# POLICY STATEMENT 46
# RESEARCH SECURITY FOR FEDERALLY FUNDED RESEARCH

POLICY DIGEST
Monitoring Unit: Office of Research & Economic Development
Initially Issued: September 30, 2025

## I. PURPOSE

This policy outlines Louisiana State University and Agricultural and Mechanical College's approach to fostering a culture of safeguarding the security of both our research enterprise and all individuals traveling in their role as an LSU researcher. This policy is in alignment with federal directives and is critical to ensuring the knowledge generated at LSU is protected from all potential threats. This includes, but is not limited to, cybersecurity risks, data breach, foreign malign influence, and other security threats that undermine the integrity of the university's research ecosystem. This policy complements LSU PS 68 University Intellectual Property Rights in Sponsored Research Projects, PS 69 Research Misconduct, and PS 119 Compliance with Export Control Regulations.

This policy is designed to ensure compliance with federal regulations, including the National Security Presidential Memorandum 33 (NSPM-33) and the CHIPS and Science Act of 2022, which provide the foundational framework for addressing national security risks in research and technology development. LSU recognizes the evolving nature of threats to the security of research and intellectual property (IP). Potential risks include, but are not limited to, foreign governments, entities, and individuals seeking to undermine U.S. interests or acquire sensitive knowledge who may attempt to infiltrate research institutions to exploit critical technologies. These threats are exacerbated by rapid technological advances and the growing global interconnectedness of research efforts. As such, it is vital to strengthen security protocols surrounding our research processes, personnel, and collaborations.

This policy is exclusively applicable to research security for federally funded research. For information regarding research security outside the scope of this policy, please contact the LSU Office of Research & Economic Development (ORED).

## II. DEFINITIONS

**Covered Individuals** – As defined per Section 10634 of the CHIPS and Science Act of 2022, an individual who contributes in a substantive, meaningful way to the development or execution of the scope of work of a federally-funded project. Covered individuals include Principal Investigators (PIs), Co-PIs, and individuals instrumental to the research project as determined by the PI

**Cybersecurity** – The practice of protecting a system against threats from criminal or unauthorized sharing of electronic data and intellectual property

**Foreign Countries of Concern** – Any country identified by the U.S. Department of Commerce as a foreign adversary country or a banned country for international travel or trade

**Foreign Maligned Talent Program Recruitment** – An effort or program directed by foreign adversary countries, as identified by the U.S. Department of Commerce, whose directive is to recruit and fund talent, faculty, researchers, and students to acquire or import proprietary research including but not limited to data, technology, software, peer review, and intellectual property

**Undue Foreign Influence** – The inappropriate or inadvertent sharing or capture of proprietary intellectual property, unpublished data, and grant proposals through leverage by a foreign adversary country

## III. GENERAL POLICY

LSU faculty, staff, and students must follow the institution's research security protocols to remain compliant with both federal and institutional research security mandates. These procedures, which are meant to protect federally funded research administered at LSU, are coordinated by the LSU Office of Research & Economic Development (ORED).

## IV. PROCEDURES

A. Undue Foreign Influence Review

Undue foreign influence poses a significant risk to academic freedom, national security, and the integrity of research. Foreign actors, whether states or entities, may seek to manipulate the direction of U.S. research or access sensitive data to further their own objectives. LSU will protect against undue foreign influence. ORED will monitor international research projects and international partnerships to ensure foreign involvement does not compromise academic independence. Per federal regulations, LSU researchers are required to disclose all foreign affiliations or foreign funding sources.

B. Foreign Malign Talent Program Reviews

This review will focus on individuals whose activities may pose a risk to the LSU research enterprise, intellectual property, proprietary data, and U.S. national security. ORED will assess foreign interactions and activities involving researchers, faculty members, and personnel from foreign adversary countries, with particular attention to any connections to foreign governments or entities that have a history of utilizing academic research for espionage, technology theft, or geopolitical advantage.

C. Cybersecurity Threats

Threats come in many forms and from many directions; therefore, LSU must ensure the protection of all research data, intellectual property, and sensitive communications from cyber threats. This includes safeguarding our research infrastructure from external attacks by state-sponsored actors, cybercriminals, and other malicious entities. To address these risks, LSU implemented robust cybersecurity measures across all research systems (see PS 122 IT Risk Management, PS 124 Data Management, PS 126 Encryption, PS 130 Application Security, and PS 131 Network Security), including secure data storage, encrypted communications, and multi-factor authentication for research-related systems. Researchers will also be trained

on cybersecurity best practices, including how to recognize phishing attempts and mitigate cyber risks associated with research data sharing. LSU will collaborate with federal agencies and industry partners to stay ahead of emerging cybersecurity threats and maintain a resilient infrastructure.

D. Risk Management and Data Management

Effective risk management is essential for protecting our institution's research endeavors. LSU will employ a comprehensive risk management framework to assess and mitigate risks related to foreign influence, cybersecurity, intellectual property protection, and compliance with federal regulations. Research data, particularly that which is classified or sensitive, must be handled in accordance with federal guidelines including Export Controls (See PM 45 Compliance with Export Control Regulations). This includes compliance with the requirements of the National Institutes of Health (NIH) and other federal agencies overseeing research. All data related to federally funded research must be securely stored, and access will be strictly controlled to prevent unauthorized use or access, especially in the context of international collaborations.

E. Foreign Travel Review

ORED will collaborate with the LSU International Travel Oversight Committee (ITOC) and review the funding source for the travel, security landscape of the destination, the purpose of the trip, and the nature of the activities planned. ORED will work with U.S. government agencies, such as the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI), to provide guidance on high-risk destinations. LSU will require travelers to report any research materials or data they intend to take with them, ensuring there is full compliance with U.S. export control laws.

F. Foreign Gift/Contract Reviews

Foreign gifts and contracts present potential conflicts of interest and security risks, particularly when they are tied to foreign governments or entities. In accordance with NSPM-33, LSU will review foreign gifts and contracts. The review will be thorough, with a focus on ensuring that foreign financial contributions do not interfere with academic freedom, the integrity of research, or national security. If any concerns arise regarding the influence or intent behind a foreign gift or contract, the university will engage in a transparent and collaborative review process, involving legal, financial, and security experts. Such a review will be coordinated by ORED.

G. Research Security Training and Covered Individuals

Research Security training is required annually for covered individuals. The training will be online, and a certificate of completion will be autogenerated upon successful completion of the course. Research Security training will be required for covered individuals as defined by Section 10634 of the CHIPS and Science Act of 2022: an individual who contributes in a substantive, meaningful way to the development or execution of the scope of work of a project funded federally. Covered LSU researchers include Principal Investigators (PIs), Co-PIs, and individuals instrumental to the research project.

## V. ROLES AND RESPONSIBILITIES

A. Office of Research and Economic Development (ORED)

The Associate Vice President for Research Compliance, Integrity & Analytics in ORED is responsible for overseeing all Research Security training and compliance reviews required as noted within the policy. The Associate Vice President and designees are responsible for communicating with covered individuals required to undergo reviews as noted above.

B. Covered Individuals

All covered individuals required to complete research security reviews noted above will submit any requested documentation including biosketches, contracts, and other documents as requested by ORED. All covered individuals are required to self-disclose any relationships with foreign maligned programs as required under NSPM-33 and the CHIPS and Science Act of 2022.

## VI. SOURCES

CHIPS and Science Act of 2022
Determination of Foreign Adversaries
National Security Presidential Memorandum-33 (NSPM-33)
PM 45 Compliance with Export Control Regulations
PS 15 Academic Freedom, Free Speech, and Tenure
PS 68 University Intellectual Property Rights in Sponsored Research Projects
PS 69 Research Misconduct
PS 119 Compliance with Export Control Regulations
PS 122 IT Risk Management
PS 124 Data Management
PS 126 Encryption
PS 130 Application Security
PS 131 Network Security
National Science Foundation No. 149: Updates to NSF Research Security Policies

## VII. APPENDICES

FASOP AS-18 High Risk Travel to Restricted Regions
LSU Office of Research & Economic Development website