



RESEARCH SECURITY ASSURANCE PLAN

What is Research Security?

The U.S. Government has defined research security as “safeguarding the research enterprise against the misappropriation of research and development to the detriment of national or economic security, related violations of research integrity, and foreign government interference.”¹ The National Science Foundation has stated, “Ultimately, research security is about ethical behavior, regardless of background or origin. Ethical behavior is foundational to the conduct of research, and it can only be achieved when everyone can collaborate in an open environment, shielded from the threats of dishonest and unethical behavior.”²

What is the IU Research Security Office?

The [Research Security Office](#) (“RSO”) is one of the core divisions in [IU Research](#). The primary mission of RSO is to assure research security at IU. The Chief Research Security Officer leads RSO, reports directly to the Vice President for Research, and is a member of IU Research’s senior leadership team.

Guiding Principles

RSO is guided by the [common values set out by the Association of American Universities \(“AAU”\) with regard to malign foreign influence](#)—academic freedom; free expression; inclusion and diversity; national interest; transparency; integrity; zero tolerance for harassment and coercion; and collaboration. RSO executes its research security program consistent with IU’s longstanding commitment to global engagement and academic freedom, as well as its [IU 2030 pledge](#) to make IU a welcoming environment of mutual respect where students, faculty, and staff from every corner of the world are embraced as Hoosiers.

Why is IU focusing on Research Security?

The U.S. academic community’s current focus on research security can be traced back to [then NIH Director Francis Collins’ “Dear Colleague Letter”](#) to various NIH funding recipients noting that “foreign entities have mounted systematic programs” to “inappropriately influence” federally funded research, noting concerns of diversion of intellectual property and failure of researchers to disclose substantial resources from other organizations, including foreign governments” which would inappropriately influence funding decisions. In the years since, Congress, the White House, and federal funding agencies have increased the number of research security requirements and guidance with which we must contend.³ Ensuring a research environment that is both secure and compliant with these requirements is key to the continued success of IU students, faculty, and staff, and to achieving the goals of the [IU 2030 Strategic Plan, Pillar Two](#).

Research Security Assurance Mission of RSO

The RSO seeks to assure faculty, staff, students, sponsors of research and other creative activities, and other stakeholders (collectively, the “**Research Community**”) of a research environment free from threats of those who wish to exploit IU’s open and inclusive academic research environment. RSO carries out this mission through engagement with the Research Community on topics related to research security, monitoring for research security concerns, and suggesting appropriate mitigation measures to the Research Community and IU leadership. RSO seeks to be a trusted advisor to the Research Community and IU leadership. **RSO does not approve or disapprove faculty/staff hiring, projects, collaborations, publications, proposals, travel, or the like.** RSO does monitor for risks to the Research Community and IU research environment posed in these areas.

RESEARCH SECURITY REVIEWS AND RISK INDICATORS

What does RSO Review? RSO reviews and provides input in a number of instances, including, but not limited to: (1) recruitment and visa sponsorship for both visiting scholars and faculty/staff (e.g., J-1, H-1B); (2) international travel; (3) sponsored awards; (4) potential conflicts of interest/commitment; and (5) international engagement.

¹ 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](#) (2022)

² National Science Foundation, Research Security, <https://new.nsf.gov/research-security> (last March 20, 2024).

³ E.g., see: National Defense Authorization Act for Fiscal Year 2019, [Pub. L. No. 115-232, § 1286, 132 Stat. 1636, 1761 \(2018\)](#); National Defense Authorization Act for Fiscal Year 2021, [Pub. L. No. 116-283, § 223, 134 Stat. 3388, 3415 \(2021\)](#); Creating Helpful Incentives to Produce Semiconductors for America and New and Enhanced Programs to Stimulate, Coordinate, and Advance Research in Semiconductors Act or the CHIPS and Science Act, [Pub. L. No. 117-245, 136 Stat. 977, 1042-1056 \(2022\)](#); [National Security Presidential Memorandum No. 33](#); U.S. Department of Defense, Department of Defense [Policy for Risk-Based Reviews of Fundamental Research](#) (June 2023); White House, Office of Science and Technology Policy, Foreign Talent Recruitment Program Guidelines (February 2024), available at <https://www.whitehouse.gov/wp-content/uploads/2024/02/OSTP-Foreign-Talent-Recruitment-Program-Guidelines.pdf>; White House, Office of Science and Technology Policy, Common Disclosure Form Policy (February 2024), available at <https://www.whitehouse.gov/wp-content/uploads/2024/02/OSTP-Common-Disclosure-Form-Policy.pdf>; National Science Foundation, [Proposal & Award Policies & Procedures Guide \(PAPPG\)](#), NSF 22-1 (2024).

Research Security Risk Reviews. A “research security risk” means an increased likelihood that research and development efforts or results will be misappropriated to the detriment of national or economic security, as well as related violations of research integrity and foreign government interference.⁴ RSO conducts reviews in various situations to mitigate research security risks. RSO seeks to work with the Research Community to mitigate research security risks in a way that maximizes the scope and impact of research and creative activities by the Research Community.

- **Visiting Scholars.** When an IU faculty or staff member seeks to sponsor a J-1 visa for a visiting scholar through IU, RSO is notified by the Office of the Vice President for International Affairs (“OVPIA”) and conducts a review for research security risks.
- **Faculty/Staff Hires.** RSO serves as a resource to hiring managers, school leadership, and other University stakeholders recruiting faculty and staff positions, and conducts reviews for research security risks on an as-requested basis.
- **International Travel.** RSO receives reports from the IU Chrome River system indicating international travel requests. RSO reviews travel for research security risks and advises travelers, as well as school leadership and other University stakeholders.
- **Sponsored Awards.** RSO is notified by the Office for Research Administration (“ORA”) when a sponsored award is made by an international sponsor to IU. RSO advises if any research security risks are posed by the engagement.
- **Conflicts of Interest/Commitment.** RSO monitors for research security risks posed by potential undisclosed conflicts of interest/commitment (“Conflicts”) through various means, including, but not limited to, review of publications, non-U.S. patent filings, and disclosures of Conflicts by IU personnel pursuant to Policy [UA-17](#).
- **International Engagement.** When new primary or sub-agreements with international institutions are considered by OVPIA, RSO is notified and advises OVPIA of any research security risks.

Potential Research Security Risk Indicators. In its reviews, RSO looks for potential research security risk indicators (“PRI”). PRIs can be different for entities as compared to individuals. **Indiana University prohibits discrimination on the basis of age, color, disability, ethnicity, sex, gender identity, gender expression, genetic information, marital status, national origin, race, religion, sexual orientation, or veteran status.** None of the foregoing may be used as a PRI in the course of RSO reviews. RSO is committed to upholding [Policy UA-01, Non-Discrimination/Equal Opportunity/Affirmative Action](#). RSO seeks to use publicly available, reliable, and objective information sources when determining the existence of a PRI.

Potential Research Security Risk Indicators (PRIs)

- Failure to make full disclosure in proposals for federal or other sponsored awards, including, but not limited to, inclusion of current and pending support, other research support, and a complete biosketch
- Individuals or entities sanctioned by United States Government or collaboration/association therewith⁵
- Involvement in STEM field or with [Critical and Emerging Technologies](#)
- Individuals or entities listed on U.S. Department of Defense list of entities engaging in “problematic activity” or collaboration/association therewith⁶
- Entities based in or existing under the laws of a “foreign country of concern” or collaboration/association therewith⁷
- Individuals or entities with evidence of cooperation, affiliation, or association with government of a foreign country of concern or collaboration/association therewith
- Indicators of participation in a malign foreign talent recruitment program⁸
- Filing patent application in a foreign country of concern or filing in any other country prior to filing in the United States

Questions or Concerns?

C. Collin Rich
Chief Research Security Officer
collinr@iu.edu

Tad Mitchell
Director, Research Security Assurance
tadmitch@iu.edu

⁴ Department of Defense, Countering Unwanted Influence in Department-Funded Research at Institutions of Higher Education (June 29, 2023), available at <https://media.defense.gov/2023/Jun/29/2003251160/-1/-1/1/COUNTERING-UNWANTED-INFLUENCE-IN-DEPARTMENT-FUNDED-RESEARCH-AT-INSTITUTIONS-OF-HIGHER-EDUCATION.PDF>

⁵ E.g., [15 C.F.R. pt. 744, supp. 4 \(2024\)](#); [15 C.F.R. pt. 744, supp. 6 \(2024\)](#); Office of Foreign Assets Control, Specially Designated Nationals (SDN) List, available at <https://ofac.treasury.gov/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists>

⁶ See FN 4

⁷ The term “foreign country of concern” is defined by the CHIPS and Science Act of 2022 (Pub. L. 117-167) as “(A) a country that is a covered nation (as defined in section 4872(d) of title 10 United States Code); and “(B) any country that the Secretary, in consultation with the Secretary of Defense, the Secretary of State, and the Director of National Intelligence, determines to be engaged in conduct that is detrimental to the national security or foreign policy of the United States.” Currently, these countries are the Democratic People’s Republic of North Korea, the People’s Republic of China, the Russian Federation, and the Islamic Republic of Iran.

⁸ [§ 10638\(4\), CHIPS and Science Act](#)