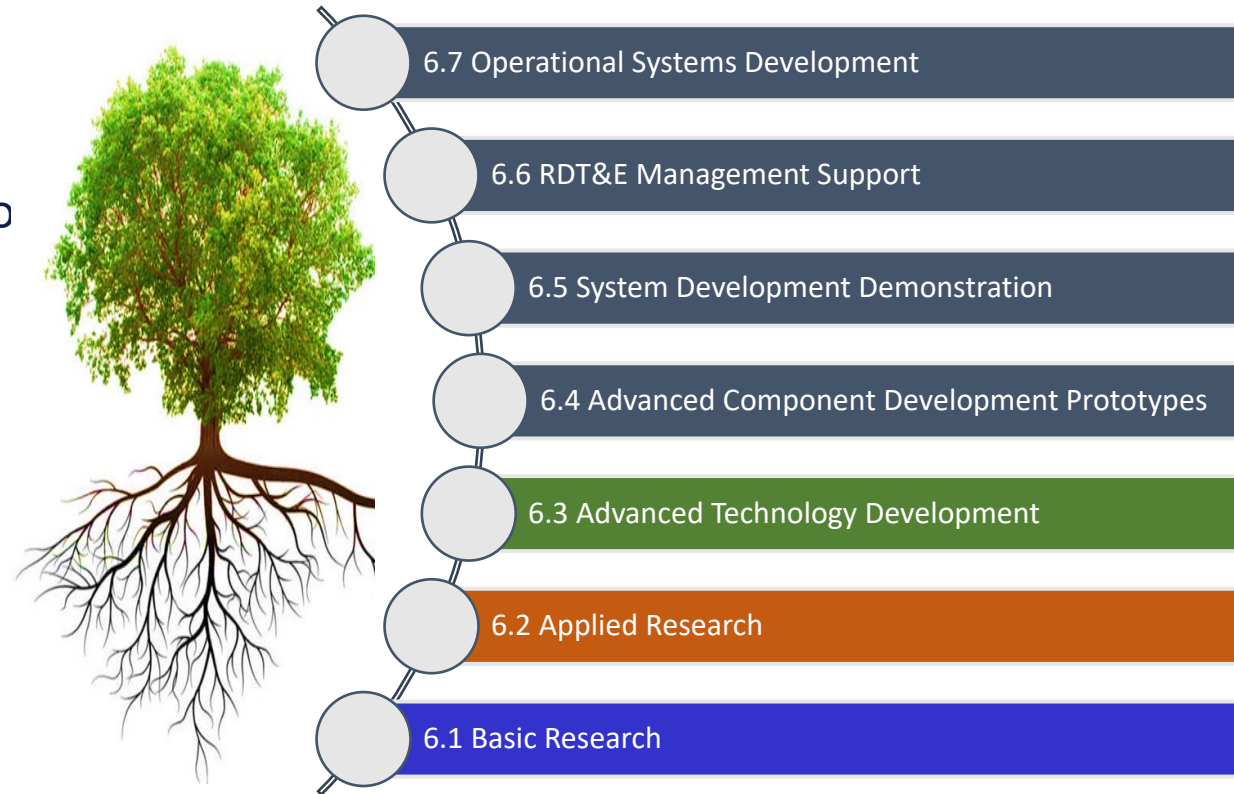
# Outline

- 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



# Securing DoD Dominance in Science and Technology Requires Investment in Open Science

- DoD invests in high technology readiness level research to advance known technologies. It has many protections around this type of research and does not conduct it in the open
- Investing in today's known problems is not enough to secure DoD's future advantage in science and technology
- DoD invests in fundamental research to source **radical ideas** that will lead to breakthroughs that will **reshape the military capabilities of the future**
- **Radical ideas come from highly trained highly creative people who are engaged in the global science conversation**
- DoD only engages in open science when the benefit outweighs the risk





# The Open Research Enterprise

- 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





# DoD's policy stems from an interagency directive

## 2021: National Security Presidential Memorandum – 33 (NSPM-33)

- ❑ NSPM-33 is an interagency coordinated activity to address foreign influence at academic institutions
- ❑ One directive is that heads of research funding agencies require disclosure of information related to potential **conflicts of interest & commitment** from participants in Federally-funded R&D
- ❑ 2022 National Science and Technology Council Implementation Guidance states: “Agencies should incorporate measures that are risk-based, in the sense that they provide meaningful contributions to addressing identified risks to research security and integrity and offer tangible benefit that justifies any accompanying cost or burden”



# Current status on Department-Wide Risk Based Review Procedures

- 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



DEPUTY SECRETARY OF DEFENSE  
1010 DEFENSE PENTAGON  
WASHINGTON, DC 20301-1010

DEC 14 2022

MEMORANDUM FOR SENIOR PENTAGON LEADERSHIP  
DEFENSE AGENCY AND DOD FIELD ACTIVITY DIRECTORS

SUBJECT: Department of Defense Memorandum on National Security Presidential  
Memorandum-33 Implementation

National Security Presidential Memorandum-33 (NSPM-33) on "United States Government-Supported Research and Development National Security Policy" (attached), dated January 14, 2021, directs a national response to safeguard the security and integrity of Federally-funded research and development in the United States. The Director of the Office of Science and Technology Policy (OSTP) is leading Federal research funding agencies, including the DoD, in developing research security measures and implementing NSPM-33. The National Science and Technology Council (NSTC) will serve as OSTP's lead office, charged to deliver an all-of-government approach to research security and a coordinated response to the threats facing the Nation's research enterprise.

As my representative to the NSTC, I am assigning the Under Secretary of Defense for Research and Engineering (USD(R&E)) the responsibility for oversight of NSPM-33 implementation for the DoD. In accordance with this assignment, the USD(R&E) is directed to ensure consistent implementation of NSPM-33 across the Department and to ensure that the Department's policies are aligned with those developed by other Federal agencies and those recommended by OSTP. To fulfill the requirements of NSPM-33, each of your Components is directed to take appropriate steps to secure Component-funded research efforts, including efforts for fundamental research, remain consistent with the NSTC's January 4, 2022 implementation guidance (attached) and any direction provided by the USD(R&E).

Within 30 days of this memorandum, I direct all Department Components to designate a point of contact for NSPM-33 implementation. Within 90 days of this memorandum, the USD(R&E) shall compile and disseminate a draft Department-level NSPM-33 implementation plan.

The USD(R&E) shall develop additional Department-level guidance, as necessary, to carry out the Department-level NSPM-33 implementation plan.

Attachments:  
As stated



OSD005055-22/CMD006428-22



# Policy for Risk-Based Security Reviews of Fundamental Research Policy

- 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.



RELEASE  
IMMEDIATE RELEASE

## Department of Defense Strengthening Efforts to Counter Unwanted Foreign Influence on DOD-Funded Research at Institutions of Higher Education

June 30, 2023 | f t r

The Department of Defense today announced the publication of a list of foreign entities that have been confirmed as engaging in problematic activity as described in Section 1286 of the Fiscal Year 2019 National Defense Authorization Act, as amended. These include practices and behaviors that increase the likelihood that DOD-funded research and development efforts will be misappropriated to the detriment of national or economic security or be subject to violations of research integrity or foreign government interference.

"Protecting and maintaining the integrity of our research enterprise is integral to national security," said Heidi Shyu, Under Secretary of Defense for Research and Engineering (USD(R&E)). "The publication of these foreign entities underscores our commitment to ensuring the responsible use of federal research funding and safeguarding our critical technologies from exploitation or compromise."

<https://www.defense.gov/News/Releases/Release/Article/3445601/department-of-defense-strengthening-efforts-to-counter-unwanted-foreign-influen/>

<https://media.defense.gov/2023/Jun/29/2003251160/-1/-1/1/COUNTERING-UNWANTED-INFLUENCE-IN-DEPARTMENT-FUNDED-RESEARCH-AT-INSTITUTIONS-OF-HIGHER-EDUCATION.PDF>



# Key Takeaways

- 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.





# DoD component risk-based security review

**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

- 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



# Decision matrix considers four factors to determine whether mitigation measures are needed

- **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 fulltime, 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.**



# Prohibited factors – prohibited by law

<b>Factor 1: Foreign Talent Recruitment Programs</b>	<b>Factor 2: Funding Sources</b>	<b>Factor 3: Patents</b>	<b>Factor 4: Entity Lists</b>
<p><b>For the Period after 9 Aug 2024</b></p> <p>Indicators of participation in a malign foreign talent recruitment program (MFTRP) meeting any of the criteria in Sec. 10638(4)(A)(i)-(ix) of the CHIPS and Science Act of 2022.</p> <p>Policy of Proposing Institution employing the covered individual does not prohibit participation in a MFTRP.</p>			



# No mitigation needed

Factor 1: Foreign Talent Recruitment Programs	Factor 2: Funding Sources	Factor 3: Patents	Factor 4: Entity Lists
<p>No indicator(s) of participation in an MFTRP; or</p> <p>No indicator(s) of participation in an FTRP meeting any of the criteria in Sec. 10638(4)(A)(i)-(ix) of the CHIPS and Science Act of 2022.</p>	<p>No indicator(s) that the covered individual is receiving or has received funding from an FCOC or an FCOC-connected entity.</p>	<p>All patent application(s) or patent(s), resulting from research funded by the USG, have been filed in the U.S. prior to filing in any other country.</p>	<p>No indicator(s) of any association or affiliation with an entity on: the U.S. BIS Entity List, the Annex of EO 14032, or superseding EOs, Sec. 1260H of the NDAA for FY 2021, Sec. 1286 of the NDAA for FY 2019, as amended, and no indicator(s) of publication in S&amp;E journals co-authored with an individual on the U.S. BIS Denied Persons List.</p>





# Mitigation measures suggested

Factor 1: Foreign Talent Recruitment Programs	Factor 2: Funding Sources	Factor 3: Patents	Factor 4: Entity Lists
<p><b>For the period after 10 Oct 2019:</b></p> <p>Covered individual’s co-author(s)<sup>9</sup> on publications in scientific and engineering (S&amp;E) journals are participants in an MFTRP or an FTRP meeting any of the criteria in Sec. 10638(4)(A)(i)-(ix) of the CHIPS and Science Act of 2022.</p> <p><b>For the period prior to 10 Oct 2019:</b></p> <p>Indicator(s) of participation in a FTRP meeting any of the criteria in Sec. 10638(4)(A)(i)-(ix) of the CHIPS and Science Act of 2022.</p>	<p><b>For the period prior to 10 Oct 2019:</b></p> <p>Indicator(s) that the covered individual received limited or partial funding from a FCOC or an FCOC-connected entity.</p>	<p>Patent application(s) or patent(s) not disclosed in fundamental research project proposal, that resulted from research funded by the USG, that were filed in a non-FCOC prior to filing in the U.S. or on behalf of an entity in a non-FCOC.</p> <p>Co-patent applicant with a person on the U.S. BIS Denied Persons List.<sup>10</sup></p>	<p><b>For the period after 10 Oct 2019:</b></p> <p>Covered individual’s co-author(s) on publications in S&amp;E journals are affiliated with an entity on: the U.S. BIS Entity List, the Annex of EO 14032 or superseding EOs, Sec. 1260H of the NDAA for FY 2021, or Sec. 1286 of the NDAA for FY 2019, as amended.</p> <p>Covered individual is a co-author on a publication in an S&amp;E journal with a person on the U.S. BIS Denied Persons List.</p> <p><b>For the period prior to 10 Oct 2019:</b></p> <p>Indicator(s) of association with an entity on: the U.S. BIS Entity List, the Annex of EO 14032 or superseding EOs, Sec. 1260H of the NDAA for FY 2021, or Sec. 1286 of the NDAA for FY 2019, as amended.</p>



# Mitigation measures recommended

Factor 1: Foreign Talent Recruitment Programs	Factor 2: Funding Sources	Factor 3: Patents	Factor 4: Entity Lists
<p><b>For the period between 10 Oct 2019<sup>8</sup> and 9 Aug 2022:</b></p> <p>Indicator(s) of participation in an FTRP meeting any of the criteria in Sec. 10638(4)(A)(i)-(ix) of the CHIPS and Science Act of 2022.</p> <p><b>For the period after 9 Aug 2022:</b></p> <p>Policy of proposing institution employing each covered individual does not prohibit participation in a MFTRP.</p>	<p><b>For the period between 10 Oct 2019 and 9 Aug 2022:</b></p> <p>Indicator(s) that the covered individual received funding from a FCOC or an FCOC-connected entity.</p>	<p>Patent application(s) or patent(s) disclosed in proposal, resulting from research funded by the USG, that were filed in an FCOC prior to filing in the U.S. or on behalf of an FCOC-connected entity.</p>	<p><b>For the period between 10 Oct 2019 and 9 Aug 2022:</b></p> <p>Indicator(s) of association with an entity on: the U.S. BIS Entity List, the Annex of EO 14032 or superseding EOs, Sec. 1260H of the NDAA for FY 2021, or Sec. 1286 of the NDAA for FY 2019, as amended.</p> <p><b>For the period prior to 10 Oct 2019:</b></p> <p>Indicator(s) of an affiliation with an entity on: the U.S. BIS Entity List, the Annex of EO 14032 or superseding EOs, Sec. 1260H of the NDAA for FY 2021, or Sec. 1286 of the NDAA for FY 2019, as amended.</p>



# Mitigation measures required, factors discouraged by DoD policy, rejection of proposal if no mitigation possible

Factor 1: Foreign Talent Recruitment Programs	Factor 2: Funding Sources	Factor 3: Patents	Factor 4: Entity Lists
<p><b>For the period after 9 Aug 2022<sup>1</sup>:</b></p> <p>Indicator(s)<sup>2</sup> of participation<sup>3</sup> in a foreign talent recruitment program (FTRP) meeting any of the criteria in Sec. 10638(4)(A)(i)-(ix) of the CHIPS and Science Act of 2022.</p>	<p>Indicator(s) that the covered individual is currently receiving funding from a Foreign Country of Concern (FCOC) or a FCOC-connected entity.</p>	<p>Patent application(s) or patent(s) not disclosed in proposal, that resulted from research funded by the U.S. Government (USG), that were filed in an FCOC prior to filing in the U.S. or filed on behalf of an FCOC-connected entity.</p>	<p><b>For the period after 9 Aug 2022:</b></p> <p>Indicator(s) of association with an entity on: the U.S. Bureau of Industry and Security (BIS) Entity List,<sup>4</sup> the Annex of Executive Order (EO) 14032<sup>5</sup> or superseding EOs, Sec. 1260H of the National Defense Authorization Act (NDAA) for FY 2021,<sup>6</sup> or Sec. 1286 of the NDAA for FY 2019, as amended.<sup>7</sup></p> <p><b>For the period after 10 Oct 2019:<sup>6</sup>:</b></p> <p>Indicator(s) of affiliation with an entity on: the U.S. BIS Entity List, the Annex of EO 14032 or superseding EOs, Sec. 1260H of the NDAA for FY 2021, or Sec. 1286 of the NDAA for FY 2019, as amended.</p>



# 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





# FY22 Lists Published in Response to Section 1286 of 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



# Table 1: List of Institutions of the People's Republic of China, Russian Federation, and other Countries with Specific Characteristics - Page 1 of 2

Academy of Military Medical Sciences (AMMS)
Academy of Military Medical Sciences, Field Blood Transfusion Institution
Academy of Military Medical Sciences, Institute of Basic Medicine
Academy of Military Medical Sciences, Institute of Bioengineering
Academy of Military Medical Sciences, Institute of Disease Control and Prevention a.k.a. <ul style="list-style-type: none"> <li>Disease Control and Prevention Institute</li> </ul>
Academy of Military Medical Sciences, Institute of Health Service and Medical Information
Academy of Military Medical Sciences, Institute of Hygiene and Environmental Medicine
Academy of Military Medical Sciences, Institute of Medical Equipment
Academy of Military Medical Sciences, Institute of Microbiology and Epidemiology a.k.a. <ul style="list-style-type: none"> <li>Institute of Microbial Epidemiology</li> </ul>
Academy of Military Medical Sciences, Institute of Radiation and Radiation Medicine a.k.a. <ul style="list-style-type: none"> <li>Institute of Radiation and Radiation Medicine</li> <li>Institute of Electromagnetic and Particle Radiation Medicine</li> </ul>
Academy of Military Medical Sciences, Institute of Toxicology and Pharmacology a.k.a. <ul style="list-style-type: none"> <li>Institute of Toxicology and Drugs</li> </ul>
Academy of Military Medical Sciences, Military Veterinary Research Institute
Beijing Aeronautical Manufacturing Technology Research Institute (BAMTRI) a.k.a. <ul style="list-style-type: none"> <li>Aviation Industry Corporation of China's (AVIC) Institute 625</li> </ul>
Beijing Computational Science Research Center (BCSRC) a.k.a. <ul style="list-style-type: none"> <li>Beijing Computing Science Research Center</li> <li>CSRC</li> </ul>
Beijing Institute of Technology
Beijing University of Aeronautics and Astronautics (BUAA) a.k.a. <ul style="list-style-type: none"> <li>Beihang University</li> </ul>
Beijing University of Posts and Telecommunications (BUPT)
Center for High Pressure Science and Technology Advanced Research (HPSTAR) a.k.a. <ul style="list-style-type: none"> <li>Beijing High Voltage Research Center</li> </ul>

Chinese Academy of Engineering Physics (CAEP) a.k.a. <ul style="list-style-type: none"> <li>Ninth Academy</li> <li>Southwest Computing Center</li> <li>Southwest Institute of Applied Electronics</li> <li>Southwest Institute of Chemical Materials</li> <li>Southwest Institute of Electronic Engineering</li> <li>Southwest Institute of Environmental Testing</li> <li>Southwest Institute of Explosives and Chemical Engineering</li> <li>Southwest Institute of Fluid Physics</li> <li>Southwest Institute of General Designing and Assembly</li> <li>Southwest Institute of Machining Technology</li> <li>Southwest Institute of Materials</li> <li>Southwest Institute of Nuclear Physics and Chemistry (a.k.a., China Academy of Engineering Physics (CAEP) 902 Institute)</li> <li>Southwest Institute of Research and Applications of Special Materials Factory</li> <li>Southwest Institute of Structural Mechanics</li> <li>The High Power Laser Laboratory, Shanghai</li> <li>The Institute of Applied Physics and Computational Mathematics, Beijing</li> <li>901 Institute</li> </ul>
Chinese Academy of Sciences - Shenyang Institute of Automation
Federal Research Center Boreskov Institute of Catalysis
Federal State Budgetary Institution of Science P.I.K.A. Valiev RAS of the Ministry of Science and Higher Education of Russia a.k.a. <ul style="list-style-type: none"> <li>FTIAN IM K.A.Valiev RAS</li> <li>FTI RAS</li> <li>FTIAN</li> </ul>
Harbin Engineering University
Harbin Institute of Technology
Hefei National Laboratory for Physical Sciences at the Microscale
Institute of High Energy Physics (IHEP) a.k.a. <ul style="list-style-type: none"> <li>Kurchatovskiy Institute ITEF</li> </ul>
Institute of Solid-State Physics of the Russian Academy of Sciences (ISSP) a.k.a. <ul style="list-style-type: none"> <li>Institute of Solid-State Physics of the Academy of Sciences SSSR</li> <li>Federal State Budgetary Institution of Science Institute of Solid-State Physics N.A. Yu. A. Osipyanof the Russian Academy of Sciences</li> </ul>
Mabna Institute
Moscow Institute of Physics and Technology (MIPT) a.k.a. <ul style="list-style-type: none"> <li>MFTI</li> </ul>



# Table 1: List of Institutions of the People’s Republic of China, Russian Federation, and other Countries with Specific Characteristics - Page 2 of 2

Moscow Order of the Red Banner of Labor Research Radio Engineering Institute JSC a.k.a. <ul style="list-style-type: none"> <li>• MNIRTI JSC</li> </ul>
Nanjing University of Aeronautics and Astronautics
Nanjing University of Science and Technology
National University of Defense Technology (NUDT) a.k.a. <ul style="list-style-type: none"> <li>• Central South CAD Center</li> <li>• CSCC</li> <li>• Hunan Guofang Keji University</li> </ul>
Northwestern Polytechnical University a.k.a. <ul style="list-style-type: none"> <li>• Northwestern Polytechnic University</li> <li>• Northwest Polytechnic University</li> <li>• Northwest Polytechnical University</li> </ul>
Ocean University of China
Rzhanov Institute of Semiconductor Physics, Siberian Branch of Russian Academy of Sciences a.k.a. <ul style="list-style-type: none"> <li>• IPP SB RAS</li> <li>• Institute of Semiconductor Physics IM A.V. Rzhanov</li> </ul>
Sichuan University
Sun Yat-Sen University
Tactical Missile Corporation, Concern “MPO—Gidropribor” a.k.a. <ul style="list-style-type: none"> <li>• Joint Stock Company Concern Sea Underwater Weapons Gidropribor</li> <li>• Research Institute “Gidpropridor”</li> </ul>
Tactical Missile Corporation, Joint Stock Company GosNIIMash a.k.a. <ul style="list-style-type: none"> <li>• PPORosprofprom V “GOSNIIMASH”</li> <li>• State Research Institute of Mechanical Engineering</li> <li>• Pervichnaya Profsoyuznaya Organizatsiya Rossiskogo Profsoyuza Rabotnikov Promyshlennosti V</li> <li>• “GOSNIIMASH”</li> <li>• Joint Stock Company “State Research Institute of Mechanical Engineering” named after “V.V.Bakhirev”</li> <li>• SKB DNIKhTI</li> </ul>
Tianjin University
University of Electronic Science and Technology of China



## Table 2: Foreign Talent Programs that Pose a Threat to National Security Interests of the United States

Changjiang Scholar Distinguished Professorship
Hundred Talents Plan
Pearl River Talent Program
Project 5-100
River Talents Plan
Thousand Talents Plan
Any program that meets one of the criteria contained in Section 10638 (4)(A) and either Section 10638 (4)(B)(i) or (ii) in the CHIPS and Science Act





# Contact Us

- 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](mailto: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:  
<https://www.defense.gov/News/Releases/Release/Article/3445601/departments-of-defense-strengthening-efforts-to-counter-unwanted-foreign-influen/>