NCURA
Supporting Research...together™

NCURA
66TH ANNUAL
MEETING

REDISCOVER
Y-OUR JOURNEY

AUGUST 4 - 7, 2024
WASHINGTON, DC

NSPM-33 and CHIPS Act Requirements: Current Status and Options for Implementation and Communications

CONTINUING EDUCATION: **Continuing Education Unit (CEU)** transcripts will be added to your NCURA Dashboard by 9/27. **CPE credits** for Certified Public Accountants - make note of the code provided in the Concurrent Sessions and Workshops to add to the survey post-conference.

INCLUSION: Pronouns are included on NCURA participant badges – please make sure to use your colleagues pronouns when addressing them.

Presenters please **use a microphone** *at all times* in the concurrent session rooms and repeat questions to support those needing amplification to hear.

Workshop Agenda

1:00 – 1:20 Introductions and polling

1:20 – 1:45 Overview of NSPM-33 & CHIPS Act research security requirements

1:45 – 2:30 Federal agency and university/institution implementation part I

2:30 – 2:45 Break

2:45 – 3:15 Federal agency and university/institution implementation part II

3:15 – 3:45 The SECURE Center and university implementation

3:45 – 4:15 Stakeholder engagement, benchmarking preparedness, and prioritization

4:15 – 4:30 Faculty guidance

Rebecca Keiser, PhD
National Science Foundation

Elizabeth Wagner
Purdue University

Lisa Nichols, PhD
University of Michigan

Amy Weber
Northwestern University

Holly Bante, PhD
University of Cincinnati

NSPM-33 and CHIPS Act Requirements Workshop: Current Status and Options for Implementation and Communication

Poll Questions

NCURA 66TH
ANNUAL MEETING

Rediscover Y-OUR Journey

Overview: NSPM-33 & CHIPS Act Research Security Requirements

NSPM-33 & CHIPS Act - Research Security Regulations

The **CHIPS and Science Act** of 2022 contained several research security provisions and requirements, including a malign foreign talent program prohibition.

NSPM-33 "…strengthen protections of USG supported R&D against foreign govt. interference and exploitation."

- Protect intellectual capital
- Discourage research misappropriation
- Ensure responsible management of U.S. taxpayer dollars, including full disclosure of potential COIs & COCs

How did we get here?

FBI Director Christopher Wray's testimony: Senate Hearing on Worldwide Threats

February 2018: Hearing focused on **China**, suggesting **infiltration of academia (by foreign professors, scientists, and students) and that Confucius Institutes are vehicles for propaganda.**

As quoted in one publication, *"They're exploiting the very open research-and-development environment that we have, which we all revere, but they're taking advantage of it," Wray said, adding that there was a "naiveté" among academics about the risks posed by foreign nationals at U.S. universities."*

Improper foreign interference and malign foreign influence

Foreign interference and influence are malign activities by another country to interfere with or influence U.S. policies or activities, or to benefit the foreign government.

Some foreign countries seek to illegally acquire U.S. academic research to advance their scientific, economic, and military development. Saving significant time, money, and resources while achieving generational advances in technology.

These malign activities deprive victimized parties of revenue and credit for their work and use U.S. funding to advance their technology goals.

The malign efforts can come in many forms, including overt theft, plagiarism, elicitation, and the commercialization of early-stage collaborative research.

How did we get here?

Inappropriate sharing of grant applications and other disruptions to the peer review process.

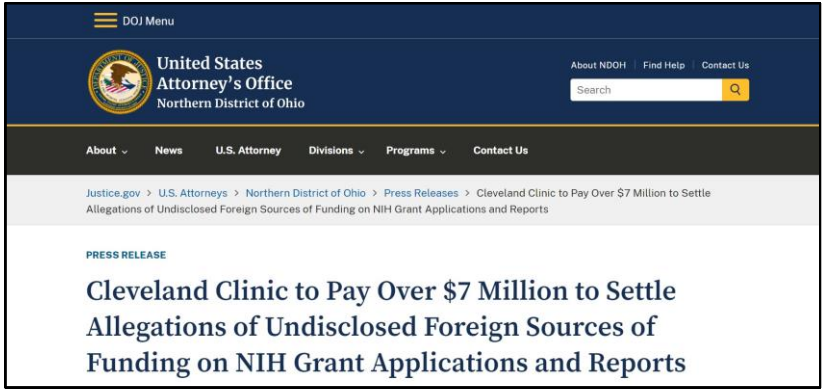
Conducting the same, or similar, research at two institutions (aka having a “shadow lab”) and/or having the same project supported by both U.S. federal funds and foreign funds.

Incomplete disclosure of relationships with foreign governments or institutions to R&D sponsors and the investigator’s home institution.

NCURA 66TH
ANNUAL MEETING

Institutional Responsibility

Cleveland Clinic - $7 million settlement



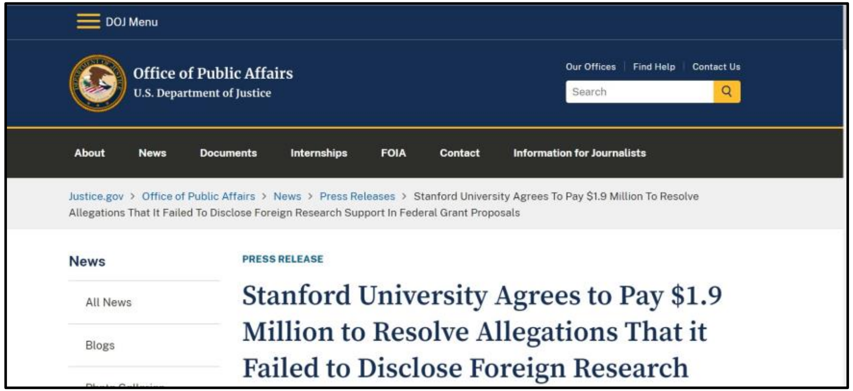
Justice.gov > U.S. Attorneys > Northern District of Ohio > Press Releases > Cleveland Clinic to Pay Over $7 Million to Settle Allegations of Undisclosed Foreign Sources of Funding on NIH Grant Applications and Reports

PRESS RELEASE

Cleveland Clinic to Pay Over $7 Million to Settle Allegations of Undisclosed Foreign Sources of Funding on NIH Grant Applications and Reports

- Alleged mismanagement of 3 grants
- Allowed employees to share passwords to NIH's reporting system

Stanford - $1.9 million settlement



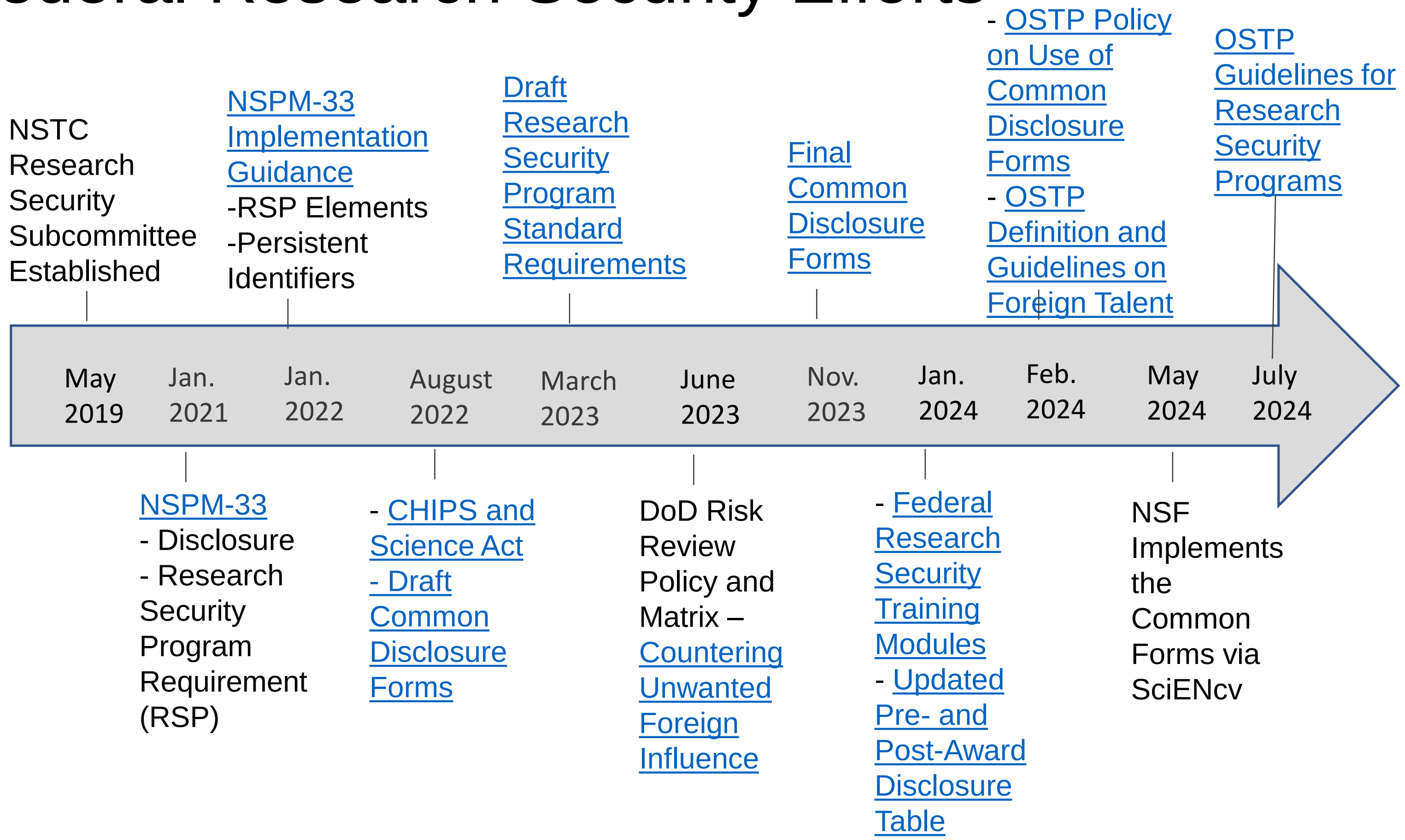
Justice.gov > Office of Public Affairs > News > Press Releases > Stanford University Agrees To Pay $1.9 Million To Resolve Allegations That It Failed To Disclose Foreign Research Support In Federal Grant Proposals

PRESS RELEASE

Stanford University Agrees to Pay $1.9 Million to Resolve Allegations That it Failed to Disclose Foreign Research

2015-2020: 16 grant proposals failed to disclose current or pending funding from foreign sources for 11 Stanford researchers

Federal Research Security Efforts



May 2019
NSTC Research Security Subcommittee Established

Jan. 2021
NSPM-33
- Disclosure
- Research Security Program Requirement (RSP)

Jan. 2022
NSPM-33 Implementation Guidance
-RSP Elements
-Persistent Identifiers

August 2022
- CHIPS and Science Act
- Draft Common Disclosure Forms

March 2023
Draft Research Security Program Standard Requirements

June 2023
DoD Risk Review Policy and Matrix – Countering Unwanted Foreign Influence

Nov. 2023
Final Common Disclosure Forms

Jan. 2024
- Federal Research Security Training Modules
- Updated Pre- and Post-Award Disclosure Table

Feb. 2024
- OSTP Policy on Use of Common Disclosure Forms
- OSTP Definition and Guidelines on Foreign Talent

May 2024
NSF Implements the Common Forms via SciENcv

July 2024
OSTP Guidelines for Research Security Programs

NSPM-33

Strengthen Disclosure Requirements

- **"Agencies shall standardize disclosure processes, definitions, and forms across funding agencies to the extent practicable"**

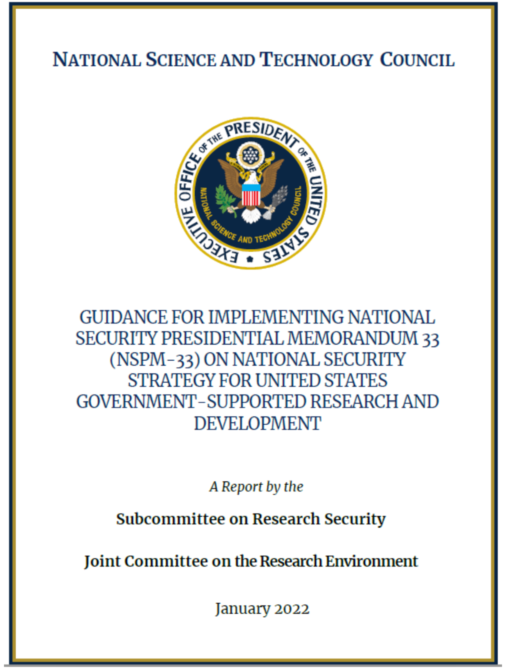
Require Persistent Identifiers (PIDs)

- Researchers on federal research grants

Establish a Research Security Program

- Research institutions receiving >$50 million federal S&E support annually
  - Cybersecurity
  - Foreign travel security
  - Research security training, and export control training, as appropriate

NSPM-33 Implementation Guidance



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

- Standardized "Common" biosketch and current and pending support disclosure forms - final forms published in Nov. 2023
- Research agencies should work to implement PIDs into their electronic systems/processes – NIH and DOE to require PIDs, others may follow
- Details on Research Security Programs: cybersecurity (14 elements), foreign travel security (organizational policy and record of covered international travel), and training
- A research security POC

Highlights from the CHIPS Act

Sec. 10331. Office of Research Security and Policy

NSF office to coordinate with OIG, research agencies, intel. & law enforcement, and NSTC to address risks to research enterprise. Office of Chief of Research Security, Strategy, and Policy

Sec. 10332. Chief of Research Security

Dr. Rebecca Keiser, Chief, OCRSSP and Co-chair NSTC Research Security Subcommittee

Sec. 10336. Authorities

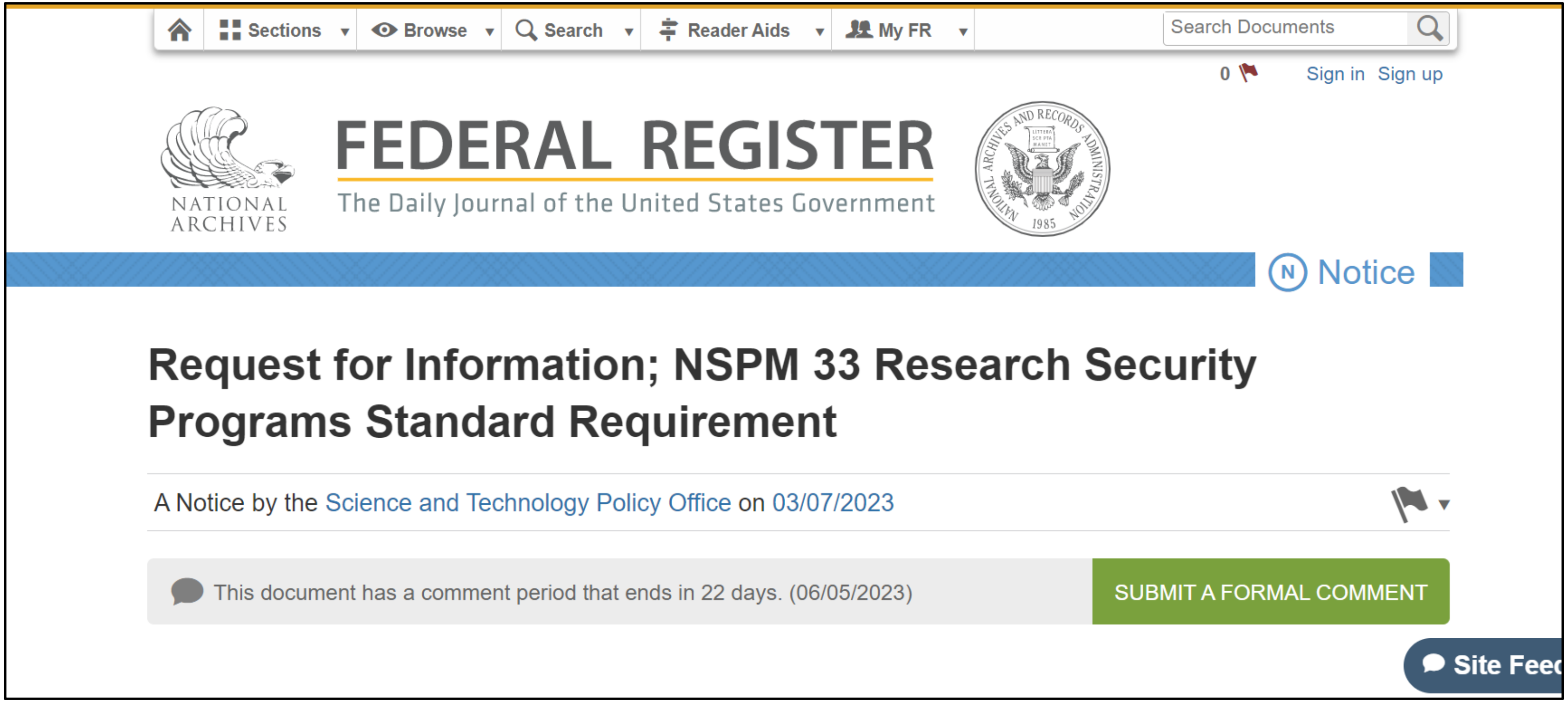
Authorizes the NSF OCRSSP, to conduct risk assessments of R&D applications/disclosures

Sec. 10338 - Research security and integrity information sharing analysis organization

…to enable the research community to share information, identify research security risks, and implement risk assessment and mitigation best practices.

Section 10632 of CHIPS and Science Act- MFTRP Prohibition

Section 10339B, Foreign Financial Reporting



Request for Information; NSPM 33 Research Security Programs Standard Requirement

A Notice by the Science and Technology Policy Office on 03/07/2023

This document has a comment period that ends in 22 days. (06/05/2023)

https://www.federalregister.gov/documents/2023/03/07/2023-04660/request-for-information-nspm-33-research-security-programs-standard-requirement

Draft Research Security Program Standards (March 2023)

Cybersecurity

- Compliance with 12 of 15 requirements of FAR 52.204-21 *Basic Safeguarding of Covered Contractor Information Systems.*

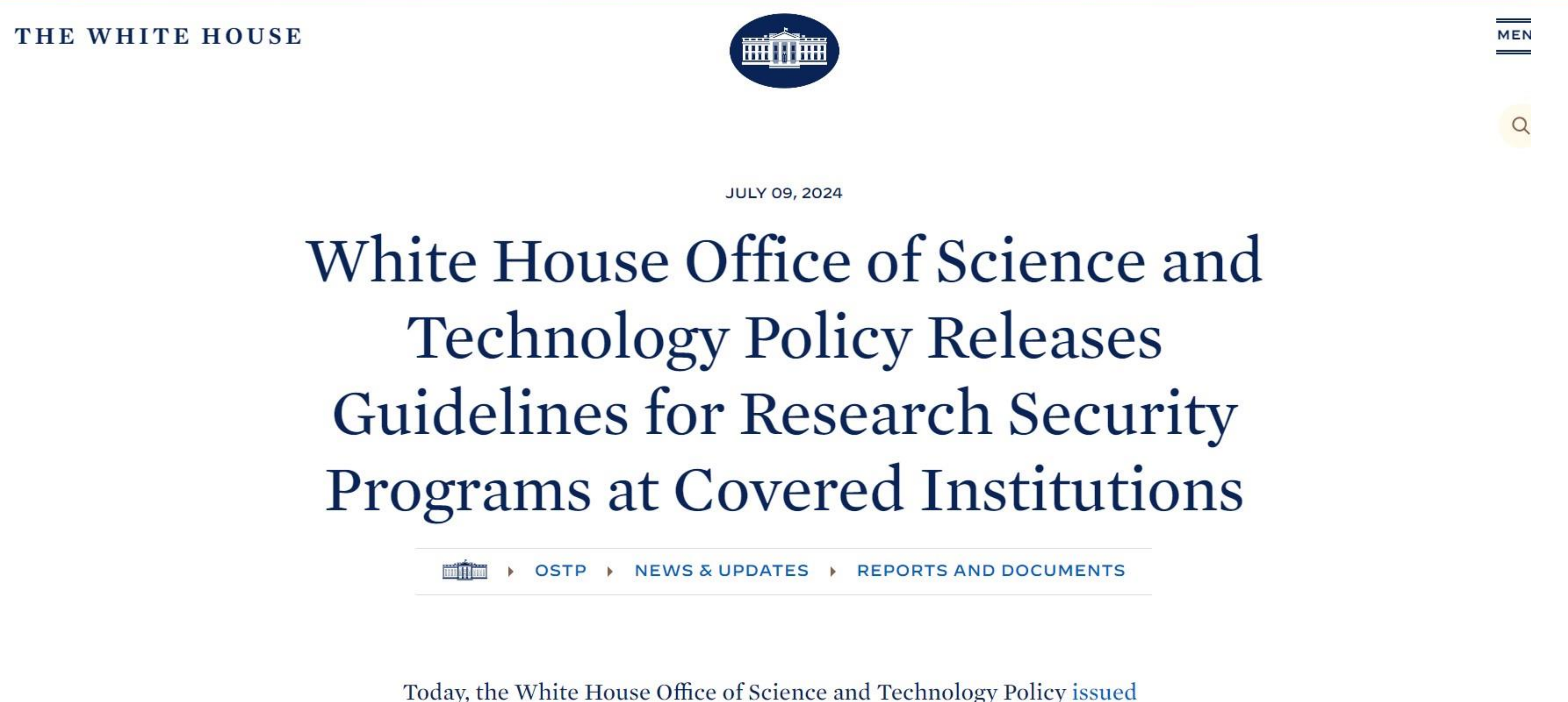
Foreign Travel Security

- Maintain org record of covered international travel by covered individuals
- Advanced disclosure and authorization
- Mandatory security briefings and advice regarding electronic device security prior to covered international travel or including electronic devices utilized/bought for federally funded R&D.

Research Security and Export Control Training

- Specific criteria for research security

Final Guidelines for Research Security Programs (July 2024)



THE WHITE HOUSE

JULY 09, 2024

White House Office of Science and Technology Policy Releases Guidelines for Research Security Programs at Covered Institutions

OSTP ▸ NEWS & UPDATES ▸ REPORTS AND DOCUMENTS

Today, the White House Office of Science and Technology Policy issued

Final Guidelines for Research Security Programs

Cyber Security

- Implement a cybersecurity program **one year** after publication of the final NIST cybersecurity resource (IR 8481: Cybersecurity for Research)

Foreign Travel Security

- Implement federal foreign travel security training to covered individuals (CI) within **1 year of availability** and at least every 6 yrs.
- Organizational record of CI international travel when agency determines security risks warrant travel reporting for an R&D award

Research SecurityTraining

- Implement research security training; certify CI completion
- Option A: NSF training modules
- Option B: Non-federal training that covers: (1) Improper transfer of USG-supported R&D; (2) importance of International research & talent

Export Control (EC) Training

- Provide EC training to CI working with controlled technology
- Option A: Govt. training (BIS, DDTC)
- Option B: Non-fed training with U.S. EC and compliance requirements & processes for reviewing foreign sponsors, collaborators, and partnerships

General consensus: Appreciation for flexibility, concern about agency latitude

Institutional Certifications

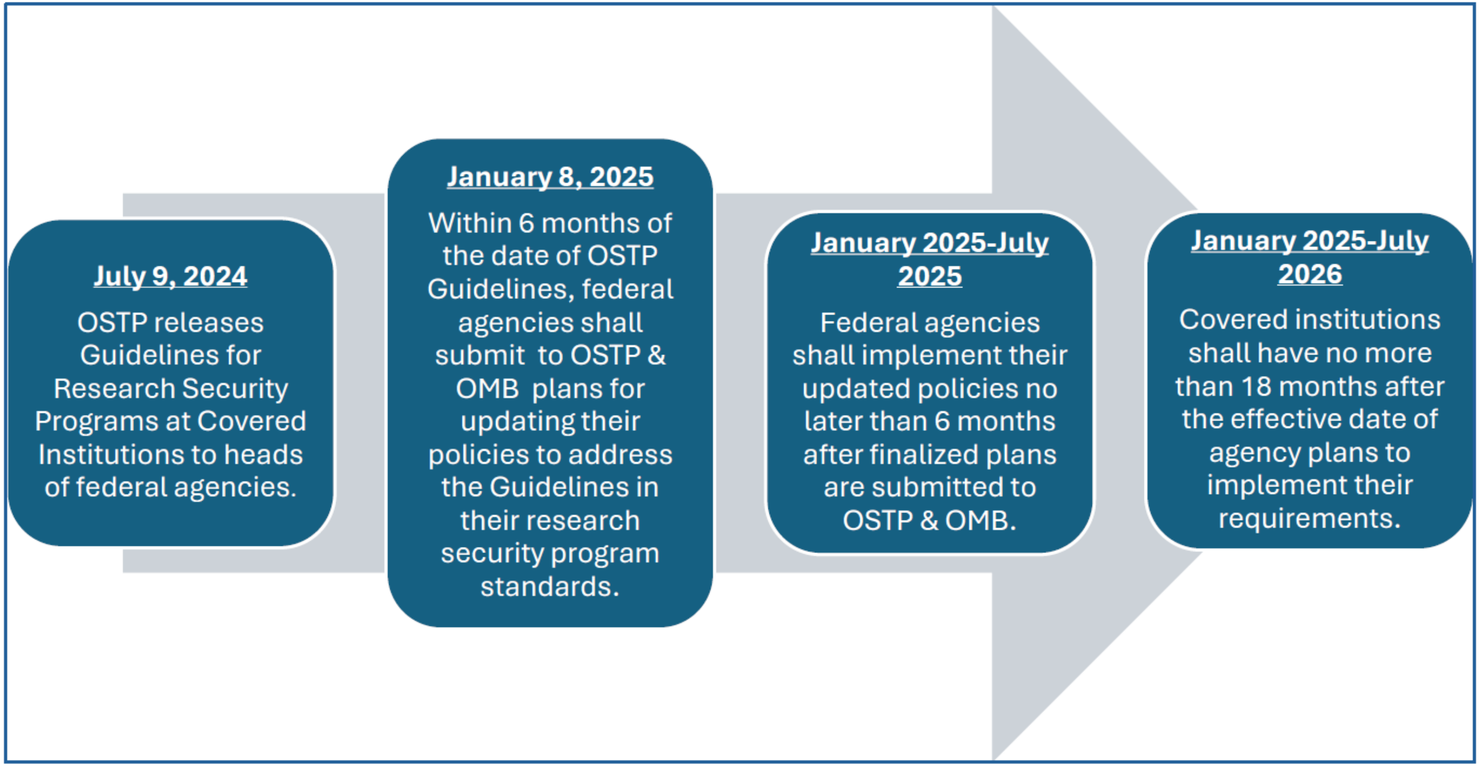
Certifications that universities/institutions have:

- A research security program, including:
  - Cybersecurity and foreign travel security
  - A research security training program for all CI,
    and EC training for CI who perform R&D involving export-controlled technologies
- Training on foreign travel security to CI engaged in international travel at least once every six years
- Non-discrimination safeguards to protect the rights of researchers, students, and research support staff

The means for certification has not yet been identified. The expectation is that it will be SAM.gov.

Implementation Timetable (COGR)

Assumes minimum windows for agency and institutional implementation - Jan. 2027 is a possible end point



July 9, 2024

OSTP releases Guidelines for Research Security Programs at Covered Institutions to heads of federal agencies.

January 8, 2025

Within 6 months of the date of OSTP Guidelines, federal agencies shall submit to OSTP & OMB plans for updating their policies to address the Guidelines in their research security program standards.

January 2025-July 2025

Federal agencies shall implement their updated policies no later than 6 months after finalized plans are submitted to OSTP & OMB.

January 2025-July 2026

Covered institutions shall have no more than 18 months after the effective date of agency plans to implement their requirements.

NCURA 66TH
ANNUAL MEETING

Rediscover Y-OUR Journey

Federal and University Implementation of NSPM-33 and CHIPS Act Requirements

International collaborations: what has changed?

National security reviews on PIs doing fundamental research (risk matrices and AI tools identifying high risk collaborations—***every collaboration with China***)

Prohibitions coming: talent program affiliations, foreign funding, patents filed outside the U.S., and denied entity affiliations

Mitigation plans (e.g., security training, travel reporting requirements, and in some cases ending collaborations and research activities)

Prohibition on malign foreign talent program participation enforced by institution

Increased disclosure requirements internally and externally on federal granting documents

Omissions in disclosures, failure to comply, and making false statements can result in civil or criminal penalties for researchers and universities

Malign Foreign Talent Recruitment Prohibition

CHIPS Act: Malign FTRPs

- Directs the White House to develop guidelines for research funding agencies that:
  - Prohibit R&D awards to senior/key personnel participating in *malign* FTRPs
  - Requires recipient institutions to prohibit these individuals from working on projects supported by R&D awards.
- DoD *Countering Unwanted Foreign Influence in DoD funded Research at Institutions of Higher Education*
  - Includes a *Policy on Risk-based Security Reviews of Fundamental Research* and *Decision Matrix*. Per the matrix:
    - **DoD prohibits dept. funding after August 9, 2024, if proposing institution does not have a malign FTRP policy/prohibition in place**

NSF MFTRP Prohibition

Section 10632 of CHIPS and Science Act

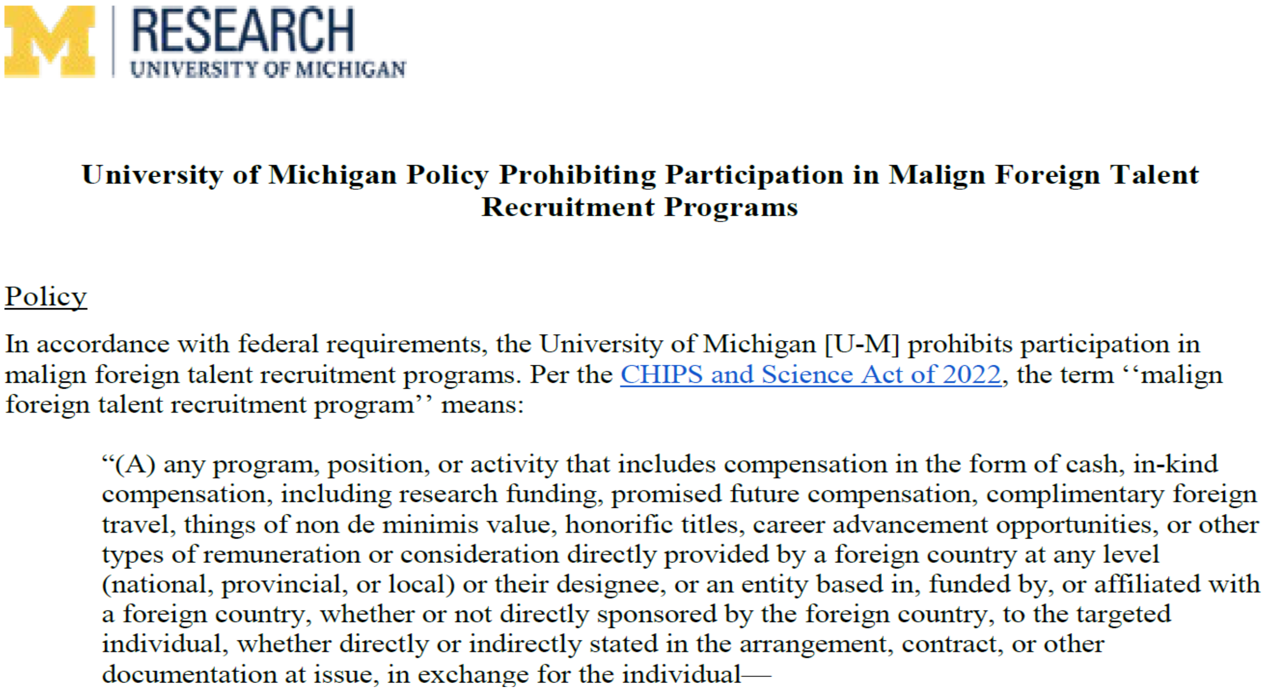
- Chapter II.D.1.d(ix): Certification Regarding MFTRP – organizational certification

  → AOR must certify that all individuals identified as senior/key personnel have been made aware of and have complied with their responsibility under that section to certify – not a party to a MFTRP
- Chapter II.D.1.e(ii): Individuals designated as senior/key persons on a proposal

  → Individuals who are a current party to a MFTRP are not eligible to serve as a senior/key person on an NSF proposal or on any NSF award made after May 20, 2024 (certify prior to proposal submission)

  → SciENcv attestation

U-M Policy Prohibiting MFTRP Participation – Jan 2024



RESEARCH
UNIVERSITY OF MICHIGAN

University of Michigan Policy Prohibiting Participation in Malign Foreign Talent Recruitment Programs

Policy

In accordance with federal requirements, the University of Michigan [U-M] prohibits participation in malign foreign talent recruitment programs. Per the CHIPS and Science Act of 2022, the term ‘‘malign foreign talent recruitment program’’ means:

> “(A) any program, position, or activity that includes compensation in the form of cash, in-kind compensation, including research funding, promised future compensation, complimentary foreign travel, things of non de minimis value, honorific titles, career advancement opportunities, or other types of remuneration or consideration directly provided by a foreign country at any level (national, provincial, or local) or their designee, or an entity based in, funded by, or affiliated with a foreign country, whether or not directly sponsored by the foreign country, to the targeted individual, whether directly or indirectly stated in the arrangement, contract, or other documentation at issue, in exchange for the individual—

https://research.umich.edu/wp-content/uploads/2024/01/U-M-Policy-on-Malign-FTRPs.pdf

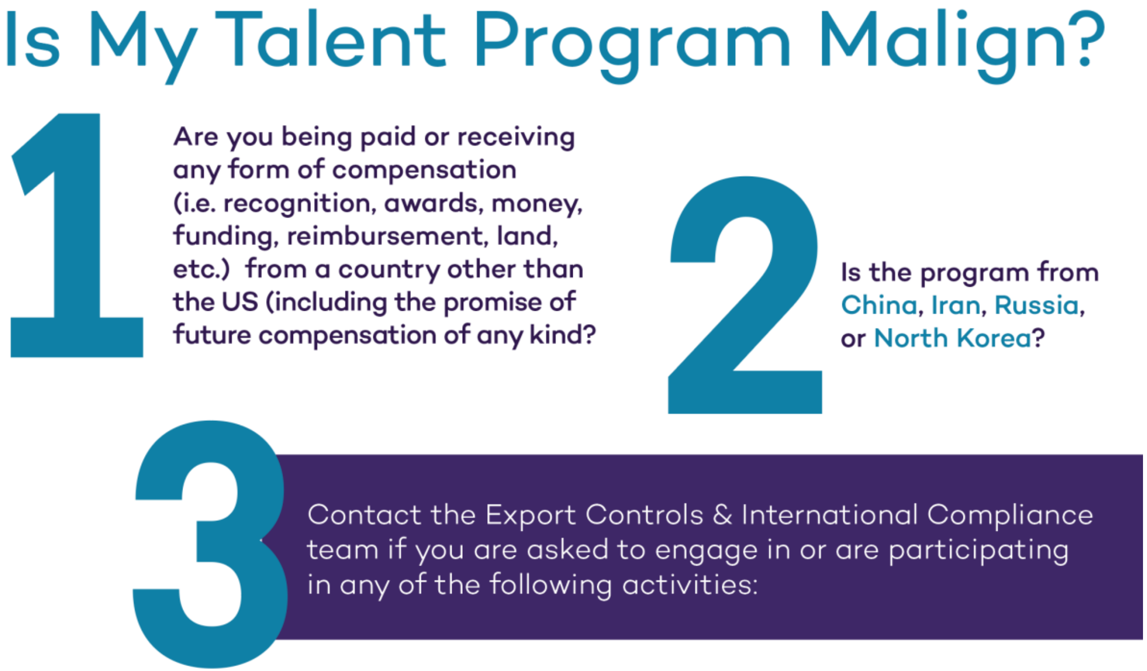
Northwestern
University

Responsible University Official: Provost
Responsible Office: Northwestern Conflict of Interest Office (NUCOI)
Origination Date: August 24, 2012
Next Review Date: August 24, 2026

Policy on Conflict of Interest in Research

Policy Statement

As noted in Northwestern's *Policy on Conflict of Interest and Conflict of Commitment*, the University encourages its faculty, staff, and students to participate in research activities and to do so with the highest ethical standards. While the potential for conflicts of interest to arise in research is understandable due to the innovative and entrepreneurial pursuits of our research community, we must identify and manage situations in which financial or other personal interests could bias or compromise – or have the appearance of biasing or compromising – objectivity or judgment relative to research. Faculty and Staff who are involved in outside consulting or business activities must clearly separate their Northwestern and

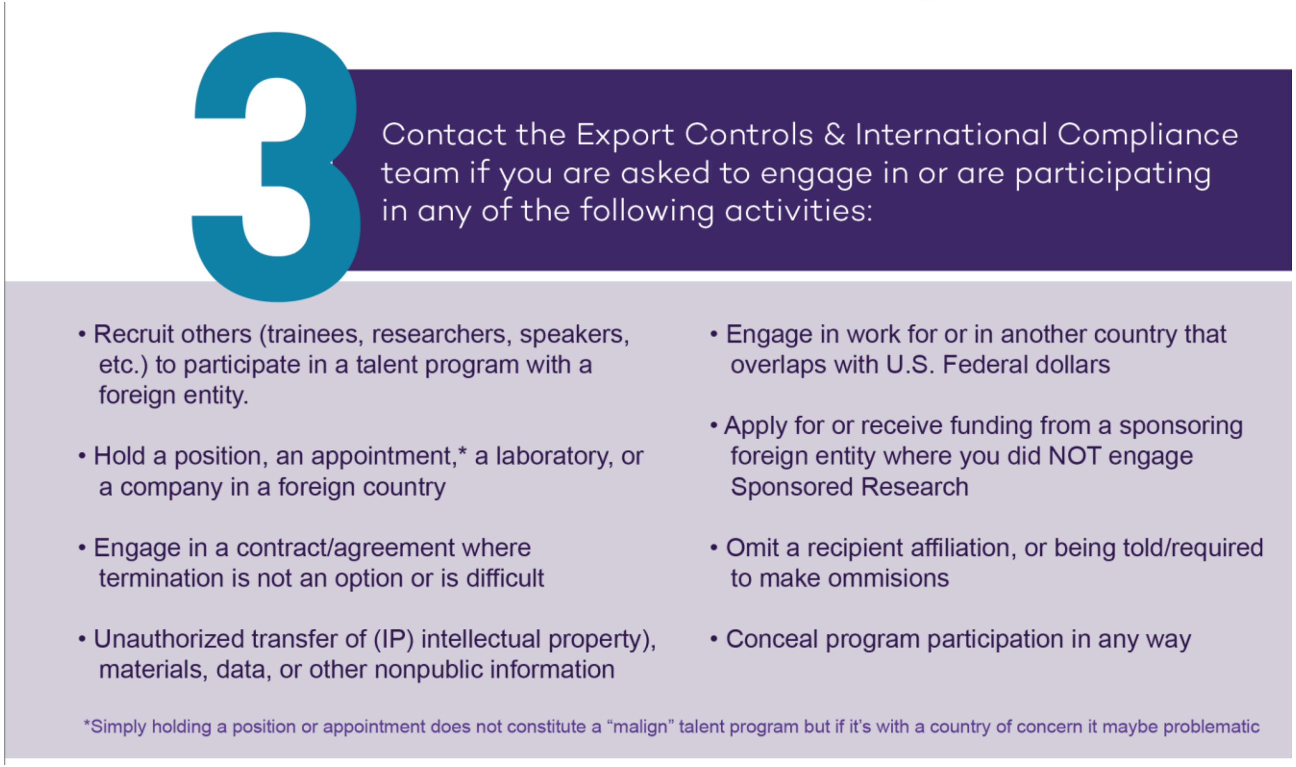


Is My Talent Program Malign?

1 Are you being paid or receiving any form of compensation (i.e. recognition, awards, money, funding, reimbursement, land, etc.) from a country other than the US (including the promise of future compensation of any kind?

2 Is the program from China, Iran, Russia, or North Korea?

3 Contact the Export Controls & International Compliance team if you are asked to engage in or are participating in any of the following activities:



3

Contact the Export Controls & International Compliance team if you are asked to engage in or are participating in any of the following activities:

- Recruit others (trainees, researchers, speakers, etc.) to participate in a talent program with a foreign entity.
- Hold a position, an appointment,* a laboratory, or a company in a foreign country
- Engage in a contract/agreement where termination is not an option or is difficult
- Unauthorized transfer of (IP) intellectual property), materials, data, or other nonpublic information
- Engage in work for or in another country that overlaps with U.S. Federal dollars
- Apply for or receive funding from a sponsoring foreign entity where you did NOT engage Sponsored Research
- Omit a recipient affiliation, or being told/required to make ommisions
- Conceal program participation in any way

*Simply holding a position or appointment does not constitute a “malign” talent program but if it’s with a country of concern it maybe problematic

Disclosure

Disclosure Requirements

Relationships

- Appointments
- Affiliations
- Collaborators
- Leading or performing research elsewhere
- Talent program participation

Funding

- All sources of funding available to your program
- Funding for similar work from other sources – both foreign and domestic

Resources

- Other research space
- Funded visitors
- Materials / equipment – even if provided “in-kind”

Activities

- Research outside of primary institution
- Investments* (e.g., startups)
- Some travel
- Consulting / paid speaking*

Disclosure Forms and Malign FTRP Certification

New common disclosure forms intended for federal-wide use.

- Current and Pending (Other) Support
- Biographical Sketch

The forms include the following certification to be completed and signed by each senior/key person:

- I certify that the **information provided is current, accurate, and complete**.
- C&P support: This includes, but is not limited to, information related to current, pending, and other support.
- Biosketch: This includes but is not limited to, information related to domestic and foreign appointments and positions.
- I also certify that at the time of submission, I am **not a party in a malign FTRP**.

Common Disclosure Forms

Goal: Agencies should require disclosure of information related to COI and commitment—the forms and processes should be *standardized across all federal agencies* (NSPM-33, 2021).

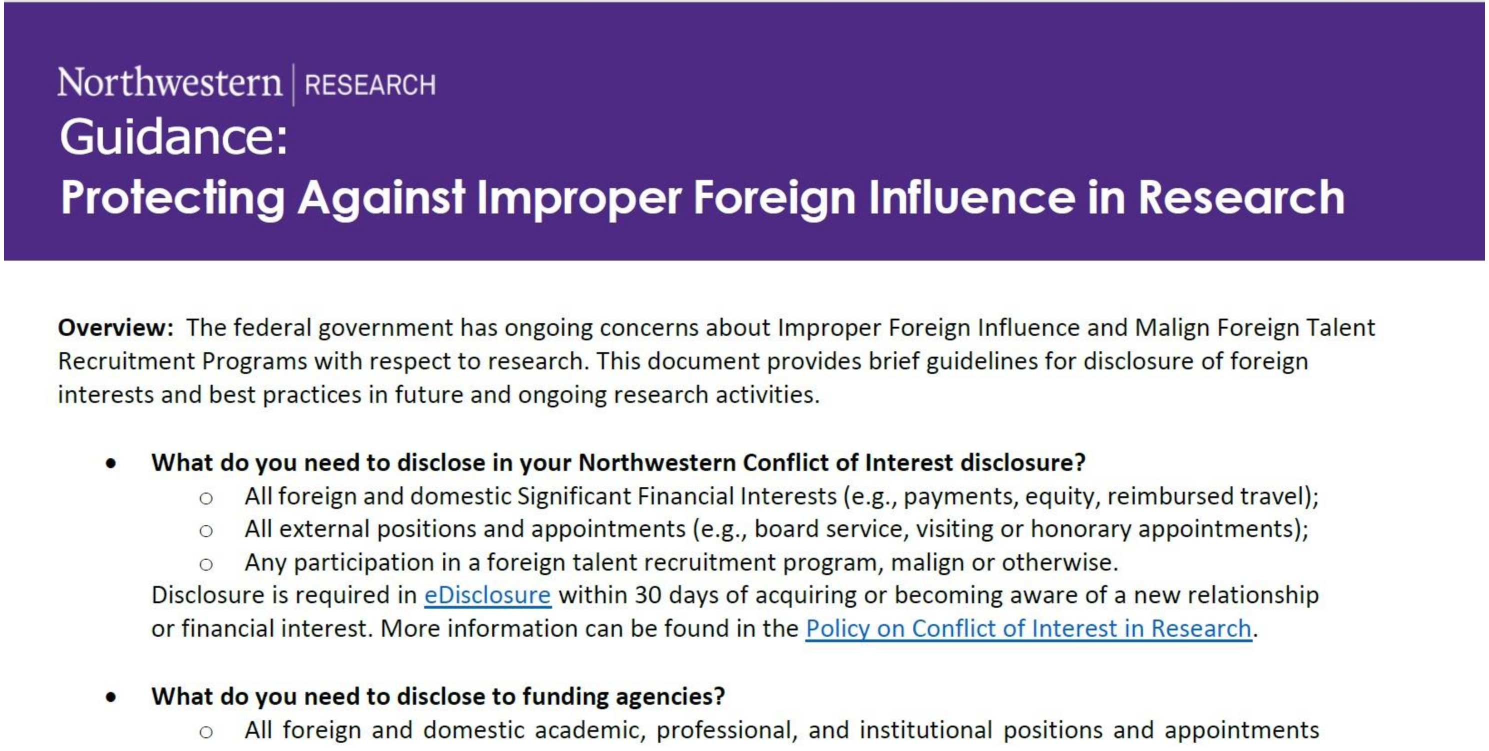
(Biosketch, Current and Pending), November 1, 2023

- Common Form for Biographical Sketch
- Common Form for Current ad Pending (Other) Support Information
- NSTC Pre-award and post-award disclosures table (Jan 2024)

COI offices should share information with pre-award offices to ensure accurate disclosures to federal agencies – “break down information silos”

U-M Policy and Process - Disclosure

- Annual disclosure of outside activities and changes within 30 days
  - Existing explicit question on FTRP participation
  - Explicit attestation of non-participation in MFTRPs in our electronic disclosure system in addition to federal proposal certifications.
  - Reported outside activities in FCOCs flagged for outreach, FTRPs escalated.
  - Review/reconcile federal C&P/Other support with internal disclosures if international activities are indicated.
    - Updated forms submitted if previously undisclosed support is identified.



Northwestern | RESEARCH

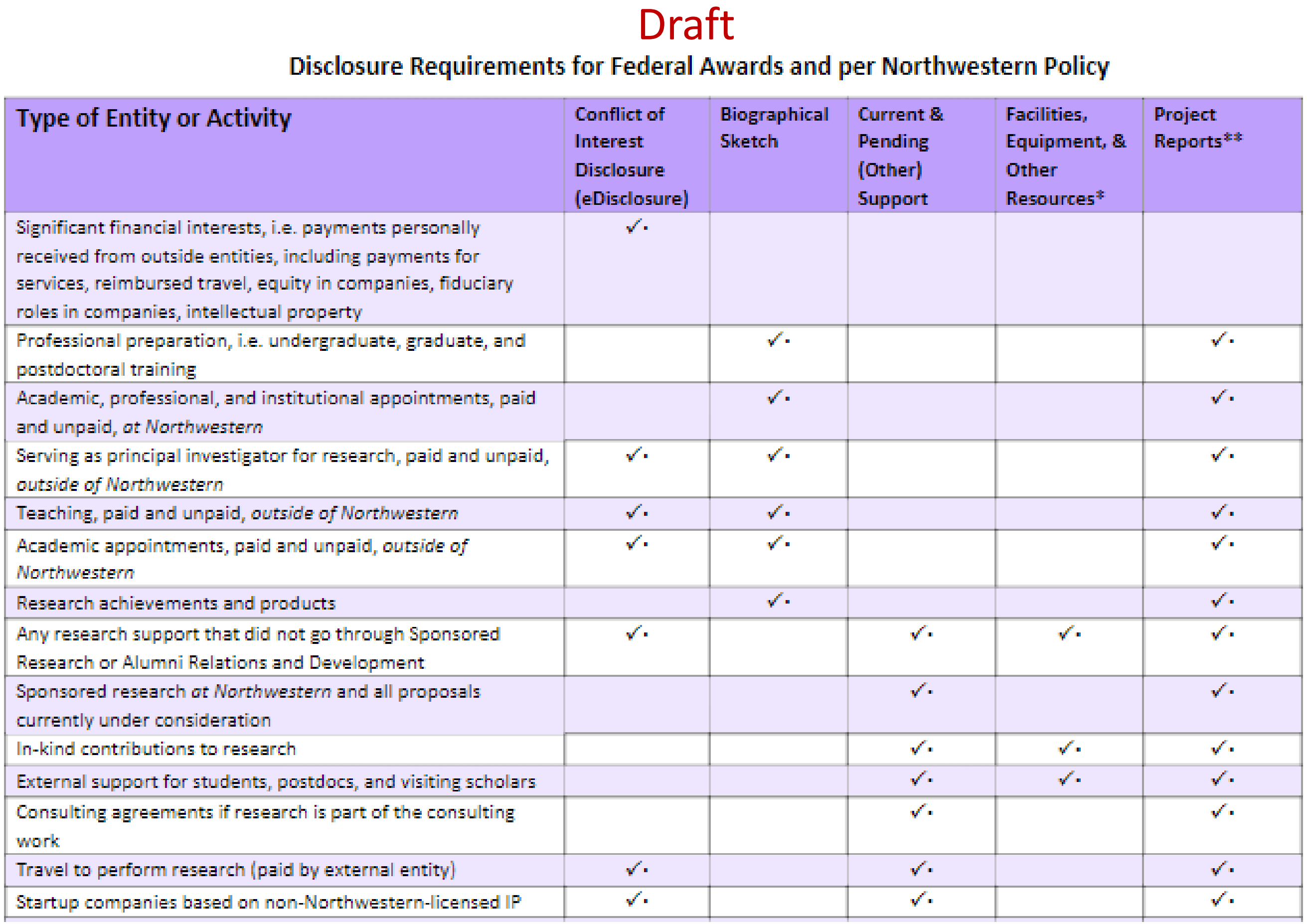
Guidance:
Protecting Against Improper Foreign Influence in Research

Overview: The federal government has ongoing concerns about Improper Foreign Influence and Malign Foreign Talent Recruitment Programs with respect to research. This document provides brief guidelines for disclosure of foreign interests and best practices in future and ongoing research activities.

- **What do you need to disclose in your Northwestern Conflict of Interest disclosure?**
  - All foreign and domestic Significant Financial Interests (e.g., payments, equity, reimbursed travel);
  - All external positions and appointments (e.g., board service, visiting or honorary appointments);
  - Any participation in a foreign talent recruitment program, malign or otherwise.

  Disclosure is required in eDisclosure within 30 days of acquiring or becoming aware of a new relationship or financial interest. More information can be found in the Policy on Conflict of Interest in Research.

- **What do you need to disclose to funding agencies?**
  - All foreign and domestic academic, professional, and institutional positions and appointments



Draft

Disclosure Requirements for Federal Awards and per Northwestern Policy

Type of Entity or Activity	Conflict of Interest Disclosure (eDisclosure)	Biographical Sketch	Current & Pending (Other) Support	Facilities, Equipment, & Other Resources*	Project Reports**
Significant financial interests, i.e. payments personally received from outside entities, including payments for services, reimbursed travel, equity in companies, fiduciary roles in companies, intellectual property	✓				
Professional preparation, i.e. undergraduate, graduate, and postdoctoral training		✓			✓
Academic, professional, and institutional appointments, paid and unpaid, *at Northwestern*		✓			✓
Serving as principal investigator for research, paid and unpaid, *outside of Northwestern*	✓	✓			✓
Teaching, paid and unpaid, *outside of Northwestern*	✓	✓			✓
Academic appointments, paid and unpaid, *outside of Northwestern*	✓	✓			✓
Research achievements and products		✓			✓
Any research support that did not go through Sponsored Research or Alumni Relations and Development	✓		✓	✓	✓
Sponsored research *at Northwestern* and all proposals currently under consideration			✓		✓
In-kind contributions to research			✓	✓	✓
External support for students, postdocs, and visiting scholars			✓	✓	✓
Consulting agreements if research is part of the consulting work			✓		✓
Travel to perform research (paid by external entity)	✓		✓		✓
Startup companies based on non-Northwestern-licensed IP	✓		✓		✓

Agency Risk Reviews and Mitigation

Agency Risk-based Security Reviews: DoD

Policy on Risk-based Security Reviews of Fundamental Research

- Assists DoD program managers in reviewing fundamental research proposals selected for award using disclosed info.

Decision Matrix to Inform Fundamental Research Proposal Mitigation

1. Participation in FTRPs - in particular “malign”
2. Funding sources - current or prior funding from FCOC/entities
3. Patents (e.g., first filed in an FCOC or on behalf of an FCOC-connected entity, or in a non-FCOC country without disclosure)
4. Associations and affiliations on U.S. Entity and other lists.

List of foreign institutions engaging in problematic activity (use caution when engaging)

List of FTRPs posing a threat to U.S. national security interests

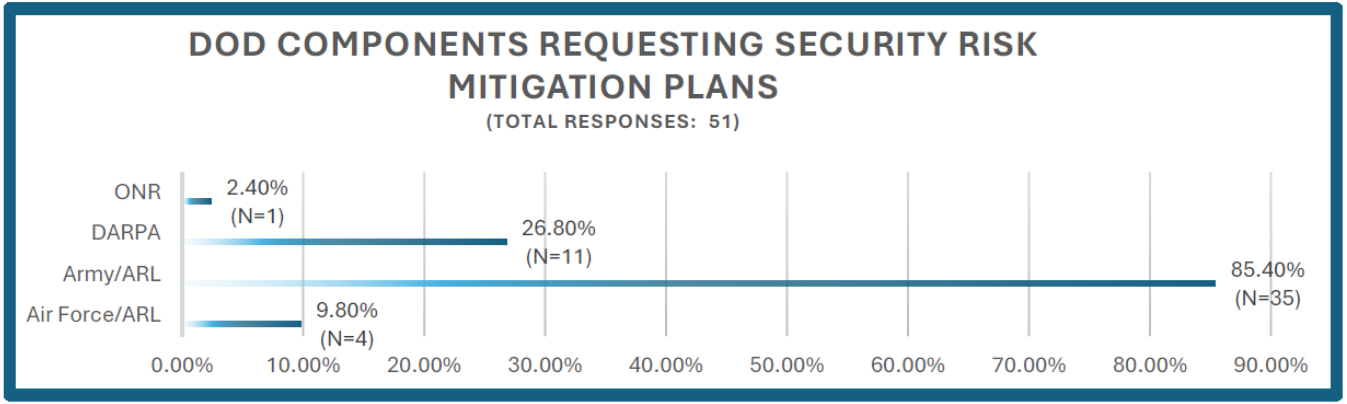
DoD is working to get all components to adopt the June 2023 central process and matrix

Factors for Assessing a Covered Individual's Associations, Affiliations, Collaborations, Funding, and the Policies of the Proposing Institution that Employs the Covered Individual

	Factor 1: Foreign Talent Recruitment Programs	Factor 2: Funding Sources	Factor 3: Patents	Factor 4: Entity Lists
Prohibited factors	**For the Period after 9 Aug 2024** 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. Policy of Proposing Institution employing the covered individual does not prohibit participation in a MFTRP.			
Factors discouraged by DoD policy, mitigation measures required, rejection of proposal required if no mitigation possible	**For the period after 9 Aug 2022[1]:** Indicator(s)[2] of participation[3] 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.	Indicator(s) that the covered individual is currently receiving funding from a Foreign Country of Concern (FCOC) or a FCOC-connected entity.	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.	**For the period after 9 Aug 2022:** Indicator(s) of association with an entity on: the U.S. Bureau of Industry and Security (BIS) Entity List,[4] the Annex of Executive Order (EO) 14032[5] or superseding EOs, Sec. 1260H of the National Defense Authorization Act (NDAA) for FY 2021,[6] or Sec. 1286 of the NDAA for FY 2019, as amended.[7] **For the period after 10 Oct 2019:[8]:** 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.
Mitigation measures recommended	**For the period between 10 Oct 2019[8] and 9 Aug 2022:** 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. **For the period after 9 Aug 2022:**	**For the period between 10 Oct 2019 and 9 Aug 2022:** Indicator(s) that the covered individual received funding from a FCOC or an FCOC-connected entity.	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.	**For the period between 10 Oct 2019 and 9 Aug 2022:** 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. **For the period prior to 10 Oct 2019:**

Agency Risk-based Security Reviews: DoD

COGR's Survey on Research Institutions' Experiences with DoD Policy for Risk-Based Security Reviews (April 2024)**:** ~80% of mitigation plan requests were Army



- ***Common required plan elements:*** Reporting international travel and inquiries from foreign operatives, restrictions on collaborations with entities in FCOCs, RS training
- >65% were able to successfully negotiate risk mitigation plans. One-third rejected.

Agency Risk-based Security Reviews: DOE

- Office of Research, Technology, and Economic Security (COGR Oct. 2023):
  - Conducting "due diligence reviews". A public version of the DOE risk criteria for agency funded research is underway.
  - DOE portfolios often involve critical and emerging tech. Examples of Targets: Advanced Batteries, Computing, Engineering Materials, and Manufacturing; AI/machine learning; Autonomous systems and Robotics; Biotechnologies; Quantum Information Technologies; Next Generation Renewable Energy Generation and Storage; Semiconductors and microelectronics.
  - U.S. Critical and Emerging Technologies List – Feb. 2024

Agency Risk-based Security Reviews

- DOE - Risk concerns can lead to removal of PI or denial of award.
  - Look back on associations, affiliations, possible FTRP involvement up to 10 yrs.
  - Solicitation language (DE-FOA-0003177-000001) - Risk considerations:

    "DOE may conduct a review, through Government resources, of the applicant and project personnel with a connection to a foreign country. This includes, but is not limited to, (1) performance of work in, (2) travel to, and (3) **awardee personnel's higher education in a foreign Country**, as well as (4) partnerships with international collaborators."

- Commerce Bureau of Industry and Security: Implications of additions to Entity List
  - Impact on ongoing collaborations and how to handle subsequent co-authorship
- NSF, DoD, and DOE to conduct quarterly FDP listening sessions on risk reviews

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) Appointments and positions w/ U.S. proscribed parties and are not a 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 - Sec. 1286 of the NDAA for FY2019, as amended

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

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

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

3) Potential foreseeable national security applications of the research

Identifying Federal Research Security Risk Mitigation Measures

NIST defines risk mitigation as “prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process.”

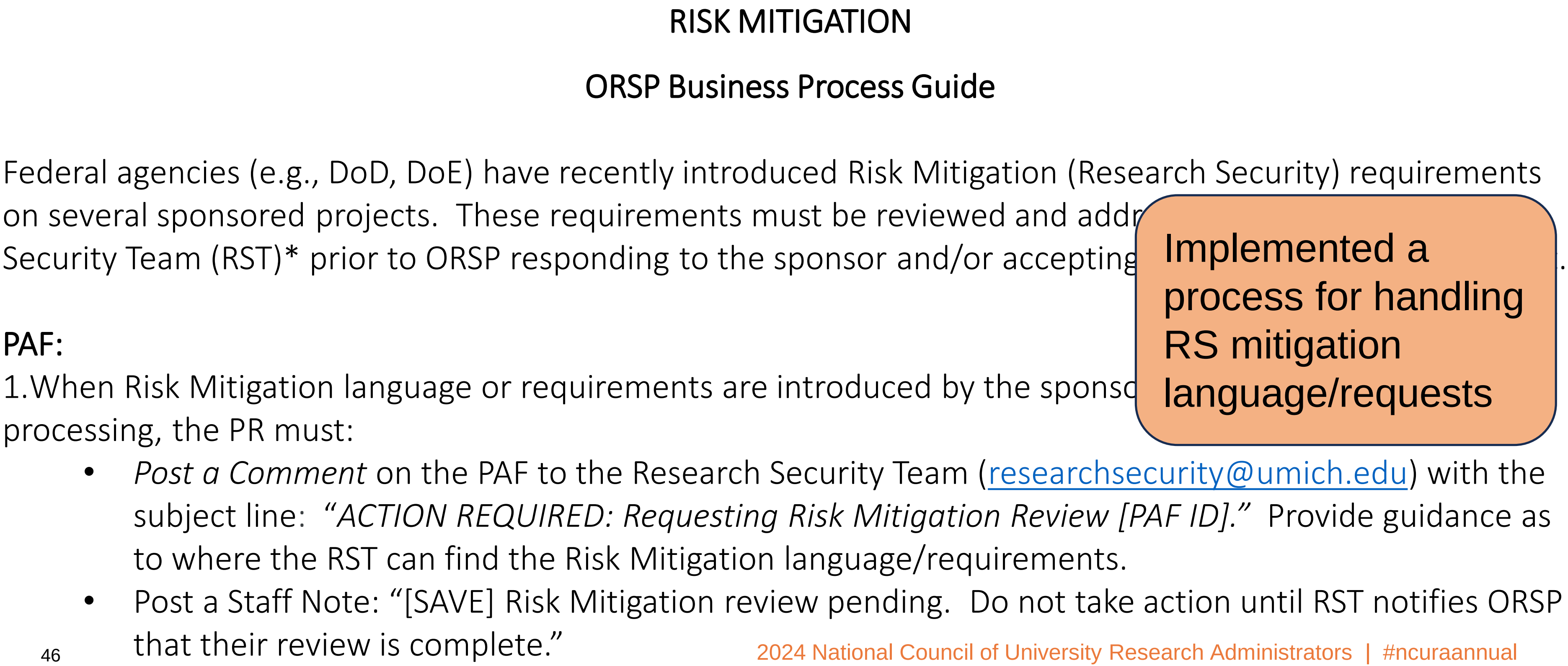
Federal agencies, including the DoD, DOE and soon, NSF, are conducting re
for proposals that have been positively reviewed and recommended for fu
identified, the agency may reach out to the institution to work with the un
POCs to identify appropriate risk mitigation measures. This outreach may i

Developed internal guidance on identifying research security/risk mitigation language

Your proposal was selected for further consideration; a pre-award security review was conducted. The security review identified potential indicators of the below risk factors:

Denied Entities – Indicators of an active affiliation or past affiliation or present association with an entity on the U.S. Government denied entity or person list or EO 13959 or subsequent similar issuances.

Agency Risk Reviews: Process for Sponsored Projects Office



RISK MITIGATION

ORSP Business Process Guide

Federal agencies (e.g., DoD, DoE) have recently introduced Risk Mitigation (Research Security) requirements on several sponsored projects. These requirements must be reviewed and addr
Security Team (RST)* prior to ORSP responding to the sponsor and/or accepting .

PAF:

1.When Risk Mitigation language or requirements are introduced by the sponsc
processing, the PR must:

- *Post a Comment* on the PAF to the Research Security Team (researchsecurity@umich.edu) with the subject line: *"ACTION REQUIRED: Requesting Risk Mitigation Review [PAF ID]."* Provide guidance as to where the RST can find the Risk Mitigation language/requirements.
- Post a Staff Note: "[SAVE] Risk Mitigation review pending. Do not take action until RST notifies ORSP that their review is complete."

Implemented a process for handling RS mitigation language/requests

Agency Risk Reviews: Compliance

- Working with the PI/Co-PIs and applicable offices, addressing risks identified by federal agencies and developing mitigation strategies
- Engagement with agency staff on risk and mitigation
- Implementing and tracking risk mitigation plans on a project basis
- Developing resources to pre-emptively address potential risk concerns in proposals

Research Security Program Implementation: Cybersecurity

RSP Guidelines: Cybersecurity

Implement a cybersecurity program one year after publication of the final NIST cybersecurity resource (IR 8481: Cybersecurity for Research)

- As COGR notes: “the referenced NIST document does not identify a specific cybersecurity framework or set of practices that institutions are required to follow.”

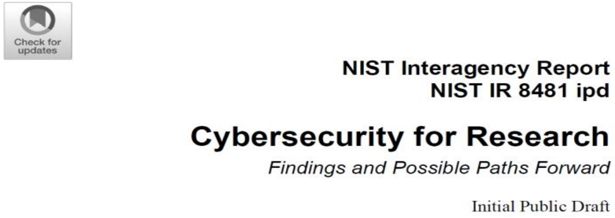
This is a significant departure from the draft RSP requirements: Compliance with 12 of the 15 requirements of FAR 52.204-21 *Basic Safeguarding of Covered Contractor Information Systems*

RSP Guidelines: Cybersecurity

The referenced NIST publication is an initial public draft that summarizes feedback NIST received on IHE cybersecurity challenges and includes possible next steps, including:

- Community-specific cybersecurity resources – research and/or particular fields of study
- Coordinate with other federal agencies on cybersecurity for research contexts
- Support cybersecurity trainings customized for a research context and audience

Encourages the IHE research community to consider how existing cybersecurity resources (many are noted) could be leveraged to support the identification, assessment, management, and reduction of cybersecurity risks related to conducting research.



Check for updates

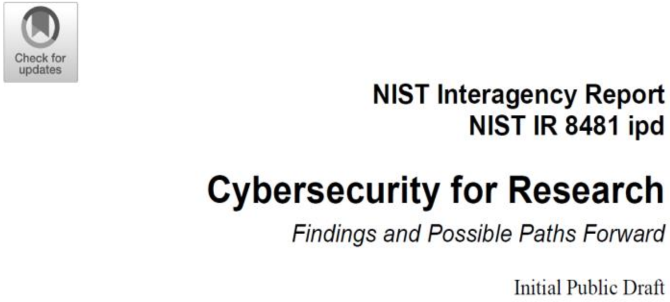
NIST Interagency Report
NIST IR 8481 ipd

Cybersecurity for Research

Findings and Possible Paths Forward

Initial Public Draft

RSP Guidelines: Cybersecurity



Check for updates

NIST Interagency Report
NIST IR 8481 ipd

Cybersecurity for Research

Findings and Possible Paths Forward

Initial Public Draft

Questions/considerations:

- Will the final NIST cybersecurity document consist of/point to the additional resources considered in “next steps”?
- Is the one-year period from final publication for institutions to document cybersecurity programs, including existing policies/processes and use of resources and any additional (newly created) resources adopted?
- Possible approach: Start documenting your institutions existing cybersecurity program

Research Security Program: Foreign Travel Security

RSP Guidelines: Foreign Travel Security

Final RSP Guidelines

- Implement federal foreign travel security training to CIs within 1 year of availability and at least every 6 yrs.
- Organizational record of CI international travel when an agency determines security risks warrant travel reporting for an R&D award

Significant Departure from DRAFT Guidelines below:

- Maintain org record of covered international travel by CIs
- Advanced disclosure and authorization
- Mandatory security briefings and advice regarding electronic device security prior to covered international travel or including electronic devices utilized/bought for federally funded R&D.

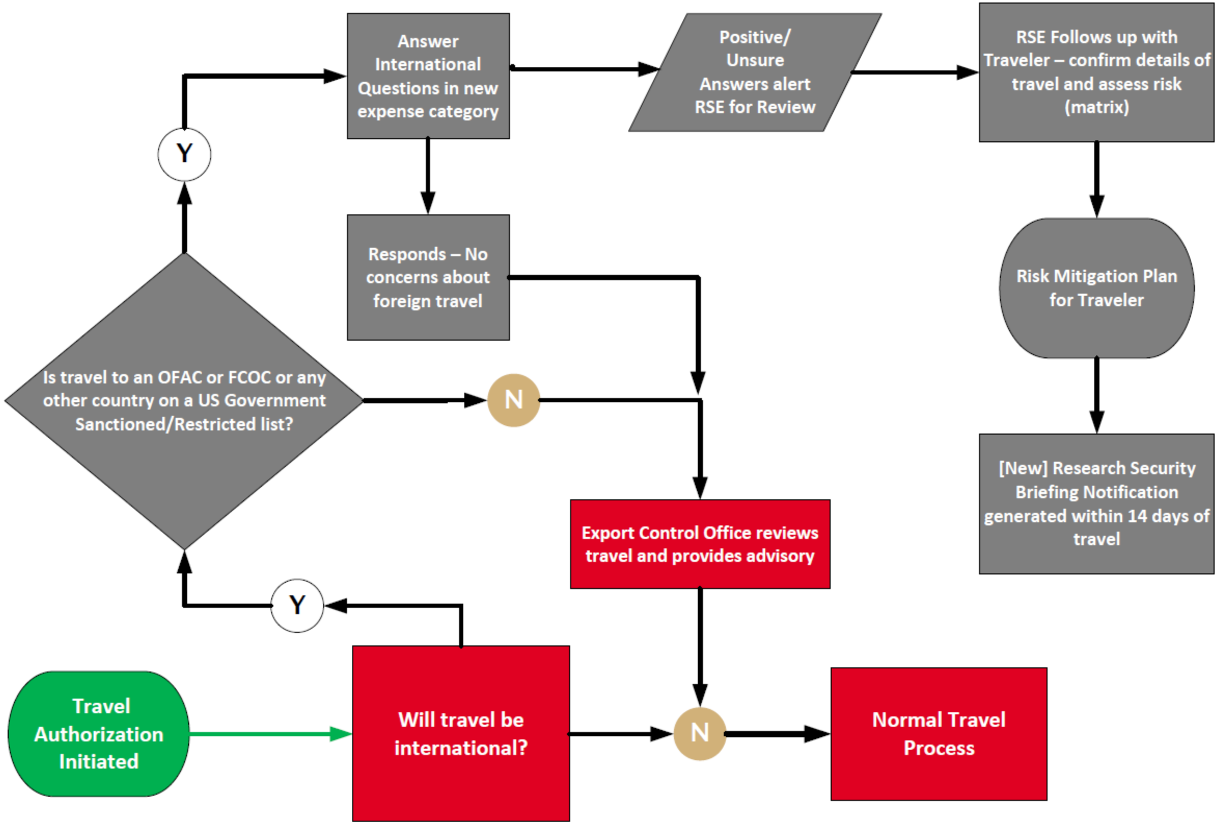
RSP Guidelines: Foreign Travel Security

University/Institution Considerations

- Consider a broad policy for recording international travel by covered individuals for larger research programs?
  - Challenging to track as a risk requirement by project and agency. Institutions could start at the project level and assess volume before moving to a policy for all CIs.

- How to facilitate compliance?
  - Education
  - Tie to travel reimbursement?
  - Reconcile with internal COI reporting on foreign travel?

- Federal expectations for how institutions might use the data hasn't been stated.

Answer International Questions in new expense category
Positive/ Unsure Answers alert RSE for Review
RSE Follows up with Traveler – confirm details of travel and assess risk (matrix)
Y
Responds – No concerns about foreign travel
Risk Mitigation Plan for Traveler
Is travel to an OFAC or FCOC or any other country on a US Government Sanctioned/Restricted list?
N
[New] Research Security Briefing Notification generated within 14 days of travel
Export Control Office reviews travel and provides advisory
Y
Travel Authorization Initiated
Will travel be international?
N
Normal Travel Process

International Questionnaire (Additional Expense Category – Concur)

Will expenses be paid for by a 3rd party? (No/Self Pay/Unsure/Yes):

- Indicate how your trip will be paid for if known. If the trip is being paid for by a 3rd party other than a UC grant/contract, select YES. If it is being paid for by UC or through UC administered grant/contract, NO. If you are unsure how the trip is being paid for, select UNSURE. If you are paying for the and not seeking reimbursement from any entity, select SELF PAY.

Will you export equipment, items, or specimens? (Yes/No):

- Indicate if you will be taking any items that would be considered Export Controlled on your trip. If you are unsure, contact the Export Control Office at exportco@ucmail.uc.edu.

Will you access UC's network while abroad? (Yes/No):

- Indicate if you plan access University of Cincinnati network in anyway (via local connection or VPN). If you do plan to do so, please reach out to Research Cybersecurity at research_security@ucmail.uc.edu.

Indicate what technology is traveling with you. (Laptop, Phone, USB/External Drive, Other)

- If other, list in the box below:
- Indicate if you are taking any University of Cincinnati technology with you. If you are taking multiple devices, please indicate which devices you are taking in the section below.

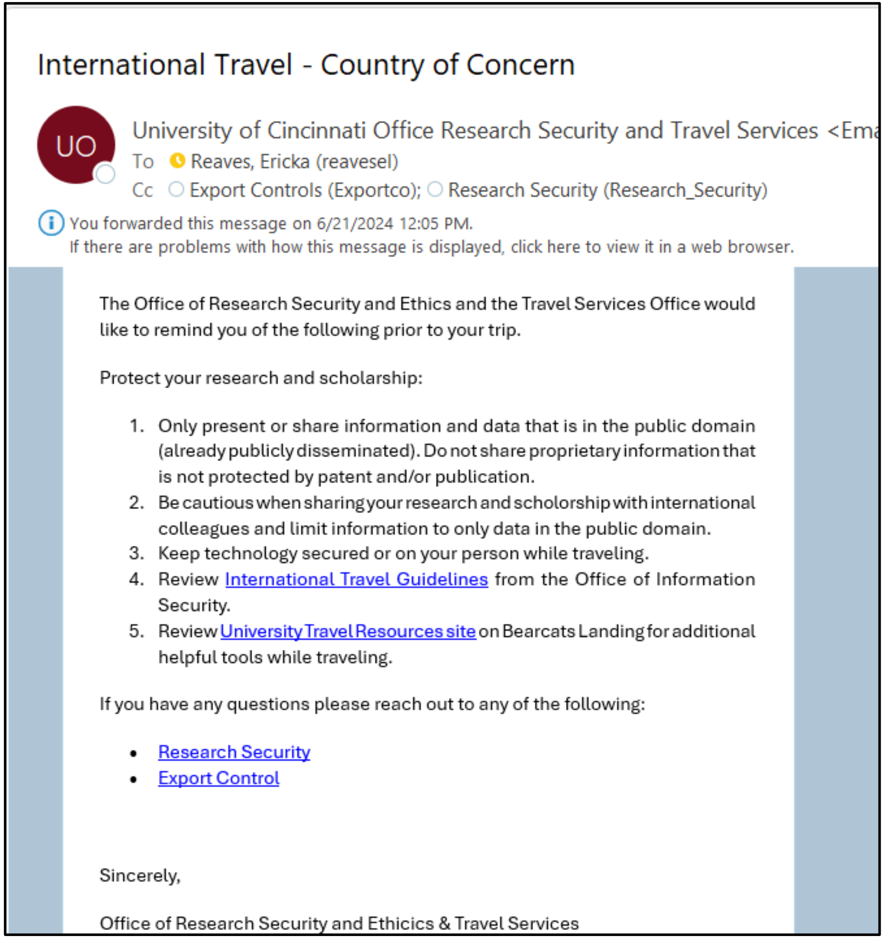
Is all information to be shared public? (Yes/No):

- Indicate if the information you will be discuss, present, display any information related to research completed, sponsored by, conducted, or administered at or by University of Cincinnati is already in the public domain. If not, please consult with the Export Control office at Exportco@ucmail.uc.edu.

Please select the purpose of travel. (Attending a Conference, Teaching, Speaking, Research, Training/Mentoring, Observing Innovative Practice, Other):

- If other, list in the box below
- Indicate the purpose of travel. If there are multiple travel purposes, please indicate in the comment box below.

14 - Day Travel Reminder



International Travel - Country of Concern

University of Cincinnati Office Research Security and Travel Services <Ema

To Reaves, Ericka (reavesel)

Cc Export Controls (Exportco); Research Security (Research_Security)

You forwarded this message on 6/21/2024 12:05 PM.
If there are problems with how this message is displayed, click here to view it in a web browser.

The Office of Research Security and Ethics and the Travel Services Office would like to remind you of the following prior to your trip.

Protect your research and scholarship:

1. Only present or share information and data that is in the public domain (already publicly disseminated). Do not share proprietary information that is not protected by patent and/or publication.
2. Be cautious when sharing your research and scholorship with international colleagues and limit information to only data in the public domain.
3. Keep technology secured or on your person while traveling.
4. Review International Travel Guidelines from the Office of Information Security.
5. Review University Travel Resources site on Bearcats Landing for additional helpful tools while traveling.

If you have any questions please reach out to any of the following:

- Research Security
- Export Control

Sincerely,

Office of Research Security and Ethics & Travel Services

Research Security Program: Training

RSP Guidelines: Training

Research Security

- Option A: NSF training modules
- Option B: Non-federal training that covers
  1. Improper transfer of USG-supported R&D
  2. Importance of International research & talent

Export Controls

Provide EC training to CI working with controlled technology

- Option A: Govt. training (BIS, DDTC)
- Option B: Non-fed training with U.S. EC and compliance requirements & processes for reviewing foreign sponsors, collaborators, and partnerships

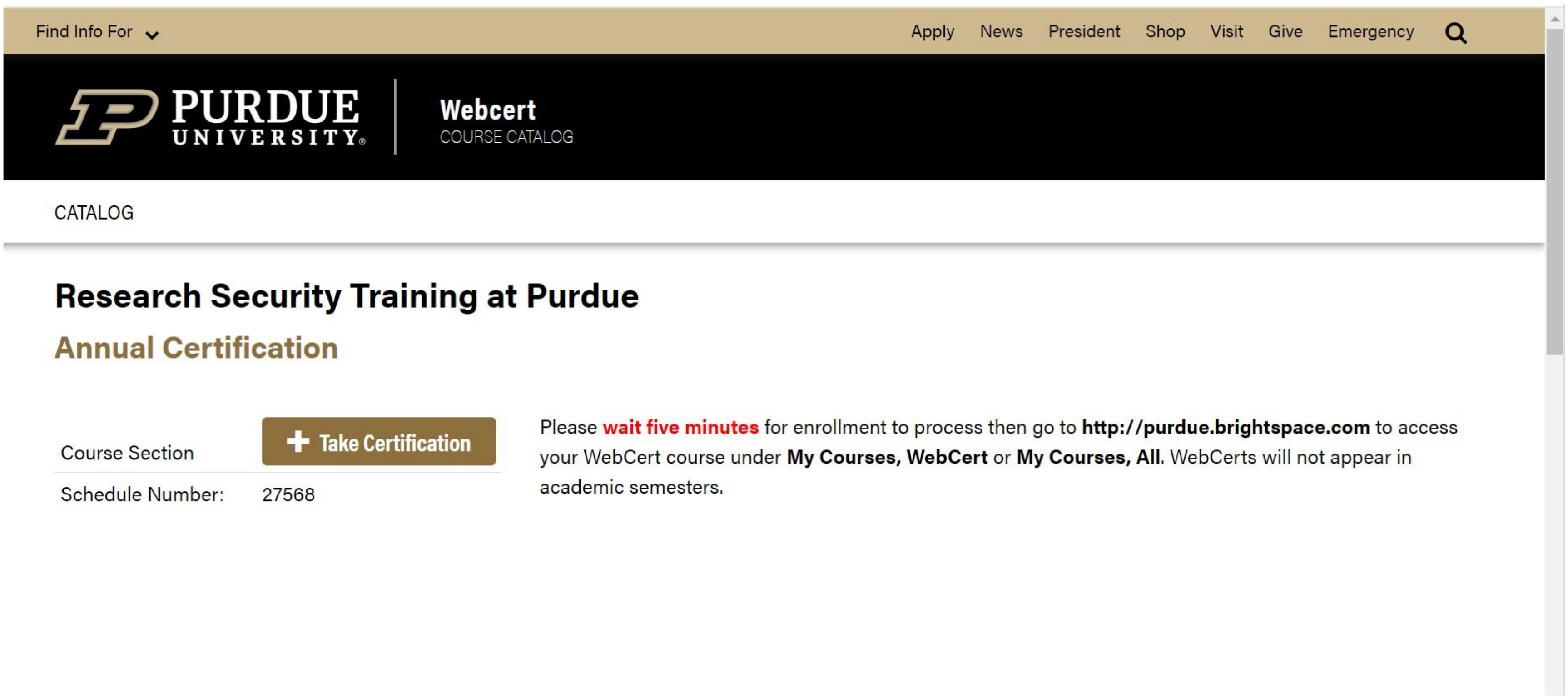
Coverage of restricted party screening. Other information on “processes for reviewing foreign sponsors, collaborators, and partnerships would be covered in research security training and documented.

Federal RS Training Modules

Four modules covering:

- Intro. to Research Security
- Importance of Disclosure
- Risk Management & Mitigation
- Importance of International Collaboration

- Content can be downloaded and integrated with an institution's learning management system and individual training tracked
- Modules can also be taken on the NSF website
- Use of modules is not required. Institutions can use part or all.
- NSF to require training on implementation of the 2025 PAPPG; other agencies will follow



Research Security Training at Purdue

Annual Certification

Course Section	+ Take Certification
Schedule Number:	27568

Please **wait five minutes** for enrollment to process then go to **http://purdue.brightspace.com** to access your WebCert course under **My Courses, WebCert** or **My Courses, All**. WebCerts will not appear in academic semesters.

NSF/CHIPS Foreign Gift and Contract Reporting

NSF - Foreign Gifts and Contracts

Section 10339B, *Foreign Financial Support* of the CHIPS and Science Act

→ Each “**recipient institution of higher education**” must annually 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”.

→ Does not include entities that receive subawards or individuals that are the beneficiaries of the award.

→ Foreign source financial support comprised of gifts to or contracts with an intermediary that benefit an institution is reportable (e.g., foundation of the institution and related entities – education, cultural or language entity).

NSF 2024 PAPPG: Research Security

Effective date: May 20, 2024

Key RS Priorities

1. Common Disclosure Forms
2. MFTRP prohibition certification
3. Foreign Gifts and Contracts (July 31, 2024 deadline; extended 9/3/2024)
4. Research Security Training (effective 2025 PAPPG)

Risk Mitigation:
University Risk Reviews

Risk Reviews/Assessments

What is being assessed? Some institutions are:

- Reviewing all existing foreign agreements (or FCOC)
- Reviewing proposals to non-U.S. sponsors
- Reviewing non-monetary agreements with international partners
- Reviewing faculty outside activities
- Engaging in data analytics

Institutional Risk Assessments

What factors might be considered when assessing international funding proposals, non-monetary agreements and outside activities?

- Country: Comprehensive sanctions? Foreign Country of Concern (FCOC)
- Funding sources: FCOC or entity associated with FCOC or military
- Presence on U.S. lists of restricted parties
- U.S. Critical or Emerging Technology
- Indicators of a malign FTRP
- U.S. federal agencies funding the researcher (e.g., DOD and DOE)
- Research stage (basic or applied)
- Risk to researcher or institution
- Publication or data restrictions
- Presence or absence or a termination clause
- Conflict of interest or commitment

Matrix to Conduct Risk-based Reviews of International Research Proposals, Unfunded Agreements, Outside Activities, or Gifts Last updated Feb. 2024

Country	Source of Foreign Funding	Presence on Entity and Related Lists/ Potential for Negative Military, Human Rights or Economic Impact	Indicators of a malign FTRP (criteria in section 10638(4)(A)(iix) of the CHIPS Act)	Involves Critical or Emerging Technologies	U.S. Federal Agencies Funding the PI	Research Stage	Potential for Risk to the Individual or Institution, Including Reputational	Publication or Data Restrictions	Termination Clause
Comprehensive Sanctions[1] (*H)	COC foreign government (H)	Restricted Party/Consolidated Screening[4] (H)	Indicators[9] present (H)	Present on list or similar tech (M)	DoD, DoE, NASA, DHS[10] (M)	Applied (M)	Yes (H)	Yes (M)	Yes
Country of Concern (COC) per CHIPS Act (China, Russia, N. Korea, Iran)[2] (*M)	COC Foreign entity closely affiliated with foreign government/ military (M)	Annex of EO14032 (**DOD FY 21 NDAA 1260H and NS-CMIC List)[5] (M)	No indicators of a malign FTRP	STEM field (L)	Other federal agencies (L)	Basic	No	No	No (M)
Country of Particular Concern per State Dept.[3] (*L)	COC Foreign entity not affiliated with foreign government/ military (L)	List of Institutions (Part 3) (FY 19 NDAA 1286 (c)(8)(A)[6] (M)						NA (e.g., data or material transfer/use agreement)	NA (e.g., data or material transfer/use agreement)
		List of FTRPs (Part 3) (FY19 NDAA 1286 (c)(9)(A)[7] (M)							
		ASPI Tracker[8] (L)							
Level:									
Notes:									

*H - Higher Concern; M – Moderate Concern; L – Lower Concern **Non-Specially Designated Nationals Chinese Military-Industrial Complex Companies List

Note: Multiple factors of moderate to higher concern suggest the need for senior-level decision making

FEDERAL DEMONSTRATION PARTNERSHIP

Redefining the Government & University Research Partnership

Demonstration of International Collaborations and Agreements Assessment Tools

March 20, 2024

- Greg Moffat, Chief Research Compliance Officer, MIT
- Lisa Nichols – Executive Director, Research Security, University of Michigan, Co-Chair FDP Research Security Subcommittee (RSS)

Moderators

- Doug Backman, Director of Compliance, University of Central Florida, Co-Chair, RSS
- Sarah Stalker-Lehoux, Deputy Chief of Research Security Strategy and Policy, NSF, Co-Chair, RSS

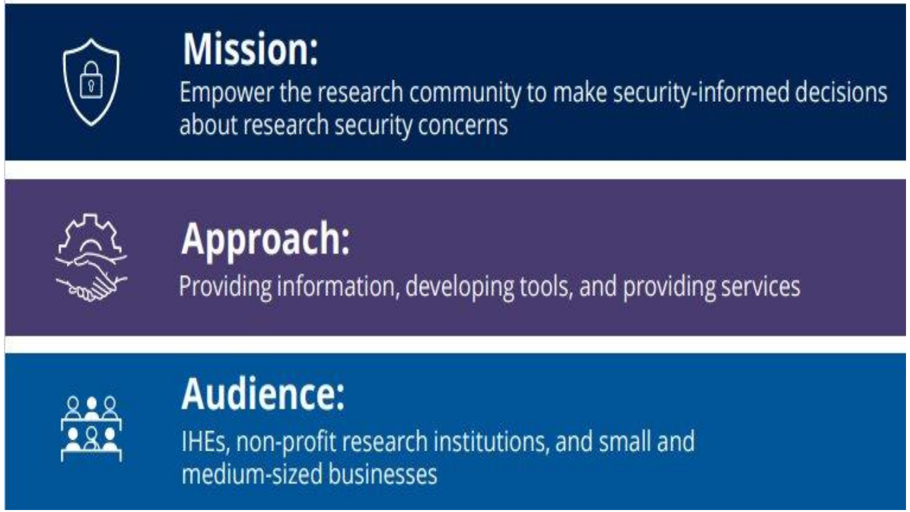
Questions

NCURA 66TH
ANNUAL MEETING

Rediscover Y-OUR Journey

SECURE and University Implementation

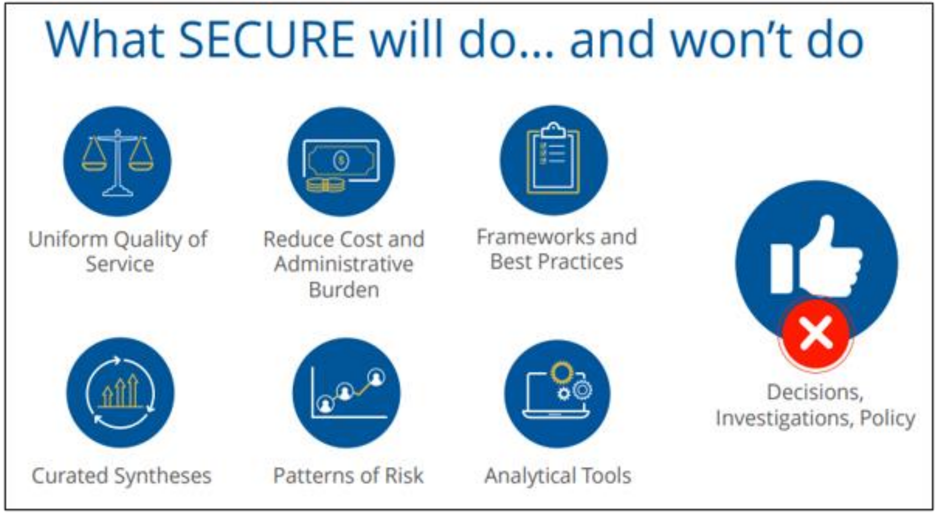
CHIPS Act: SECURE Center



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



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

✗ Decisions, Investigations, Policy

- Proposal/Team selected in May 2024
- Awarded in August-September 2024

NCURA 66TH
ANNUAL MEETING

Rediscover Y-OUR Journey

Stakeholder Engagement, Communication, and Prioritization

Poll Questions

Poll Questions

1. Has your organization started to develop a Research Security Program?
   a. Yes
   b. No
   c. Don't know
2. If Yes, how were you able to identify what areas are a priority for your organization?
   a. Conducted a gap analysis
   b. Benchmarked with other organizations about their strategy/approach
   c. Senior leadership informed next steps
   d. I'm not involved in that decision-making
3. If Yes, what area of research security is a priority (or an area that will require the most effort)?
   a. Cybersecurity
   b. Export Control
   c. Research Security Training
   d. Disclosure practices
   e. Travel registry
   f. Developing policy for security incidents
   g. Malign foreign talent prohibition
   h. Other

Developing priorities

- Establish a team approach to Research Security
    - Informal Working Group with cross campus leaders
    - Formal Committee with broad representations
    - Sub-committees – it takes a village!
- Conduct a gap analysis and set goals
- Educate senior leadership on the state of play
- Conduct regular check-ins to keep things moving forward
    - Identify speed bumps and roadblocks
    - Leverage allies and leadership to move things forward

Policy and Stakeholders

Policy Review

- What policies authorize the gathering and review of information related to research security?
- Which departments/units ("policy owners") oversee those policies?
- Identify the key provisions in the policies that are:
  - Related to research, foreign entities and/or non-US persons
  - Is there a natural "checkpoint" in the review process or does one need to be added

Policy Example: Travel policy

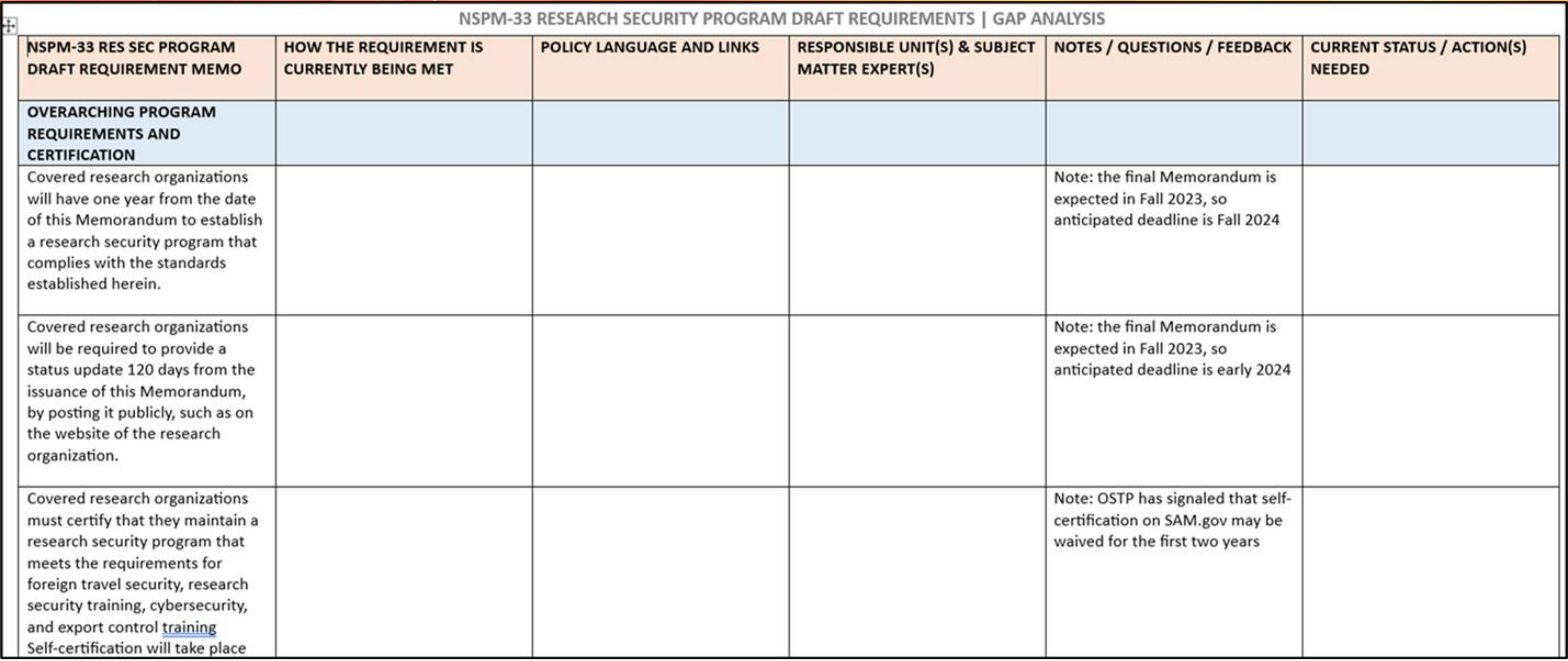
- Administration and Finance
- Faculty and Staff - traveling on university business
- Travel authorization and allowable expenditures for travel
- Includes travel reimbursement
- **Prior Approval** for overnight and **international travel**, same day air travel - must be submitted when traveling on university business
  - Travel request - Concur
  - Approved by supervisor prior to trip commencement

U-M: Requirement to register international travel. Resources on traveling safely and with technology. Consultation if to comprehensively embargoed country.

Stakeholder Example

Stakeholder	Checkpoint
Sponsored programs	Grant application Foreign components Other support/biosketch Often, first contact by NIH
Research contracts	Problematic contract clauses. Foreign entities.
Research IT	Cybersecurity and access management. Geoblocking and loaner devices.
Tech Transfer	IP protection. Disclosure of inventions and foreign patents.
Human Resources	Researcher onboarding, visiting scholars/interns. Visa applications.
Travel	Travel registry and authorizations.
Global Office	International students, visiting scholars, hiring of Foreign Nationals.
Export controls	Restricted party screening. identification of controlled items, persons, and/or entity.
Conflict of Interest	Collection/disclosure of foreign relationships.
Shipping/Receiving	Shipping and receiving of international samples.
Gifts/Foundation	Acceptance of gifts from foreign donors to support research.
Biosafety	Overlap between export controlled/CUI and materials/specimens that are also regulated.

Gap Analysis



NSPM-33 RESEARCH SECURITY PROGRAM DRAFT REQUIREMENTS | GAP ANALYSIS

NSPM-33 RES SEC PROGRAM DRAFT REQUIREMENT MEMO	HOW THE REQUIREMENT IS CURRENTLY BEING MET	POLICY LANGUAGE AND LINKS	RESPONSIBLE UNIT(S) & SUBJECT MATTER EXPERT(S)	NOTES / QUESTIONS / FEEDBACK	CURRENT STATUS / ACTION(S) NEEDED
OVERARCHING PROGRAM REQUIREMENTS AND CERTIFICATION					
Covered research organizations will have one year from the date of this Memorandum to establish a research security program that complies with the standards established herein.				Note: the final Memorandum is expected in Fall 2023, so anticipated deadline is Fall 2024	
Covered research organizations will be required to provide a status update 120 days from the issuance of this Memorandum, by posting it publicly, such as on the website of the research organization.				Note: the final Memorandum is expected in Fall 2023, so anticipated deadline is early 2024	
Covered research organizations must certify that they maintain a research security program that meets the requirements for foreign travel security, research security training, cybersecurity, and export control training Self-certification will take place				Note: OSTP has signaled that self-certification on SAM.gov may be waived for the first two years	

Preparedness Assessment and Timeline

Requirement	Policy	Education	Risk Level	Timeline	Team
Malign talent prohibition	🟩	🟨	🟧	May 2024	COI/ECIC/OGC/SR
New gift and contract reporting	🟨	🟨	🟨	July 2024	Risk & Compliance/ ????
Disclosures	🟩	🟨	🟧	Now	COI/SR/ECIC
Travel registration	🟧	🟧	🟧	TBD	ECIC/RIT/OGSS
Research security training	🟨	🟧	🟨	RCR June 2023 RS 2025	ECIC/Research Integrity/Others
NSPM-33 cyber requirements	🟧	🟧	🟧	TBD	NUIT/RIT/ECIC
Digital Persistent Identifiers	🟨	🟨	🟨	Est. 2025 for requirement	OR Data Analytics/ECIC
Manual/SOP for research security program ~~published on website~~	🟧	🟧	🟧	Est. 2025	ECIC/Group

Socializing Research Security

Research Security & Ethics

Sponsored Research

Enterprise Risk

Information Security

OGC

Training

UC International

Technology Transfer

Human Resources

Faculty/Researchers

Office
of the Provost

Government
Relations

Leadership - Risks to Investigator and Institution

- Rejection of an R&D award application
- Loss of federal research current and potential/future funding
- Potential loss of intellectual property (IP)
- Reputational damage (personal and organizational)
- Individual criminal, civil, and/or administrative penalties

Leadership – University-wide Committees

Northwestern

- Research Security Senior Leadership Working Group
- Research Security Review Committee
- Several subcommittees

.

University of Michigan

- Coordinating Committee on International Engagement
- ITS/IA-OGC-Research/Information Security WG

Include faculty/researchers to build awareness and collaborate to problem solve

NCURA 66TH
ANNUAL MEETING

Rediscover Y-OUR Journey

Faculty Guidance

Faculty – Communications Strategy

- U.S. academic values are not necessarily the same values elsewhere
- Partnering and Protection Campaign – Goal is to secure future federal research funding
- Be a resource to Faculty
    - How well do you know your collaborator? (JASON Report, 2019)
    - Are you adequately protecting your intellectual property?
    - Do you know what to disclose and where?
    - Predatory conference checklist
    - Domestic/International collaboration checklist

International Collaboration Guidance

“How well do I know my collaborator”?

1. Are the terms of engagement made clear in writing? Is it fundamental research? If not, what are the institution’s policies around creating the engagement?

2. Have all participants been identified and are they all known to the PI and the PI’s institution?

3. Is there any aspect of the engagement that seems unusual, unnecessary or poorly specified?

4. Are all the participants conflicts of interest and commitment documented? Are there any aspects of the engagement that are not to be disclosed to any of the participants? If so, what is the reason?

5. Where does the funding and other resources needed for the activity come from? Is it clear what each party is providing?

Jason Report, 2019

Can I collaborate with China? – Helping researchers navigate unwritten rules

- Review research portfolio. DOE or DoD funding? Suggest no FCOC affiliations, associations, or FTRPs. If the Army, any collaborations with China are considered a risk – proposal may be rejected. No FCOC govt. funding – optimally no FCOC entity funding – risk to be mitigated.
- Critical technologies, potential military or dual-use, closer to applied, of greater concern; However, NSF proposes to consider if China is leading in critical tech area and to allow projects to proceed if they are.
- Conduct restricted party screening. Assess collaborators.
- Avoid proposal rejection due to risk concerns:
  - Acknowledgements section of articles – make it clear who performed what work and who funding sources are attributed to.
  - If collaborating with an entity added to the Entity List, consider noting in proposals that collaboration took place prior to, if collaborations are active or not, and what they entailed (e.g., materials obtained several years ago – no further collaboration, or in-kind fellowship is not funded by the PRC). Army and DOE welcome transparency.

International Collaboration Tips

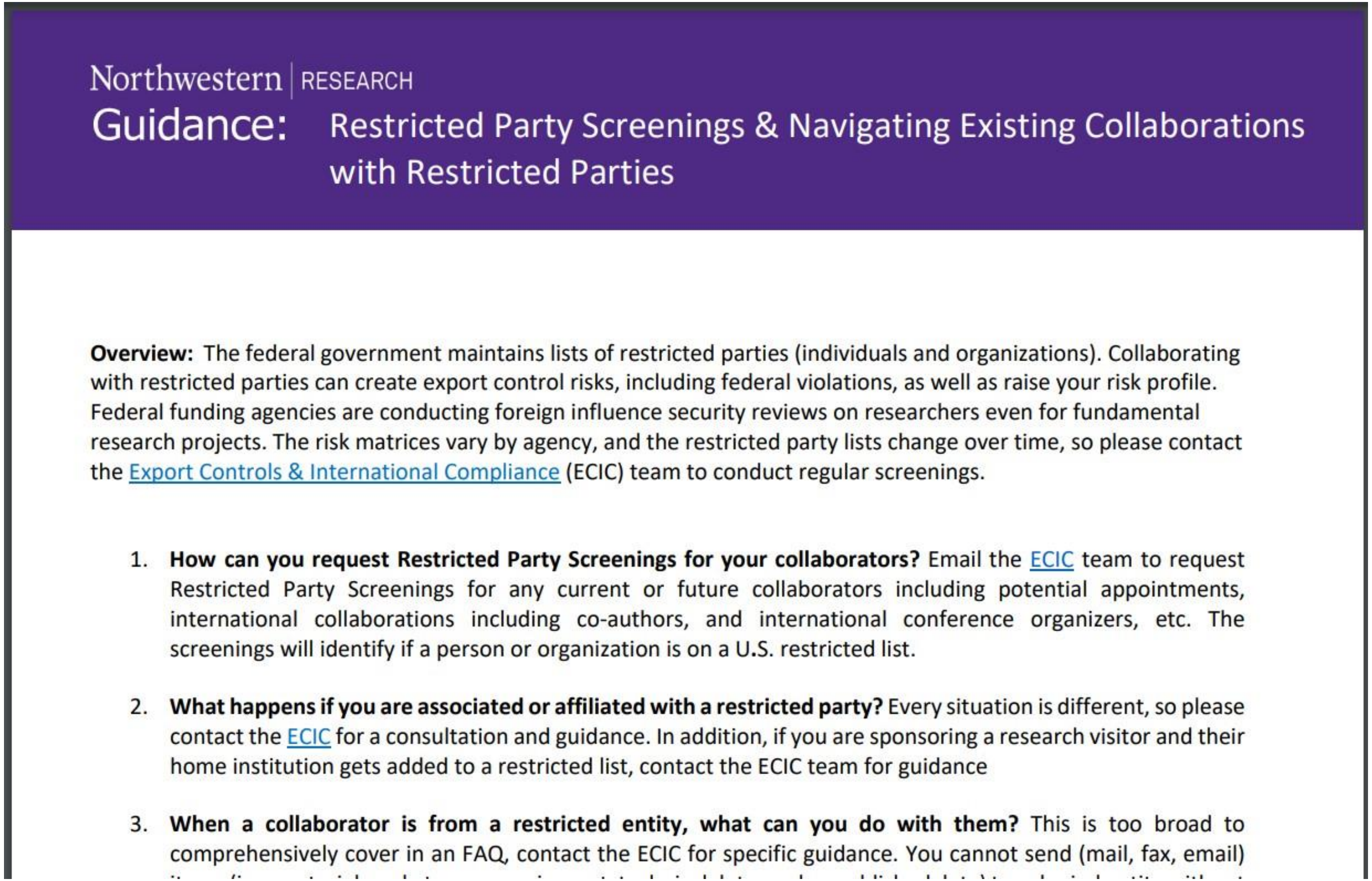
True collaboration: pursue interests that are shared among all investigators; **make sure that everyone involved will benefit.**

Establish a relationship of **trust and openness**. It needs to be a **"two-way street"** so that "they will tell you when things don't go well.

The **sharing of data and biological samples** can be challenging**.** You need to obtain adequate transfer agreements and also be aware that there is a history of foreign scientists misusing data and material.

Make sure you understand the cultural, political, and regulatory context of your partners as well as the **expectations and guidelines** of your funding body at home.

Careful planning is essential. Lay out everyone's **responsibilities and expectations**, define ways to build a supportive network, put in place strategies to meet all the logistical needs of the project, and make sure there is **good scientific and financial monitoring.**



Northwestern | RESEARCH

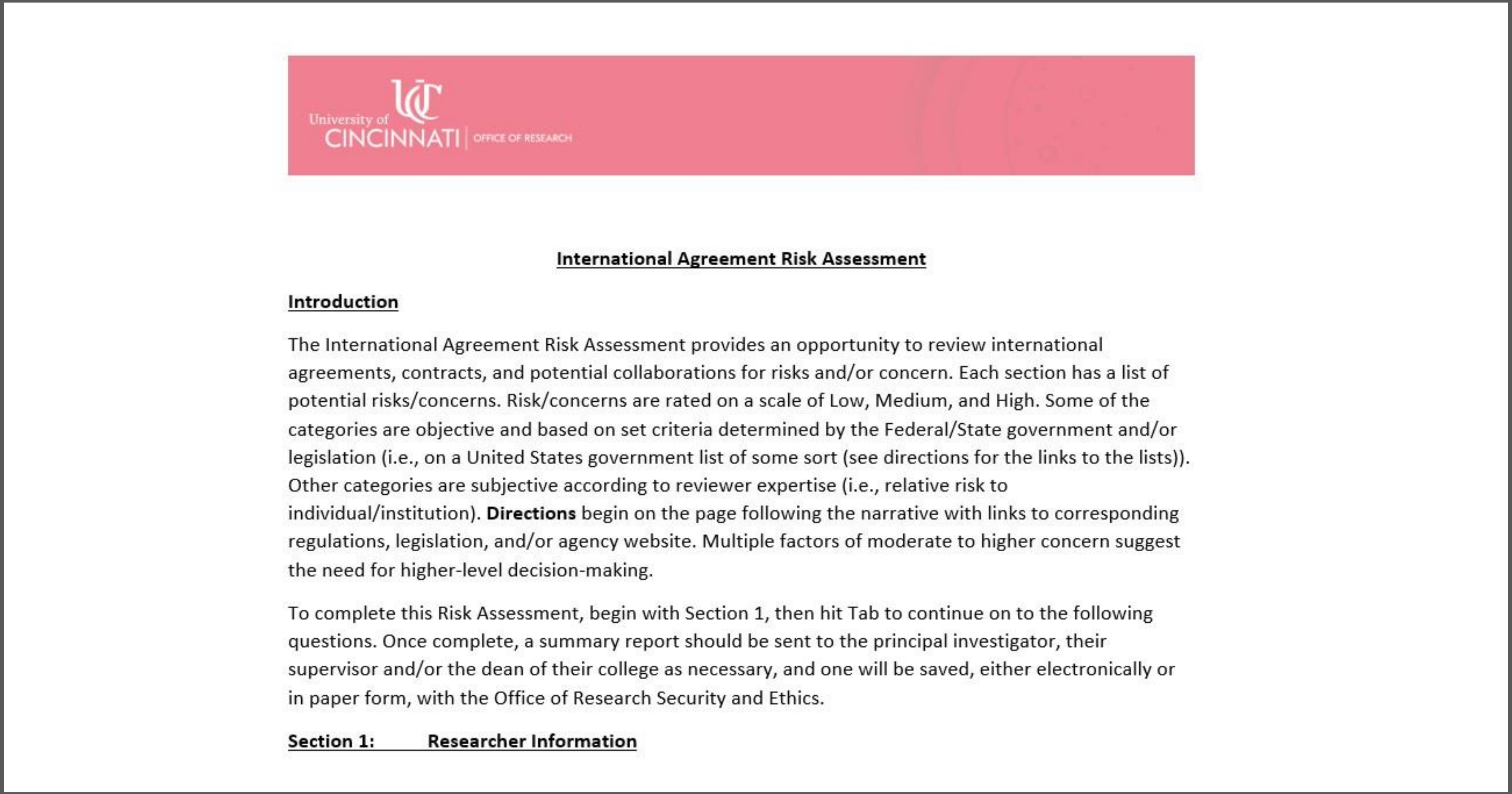
Guidance: Restricted Party Screenings & Navigating Existing Collaborations with Restricted Parties

Overview: The federal government maintains lists of restricted parties (individuals and organizations). Collaborating with restricted parties can create export control risks, including federal violations, as well as raise your risk profile. Federal funding agencies are conducting foreign influence security reviews on researchers even for fundamental research projects. The risk matrices vary by agency, and the restricted party lists change over time, so please contact the Export Controls & International Compliance (ECIC) team to conduct regular screenings.

1. **How can you request Restricted Party Screenings for your collaborators?** Email the ECIC team to request Restricted Party Screenings for any current or future collaborators including potential appointments, international collaborations including co-authors, and international conference organizers, etc. The screenings will identify if a person or organization is on a U.S. restricted list.

2. **What happens if you are associated or affiliated with a restricted party?** Every situation is different, so please contact the ECIC for a consultation and guidance. In addition, if you are sponsoring a research visitor and their home institution gets added to a restricted list, contact the ECIC team for guidance

3. **When a collaborator is from a restricted entity, what can you do with them?** This is too broad to comprehensively cover in an FAQ, contact the ECIC for specific guidance. You cannot send (mail, fax, email)



University of CINCINNATI | OFFICE OF RESEARCH

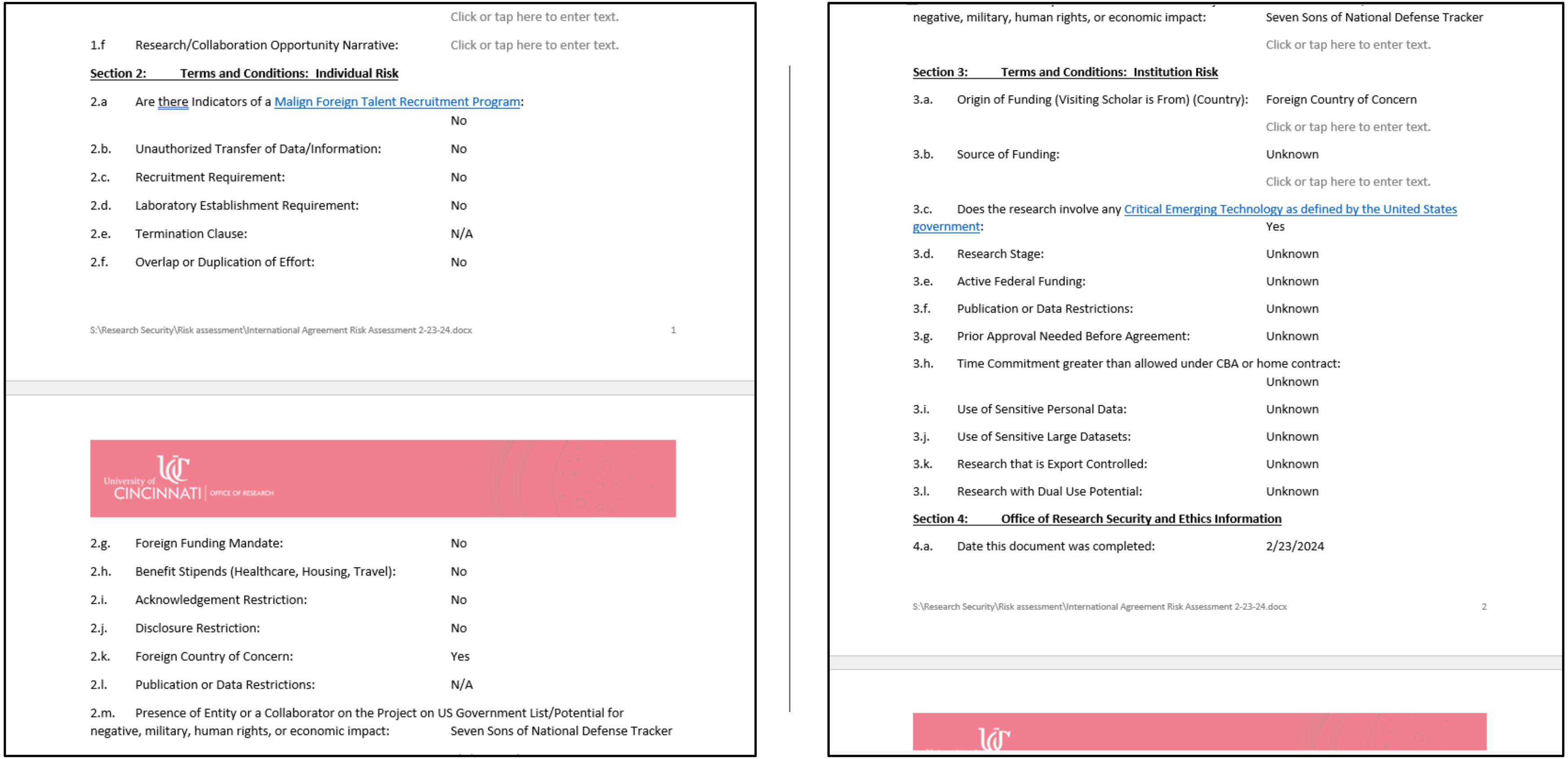
International Agreement Risk Assessment

Introduction

The International Agreement Risk Assessment provides an opportunity to review international agreements, contracts, and potential collaborations for risks and/or concern. Each section has a list of potential risks/concerns. Risk/concerns are rated on a scale of Low, Medium, and High. Some of the categories are objective and based on set criteria determined by the Federal/State government and/or legislation (i.e., on a United States government list of some sort (see directions for the links to the lists)). Other categories are subjective according to reviewer expertise (i.e., relative risk to individual/institution). **Directions** begin on the page following the narrative with links to corresponding regulations, legislation, and/or agency website. Multiple factors of moderate to higher concern suggest the need for higher-level decision-making.

To complete this Risk Assessment, begin with Section 1, then hit Tab to continue on to the following questions. Once complete, a summary report should be sent to the principal investigator, their supervisor and/or the dean of their college as necessary, and one will be saved, either electronically or in paper form, with the Office of Research Security and Ethics.

Section 1: Researcher Information



Click or tap here to enter text.

1.f Research/Collaboration Opportunity Narrative: Click or tap here to enter text.

Section 2: Terms and Conditions: Individual Risk

2.a Are there Indicators of a Malign Foreign Talent Recruitment Program: No

2.b. Unauthorized Transfer of Data/Information: No

2.c. Recruitment Requirement: No

2.d. Laboratory Establishment Requirement: No

2.e. Termination Clause: N/A

2.f. Overlap or Duplication of Effort: No

2.g. Foreign Funding Mandate: No

2.h. Benefit Stipends (Healthcare, Housing, Travel): No

2.i. Acknowledgement Restriction: No

2.j. Disclosure Restriction: No

2.k. Foreign Country of Concern: Yes

2.l. Publication or Data Restrictions: N/A

2.m. Presence of Entity or a Collaborator on the Project on US Government List/Potential for negative, military, human rights, or economic impact: Seven Sons of National Defense Tracker

negative, military, human rights, or economic impact: Seven Sons of National Defense Tracker

Click or tap here to enter text.

Section 3: Terms and Conditions: Institution Risk

3.a. Origin of Funding (Visiting Scholar is From) (Country): Foreign Country of Concern

Click or tap here to enter text.

3.b. Source of Funding: Unknown

Click or tap here to enter text.

3.c. Does the research involve any Critical Emerging Technology as defined by the United States government: Yes

3.d. Research Stage: Unknown

3.e. Active Federal Funding: Unknown

3.f. Publication or Data Restrictions: Unknown

3.g. Prior Approval Needed Before Agreement: Unknown

3.h. Time Commitment greater than allowed under CBA or home contract: Unknown

3.i. Use of Sensitive Personal Data: Unknown

3.j. Use of Sensitive Large Datasets: Unknown

3.k. Research that is Export Controlled: Unknown

3.l. Research with Dual Use Potential: Unknown

Section 4: Office of Research Security and Ethics Information

4.a. Date this document was completed: 2/23/2024

NCURA 66TH
ANNUAL MEETING

Rediscover Y-OUR Journey

Thank you!