ACUA
Association of College & University Auditors

March 24-26, 2026

ACUA VIRTUAL SPRING SUMMIT

Audit in Action

Research Security Program Audits: Focus on Researchers

Presented by: Allen Phelps, CPP, PCI, CISSP, CISA
Founder + CEO of IPTalons

Thursday, March 26, 2026

Housekeeping: Presumptions

- Research investments (government and corporate) will continue to trend towards applied research, increasing the number of university research programs involved in sensitive critical technologies, and subsequently, the number of principal investigators and covered individuals.

- Government funding agencies will increase their mandates for more transparency and risk mitigation planning related to foreign influence and research security risks, such as unreported research collaborations or sources of funding.

- Research universities will see more specific compliance requirements related to research security controls and similar terms and conditions in grants, contracts, and other agreements.

Housekeeping: 2026 Prediction

Federal funding agencies will begin to audit your institutions for compliance with research security program controls.*

* Based on the comments from panel speakers at the Academic Security and Counterexploitation (ASCE) seminar in February 2026.

Housekeeping: Session Purpose

This session is designed to provide university auditors with essential, practical approaches, tools, and methodologies to assess compliance effectively in the rapidly evolving domain of research security.

Learning Objectives

After attending this session, you will be able to:

- Understand the Research Security Management practice and recognize the regulatory landscape impacting research security (State/Federal).
- Identify the components of an effective research security program audit.
- Articulate the strategic importance of implementing a professional research security program – and become its audit champion!
- Understand what research security program components must be implemented to meet the basic requirements and be able to describe what an effective program looks like.
- Design a practically-scoped audit plan for your research security program.

Session Talk Tracks

1

Basecamp Recap: Understanding Research Security, State and Federal Regulatory Landscapes, and Research Security Audit Plans.

2

Risk-Based Audit Frameworks: Standardized matrices for classifying research projects by risk tier (e.g., federally funded, proprietary IP, dual-use technology) to prioritize audit resources.

3

Compliance Checklists: Actionable, focused checklists targeting high-risk areas such as annual research security training, foreign talent program participation, export control adherence, and required disclosure completeness (Conflicts of Commitment/Interest).

4

Data Verification Tools: Techniques and system requirements for verifying researcher disclosures against institutional data, grant records, and public source information.

Recap: What is Research Security?

- Research security involves protecting the research enterprise—including intellectual property, data, and technology—from misappropriation, foreign interference, and exploitation.

- It ensures that federally funded, basic research remains secure, ethical, and used for its intended purpose, preventing the misuse of research assets and proprietary information by foreign actors.

- NSF: “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.”

Recap: Goal of Research Security

Reduce the risk of research asset misuse, loss, theft, and misappropriation by internal and external threat actors, foreign and domestic.

Audits should be test for risk management and reduction.

Recap: Federal Research Security

- **National Security Presidential Memorandum 2 (NSPM-2):** Outlines U.S. government policy on scientific and technological cooperation, emphasizing the need to protect national security interests from foreign adversaries. (Feb. 2025 - Iran focused)

- **National Security Presidential Memorandum 33 (NSPM-33):** Requires federal agencies to strengthen protections against foreign influence in federally funded R&D. Key areas include disclosure requirements, digital persistent identifiers (DPIs), and research security programs at awardee institutions.

Recap: Federal Research Security (continued)

- **CHIPS and Science Act**: Aims to boost U.S. competitiveness in semiconductor manufacturing and scientific research. It contains provisions to protect federally funded research and technology from foreign adversaries, aligning with NSPM-33.

- **NIST Interagency Report 8484 (NIST IR-8484)**: Provides a framework for assessing and mitigating foreign influence risk in research. It offers a structured approach to risk management, including identifying, analyzing, and treating risks related to foreign talent recruitment programs and other global engagements.

Recap: Federal Research Security (continued)

- **Federal Research Funding Agencies:** Each of the federal agencies that provides research grants and contract funding has applied its own research security and compliance requirements.

- **Department of War / Defense:** most comprehensive and specific, citing NDAA requirements and risk matrix-derived decisions that impact the individual researchers on the grant or contract.

- **NSF, NSF, DoE, NASA, and NOAA:** agencies have also implemented risk matrices that may augment how individual grant research security controls should be applied.

(see COGR matrix: https://www.cogr.edu/cogr-matrix-science-security-laws-regulations-and-policies)

Recap: Federal Research Security (continued)

Federal Guideline or Regulation	Key Requirements
NSPM-33	• **Designate a Research Security Officer** • **Implement a Formal Research Security Program:** Institutions must implement research security programs that include elements of cybersecurity, foreign travel security, and research security training. • **Standardized Disclosure Requirements:** implement standardized disclosure forms for conflicts of interest and commitment. • **Consequences for Violations:** Establishes consequences for researchers who violate disclosure requirements. • **Digital Persistent Identifiers (DPIs):** Requires the use of DPIs, like ORCID iD, to make it easier for researchers to track their activities and for agencies to verify disclosures.

Recap: Federal Research Security (continued)

Federal Guideline or Regulation	Key Requirements
CHIPS Act	• **Codifies NSPM-33:** The research security guidelines provided in the NSPM-33 are now federal law and research universities must implement the research security program components and related compliance controls.
NIST IR-8484	• Published by the National Institute of Standards and Technology (NIST), this report provides a **framework for a research security plan.** It serves as a guide for organizations to implement the research security programs required by NSPM-33. • **Research Security Plan Checklist:** Provides a checklist to help organizations develop and review their research security plans. • **Risk-Balanced Approach:** Recommends a risk-balanced methodology to protect intellectual property while promoting open collaboration. • **Cybersecurity and Export Controls:** Outlines best practices for integrating cybersecurity and export control measures into a comprehensive research security program.

Recap: Federal Research Security (continued)

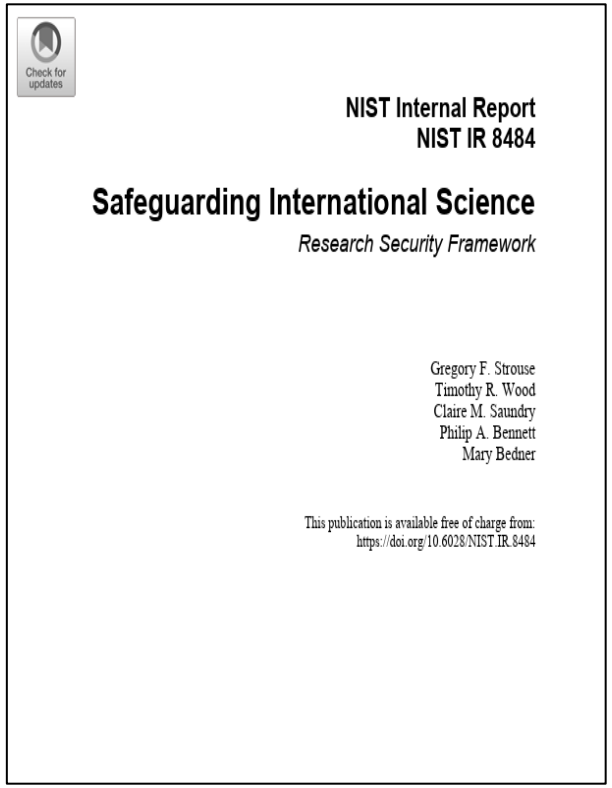
Federal Guideline or Regulation	Key Requirements
NSPM-2	• This memorandum focuses on a specific foreign policy and national security objective, primarily targeting the Iranian regime. Its key requirements are centered on using a "maximum pressure" campaign through economic sanctions and export controls. It directs U.S. departments to enforce a **robust export control and sanctions campaign** to restrict the flow of technology and components to Iran for military purposes

Recap: Federal Research Security (continued)

Research Security Program Framework

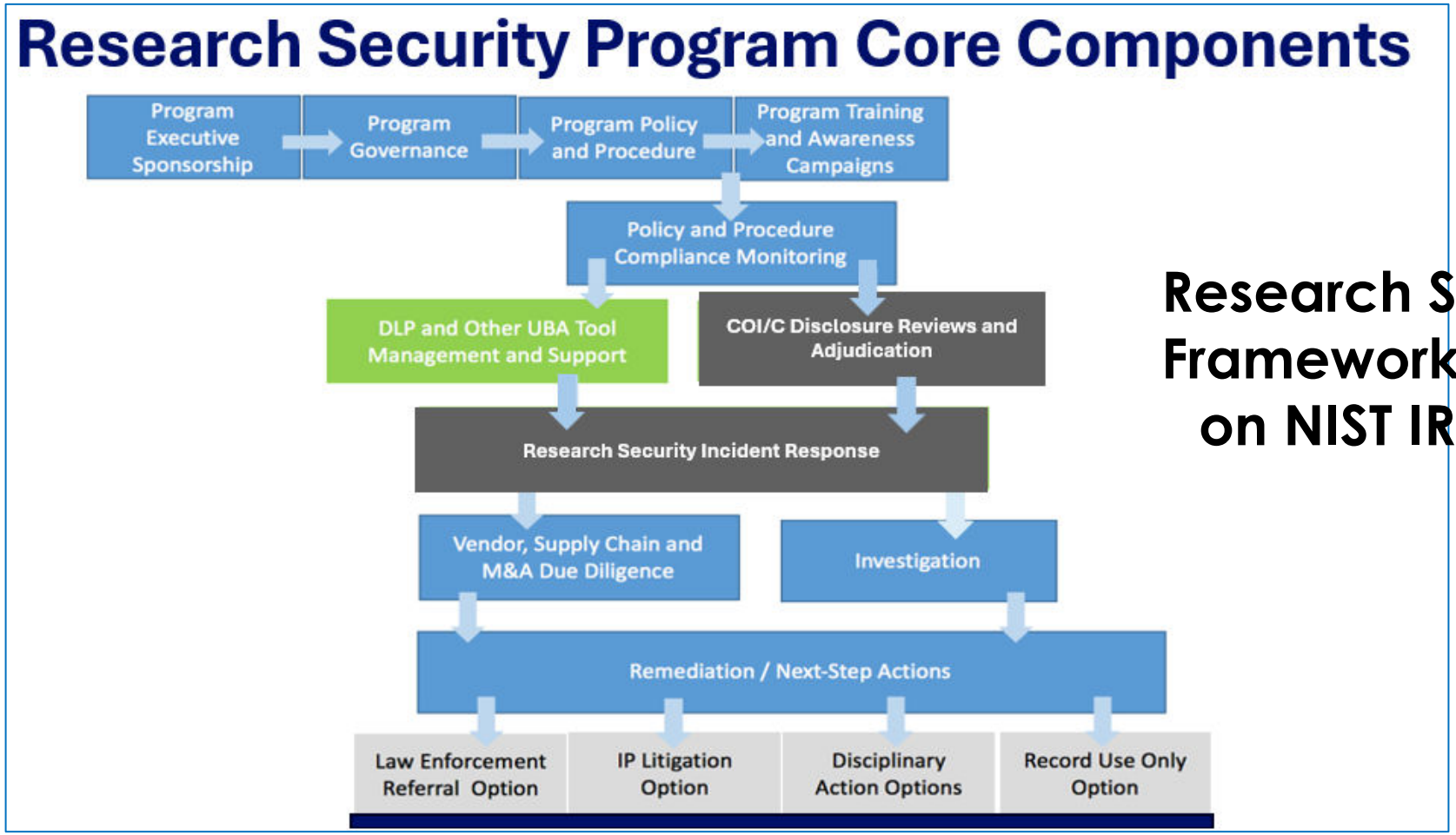
- National Research Security Program Standard – at least it's a viable candidate
- Follows the evolution of the NIST cybersecurity framework models
- Provides consistent and repeatable foreign influence risk reviews and adjudications

- **Audit Recommendation:** build your audit plan to focus on compliance with these research security program elements



https://doi.org/10.6028/NIST.IR.8484

Recap: Federal Research Security (continued)



Research Security Framework Based on NIST IR-8484

Recap: State Laws + Rules

Current State-Level Research Security Requirements

- Florida
- Texas
- Louisiana
- Arkansas
- Ohio

- …other States have similar legislation or are considering it.

Recap: Florida Research Security

Florida: SB 846 (The "Gold Standard" of Restriction)

- Florida remains the most aggressive state in this arena. This law fundamentally changed how public universities interact with "Foreign Countries of Concern" (e.g., China, Russia, Iran, North Korea).

- **Prohibited Agreements:** State universities and colleges are barred from entering into agreements or partnerships with any entity based in a country of concern unless specifically authorized by the Board of Governors.

- **Hiring Restrictions:** Strict vetting is required for researchers and graduate assistants from these countries. Many institutions now require an additional layer of security clearance for such hires.

- **Gift Transparency:** Lowered the threshold for reporting foreign gifts to **$50,000**, with severe financial penalties for non-compliance (up to 105% of the gift's value).

Recap: Texas Research Security

SB 1565 (The Institutional Framework)

Texas focused on mandating a security infrastructure within its massive university systems.

- **Research Security Officers (RSOs):** Every public institution of higher education must designate a dedicated RSO.
- **Policy Frameworks:** Boards must establish frameworks to mitigate espionage and ensure compliance with federal CUI (Controlled Unclassified Information) standards.
- **Mandatory Training:** RSOs are required to attend an annual ASCE seminar hosted by Texas A&M University to ensure a unified state-wide defense posture.

Recap: Louisiana Research Security

HB 454 (The Emerging Model)

Louisiana has recently moved to formalize research integrity requirements that mirror federal "Malign Foreign Talent Recruitment Program" (MFTRP) prohibitions.

- **Disclosure of Support:** Requires researchers to disclose all "Significant Financial Interests" and third-party funded travel.

- **Intellectual Property (IP) Safeguards:** Explicitly mandates that any transfer of proprietary data to foreign entities must be governed by state-approved Material Transfer Agreements (MTAs).

Recap: Arkansas Research Security

Act 473 (The Research and Education Protection Act of 2025)

Arkansas adopted a preventative approach to research security to reduce foreign influence at the perimeter.

- **Foreign Influence Screening:** Requires universities to screen candidates for research positions who meet certain Countries of Concern citizenship factors against restricted party (export controls) and foreign influence databases.
- **Pre-Employment and Pre-Invitation:** Screening is conducted as part of the suitability due diligence phases of pre-employment (faculty, staff) and pre-invitation to research (students) processes.
- **Reporting:** Universities must report screening metrics annually to their Boards of Trustees and the Arkansas legislature to ensure compliance.

Recap: Ohio Research Security

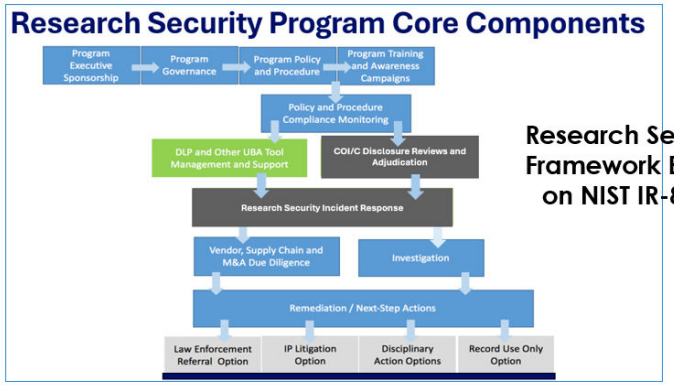
SB-1 (Advance Ohio Higher Education Act)

Ohio made sweeping reforms to its higher education system in 2025 that resulted in specific research security requirements.

- **Prohibition:** Explicitly prohibits public colleges and universities from accepting funding, donations, or gifts from China in an effort to protect intellectual property from theft.

- **Research Partnerships:** Requires greater oversight of university activities, which indirectly affects how research partnerships and funding are managed.

Research Security Audit Plans



Research Security Framework Based on NIST IR-8484

- Auditing a research security program is less about "policing" researchers and more about creating a **resilient shield** around intellectual property and national interests.
- As research becomes increasingly global, the risks of data theft, foreign interference, and regulatory non-compliance have skyrocketed.
- The primary purpose of these audits is to ensure that a research institution is actually doing what it says it's doing to protect its work and serving as responsible financial stewards of federal research funding.

Research Security Audit Plans

Your audit plan should map to these research security drivers.

Research Security Audit Plans: Regulatory

Goal: Ensure the university adheres to all federal, state, and international regulations, policies, and national security laws. This is essential for protecting university and national interests and avoiding legal action.

Understand the Requirement: Verify that research projects are compliant with regulations like NSPM-33, export control laws (EAR, ITAR), and sponsor-specific requirements (e.g., NIH, NSF, DOD).

Research Security Audit Plans: Regulatory (continued)

How to Test Compliance:

- **Verify Institutional Policies and Procedures:** Confirm that the university has robust and clearly defined policies regarding export controls, conflict of interest, and cybersecurity. Verify these policies are regularly reviewed and updated.

- **Review Disclosure of Other Support/Affiliations:** Audit disclosures made by key research personnel regarding foreign affiliations, financial interests, and other sources of support to ensure compliance with NSPM-33 and sponsor requirements. Check for completeness and accuracy against other available records.

- **Review Export Control Classifications and Technical Data Controls:** For relevant projects, verify that technological data and physical items have been correctly classified under EAR or ITAR and that appropriate controls (e.g., access restrictions, secure storage) are implemented.

- **Audit Compliance Training Records:** Confirm that relevant faculty, staff, and students are required to complete mandatory training on research security, export controls, and conflict of interest. Verify high rates of participation.

Research Security Audit Plans: Financial Stewardship

Goal: Ensure that research grants and funds are managed responsibly, with transparency, accountability, and proper usage of resources.

Understand the Requirement: Review procedures, financial conflicts of interest, and outside activity disclosure forms to ensure that the university is properly accounting for all research funding, protecting against fraud and misuse, and fulfilling the fiduciary expectations of sponsors.

Research Security Audit Plans: Financial Stewardship

- **Review Expense Allowability:** For a sample of grants, review expenditures for compliance with OMB Uniform Guidance and specific award terms. Verify that expenses are allocable, reasonable, and necessary for the research.
- **Verify Effort Reporting/Effort Certification:** Confirm that the university has a reliable system for researchers to certify the amount of effort committed to different projects. Test the timeliness, completeness, and accuracy of effort certifications against payroll records.
- **Review Grant Accounting and Financial Reporting:** Select a sample of financial reports submitted to sponsors and verify that the figures reconcile with the university's general ledger. Review reconciliations and internal control reviews.
- **Review Financial Conflict of Interest (FCOI) Management Plans:** Where conflicts exist, verify that management plans are in place and ensure compliance with PHS/NIH regulations. Test whether controls in the plan are being implemented and monitored.

Research Security Audit Plans: Contract Obligations

Goal: Meet all research agreement terms, confidentiality clauses, and commitments with sponsors and partners.

Understand the Requirement: Fulfill all legal promises made in grants, contracts, and other research-related agreements, ensuring that the work is performed as agreed and data is protected.

Research Security Audit Plans: Contract Obligations

- **Review Data Use and Data Sharing Agreements (DUA/DSA):** Select projects involving controlled unclassified information (CUI) or protected health information (PHI) and verify that required DUAs are executed. Verify adherence to requirements for data storage, access, and destruction. (Prepare for CMMC 2.0)
- **Confirm Subrecipient Monitoring Processes:** For awards where the university is the primary recipient, audit procedures for monitoring subrecipients. Verify that the university ensures subrecipient compliance with terms, conditions, and regulations. (NOFORN?)
- **Confirm Timely Reporting of Project Milestones:** For selected contracts, verify that all technical, financial, and progress reports have been submitted according to the agreed-upon schedule.
- **Confirm Management of Proprietary/Confidential Information:** Audit procedures for the handling and storage of proprietary information provided by research partners. Verify that access controls and non-disclosure agreements are in place.

Research Security Audit Plans: Lawsuit Avoidance

Goal: Mitigate legal risks and prevent intellectual property (IP) disputes, non-compliance issues, and liability claims.

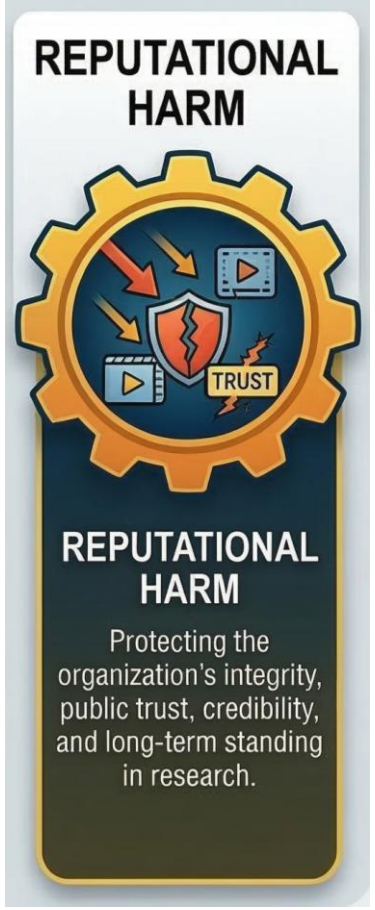
Understand the Requirement: Implement strong internal controls to minimize the university's legal exposure related to research activities and protect the university from lawsuits that could impact finances and operations.

False Claims Act (FCA) violations in research universities involve knowingly submitting false claims for federal funding, often resulting in treble damages. Common violations include research misconduct (fabrication, falsification), mischarging grant accounts (salary, equipment), and certifying compliance with regulations (like NSPM-33 or other grant requirements) while failing to meet them.

Research Security Audit Plans: Lawsuit Avoidance

- **Review Export Control Classifications and Technical Data Controls (Again):** Non-compliance with EAR or ITAR can result in significant legal consequences, making robust data control testing crucial.
- **Verify Intellectual Property Disclosure and Management:** Review policies for the disclosure of inventions and IP developed during research. Confirm that disclosures are made in accordance with policy and that appropriate protection (patents, etc.) is sought.
- **Test Conflict of Interest and FCOI Management Processes:** Inadequate management of financial or personal conflicts can lead to legal challenges over the integrity of the research. Confirm robust review and enforcement mechanisms. (Check foreign collaborations)
- **Confirm Management of Compliance Violations and Allegations:** Review university processes for investigating allegations of research security breaches, research misconduct or non-compliance. Test if these processes are impartial, thorough, and in line with regulatory requirements.

Research Security Audit Plans: Reputational



Goal: Protect the organization's integrity, public trust, credibility, and long-term standing in the research community. Failing research security compliance can result in permanent reputational damage, essentially barring the university from attracting federal funding for critical technology research.

Understand the Requirement: Safeguard the university's reputation by ensuring research is conducted ethically and transparently, preserving trust with the public, government agencies, and research partners.

Research Security Audit Plans: Reputational

- **Verify Public Disclosures and Reporting Integrity:** Select a sample of public statements, press releases, or official reports related to research findings and verify that they are accurate and not misleading.
- **Review Ethics in Research Misconduct Reporting:** Evaluate the university's processes for handling allegations of plagiarism, fabrication, or falsification. Verify that investigations are conducted objectively and in compliance with requirements.
- **Verify Oversight of High-Risk Research:** Review the university's mechanisms for overseeing research involving human subjects, animal subjects, or biohazards. Confirm that relevant oversight committees (e.g., IRB, IACUC, IBC) are active, well-staffed, and conducting proper reviews.
- **Audit Disclosures of Research Collaborations and Foreign Talent Recruitment Programs:** Verify that university personnel disclose participation in any foreign talent recruitment programs, which can raise concerns about foreign influence and intellectual theft. Test against university-wide reporting mechanisms.

Risk-Based Audit Plan Framework

Risk Tier	Research Characteristics	Potential Drivers Impacted	Audit Priority & Frequency	Recommended Audit Procedures
Tier 1: High Risk	Dual-use technology (military/civilian), Export Controlled (ITAR/EAR), Select Agents/Biohazards, Fundamental Research with "foreign talent“ participants or high-risk research collaborations.	Regulatory Compliance, Lawsuit Avoidance, Reputational Harm	**Highest** (Annual or Project-Specific)	Deep dive into Technology Control Plans (TCPs), physical/digital access logs, and 100% verification of foreign affiliation disclosures. (Seek Risk Mitigation Plans)
Tier 2: Elevated Risk	Proprietary IP with corporate sponsors, Controlled Unclassified Information (CUI), high-dollar federal grants (>$5M), international sub-awards.	Financial Stewardship, Contract Obligations, Lawsuit Avoidance	**Medium-High** (Every 18–24 months)	Review of Data Use Agreements (DUAs), testing of sub-recipient monitoring, and detailed expense reconciliation for "burn rate" anomalies.
Tier 3: Moderate Risk	Federally funded "Fundamental Research" with no export restrictions, human subjects (IRB), standard Material Transfer Agreements (MTAs).	Financial Stewardship, Regulatory Compliance	**Medium** (Rotational/Cycle-based)	Verification of effort reporting, COI disclosure completion rates, and standard IRB/IACUC protocol adherence.
Tier 4: Low Risk	Internally funded research, humanities/social sciences (non-sensitive data), no international collaborations or foreign funding.	Reputational Harm (Minimal), Financial Stewardship	**Low** (Ad-hoc or Desktop Review)	Periodic "spot checks" of financial transactions and general policy awareness surveys.

Risk-Based Audit Plan Framework: Scope

Before selecting samples, pull data from the **Research Security Office**, **Office of Sponsored Programs (OSP),** and the **Tech Transfer Office**. Look for "High-Risk Flags" such as:

- Research collaborations or funding sources from high-risk Foreign Influence Groups (FIGs) from Countries of Concern (China, Russia, Iran, and North Korea)
- Keywords in abstracts (e.g., "hypersonic," "pathogen," "semiconductor")
- Sponsors from the Section 1286 List (Foreign Entities of Concern)
- Projects requiring a **CMMC (Cybersecurity Maturity Model Certification)** level of 2 or higher

Risk-Based Audit Plan Framework: Resource

Resource Allocation: Instead of auditing 5% of all grants, use a weighted model:

- **60% of audit hours** dedicated to **Tier 1 & Tier 2** (The "Deep Dives")
- **30% of audit hours** dedicated to **Tier 3** (The "Systemic Controls")
- **10% of audit hours** dedicated to **Tier 4** (The "Baseline Compliance")

Reminder: Mandatory NSPM-33 Compliance Requirements:

- All federally funded researchers – principal investigators and covered individuals (i.e., students, post-docs, and visiting scholars working on those projects) – must complete an annual research security training and attest that they are not participants in a Malign Foreign Talent Recruitment Program (MFTRP).

Risk-Based Audit Plan Framework: Testing

Don't audit research security in a vacuum. When performing a standard **Financial Audit** of a department, "piggyback" on the visit to check for **Research Security** indicators:

- Do federally funded researchers have a **Research Security Risk Mitigation Plan** (NSPM-33, CHIPS Act, and NDAA compliance)?
- Are lab doors propped open (Physical Security)?
- Are there foreign visitors in the lab who aren't on the official project roster (Export Control)?
- Are laptops used for CUI-level research encrypted and managed by Central IT?

Risk-Based Audit Plan Framework: Checklist

Tier 1: Export Control & High-Security Audit Checklist

Audit Area	Specific Control to Test	Auditor's "Red Flag"
Personnel Screening	Verify all project personnel (including students/visiting scholars) have undergone **Restricted Party Screening (RPS)**.	Personnel added to the lab payroll before the RPS clearance was granted.
Physical Security	Conduct a site visit to ensure labs containing restricted tech have **locked doors, badge access**, and "Authorized Personnel Only" signage.	Propped-open doors or shared lab spaces where unauthorized students can see restricted screens/equipment.
Information Security	Confirm that data is stored on **air-gapped or encrypted servers** and not on personal cloud drives (Dropbox, Google Drive).	Use of personal email addresses or unencrypted USB drives to transfer project data.
Foreign Travel	Review travel logs for researchers. Did they take **"clean" loaner laptops** when traveling to high-risk countries?	Laptops containing restricted software taken to countries on the EAR/ITAR restricted list without a license.
Visual Compliance	Check if equipment/blueprints are covered or shielded from the view of foreign nationals not on the approved TCP.	Restricted blueprints left on a communal workbench or visible through a window.
Disclosure Accuracy	Cross-reference the researcher's **Conflict of Interest (COI)** filing with their recent publications and international speaking engagements.	Publications co-authored with foreign entities that were never disclosed to the Research Security Office.

Policy | Procedure Checklist

- Are there documented policies that align with NSPM-33 requirements?
- Do the policies address conflicts of interest and commitment, and foreign influence?
- Is there a clear procedure for reporting foreign engagements and gifts?
- Are the policies easily accessible to all relevant personnel?
- Does your university train researchers, staff, graduate assistants, and students on research security issues (e.g., research security, cybersecurity, export controls, foreign travel security, foreign talent recruitment programs)?

Risk Management Checklist

- Is there a documented **risk assessment process** for global engagements?
- Does the process include due diligence on visiting professors, collaborations, and partnerships?
- Is there a formal review process for all **foreign gifts over $50,000**?
- Are there controls in place to manage the research security risks identified in **NIST IR-8484**?
- Does your university conduct a research security annual assessment to ensure that it is updated to the changing risk landscape?

Risk Management Checklist

- Is there a straightforward process for reporting foreign engagements to the internal working group and federal agencies as required?
- Are there documented procedures for handling alleged violations or concerns?
- Is there a research security incident response team?
- Is there a research security investigation protocol?
- Are international travel briefings provided to researchers carrying research information?
- Is there a “loaner laptop” program to ensure researchers do not travel with their daily work laptops?

Challenge:
Measuring Research Security Program Effectiveness

This two-day public workshop focused on potential measures of effectiveness and performance, and the data needed, to assess research security and protection efforts in higher education by a range of federal agencies.

AGENDA

DATE(S)
May 22 - 23, 2025

LOCATION
National Academy of Sciences Building
2101 Constitution Ave NW
Washington DC 20418
USA

PROJECT
Assessing Research Security Efforts in Higher Education: Experts Meeting and Workshop Series

DIVISION
Policy and Global Affairs

UNITS
Committee on Science, Engineering, Medicine, and Public Policy

U.S. Science and Innovation Policy

Video Playlist

Dr. Rebecca Keiser
Chief of Research Security, Strategy, and Policy and acting Chief of Staff
U.S. National Science Foundation

Before the
Subcommittee on Investigations and Oversight
Committee on Science, Space, and Technology
United States House of Representatives

"Research Security: Examining the Implementation of the CHIPS and Science Act and NSPM-33"

December 18, 2025

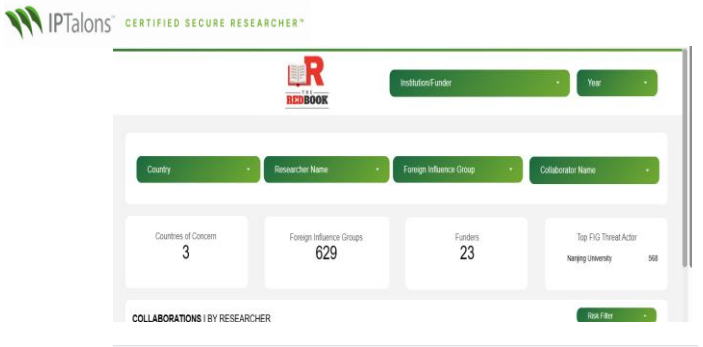
Data Verification Tools

Critical Requirement: Understand Your Researcher Foreign Influence Risks

- There are over **16,000** Foreign Influence Groups (FIGs) targeting your research programs via exploitation of research collaborations and funding.

- Data verification tools provide visibility into your research portfolio risks – and federal funding agencies are searching for unreported research collaborations.

- Do your federally funded researchers have a **Research Security Risk Mitigation Plan** (NSPM-33, CHIPS Act, and NDAA compliance)?



RISK MANAGEMENT

Risk Mitigation Plans

Managed Research Security Services

- Federal funding agencies are starting to requiring formal **Research Security Risk Mitigation Plan** as a condition of initial or renewed research project funding.
- **Risk Mitigation Plans** outline how the researcher and the research university plan to manage the foreign influence risks down to an acceptable level.
- **Audit teams** verify that researchers are complying with their risk mitigation plans.

Certified Secure Researcher™
RESEARCH SECURITY CERTIFICATION

https://certifiedsecurereseacher.com

- Adjudicates research security concerns at the researcher level
- Generates audit-ready Research Security Risk Mitigation Plans acceptable to federal funders

Research Security Program Audit Tool

- Minimal Viable Research Security Program (MV-RSP) is a baseline security control framework assessment tool to determine the research university's compliance readiness to meet NSPM-33 and CHIPS Act requirements.
- The audit team can use the results to identify the domains to scope their audit plan, based on perceived compliance gaps.
- There are five research security program domains included in the MV-RSP scoring that are weighted to achieve an overall research security program maturity risk score, leading to a Pass or Fail determination:
  - Communication and Integration
  - Policies and Procedures
  - Training Program
  - Information Protection and Research Data Safeguards
  - Audit

Research Security Program Audit Tool

RSP Domain	Total Available Points	Weighted Percentage
Communication and Integration	15	11%
Policies and Procedures	40	29%
Training Program	25	18%
Information Protection + Research Data Safeguards	40	29%
Audit	20	14%
MV-RSP Total Assessed Score	Point Range	Letter Grade
Pass	120 - 140	A
	100 - 119	B
Fail	80 - 99	C
	60 - 79	D
	0 - 59	F

- Minimal Viable Research Security Program (MV-RSP) tool is available to ACUA members and associates **free of charge**.
- Email: support@iptalons.com for a registration link and further details.

Questions?

Thanks for your attendance!

Let’s Stay Connected:

LinkedIn: https://www.linkedin.com/company/iptalons-inc/

Email me: allen.phelps@iptalons.com