TEXAS

The University of Texas at Austin

# Research Security

*Office of Vice President for Research, Scholarship and Creative Endeavors*

***August 2023***

**Office of Internal Audits**

*UT Austin's Agents of Change*

# Executive Summary

## Research Security

Office of Vice President for Research, Scholarship, and Creative Endeavors
Project Number: 22.009

## Audit Objective

This engagement was included on the Fiscal Year 2022 Annual Plan to assist The University of Texas at Austin (UT Austin) in preparing for the implementation of the National Security Presidential Memorandum (NSPM-33) requirements and creation of a formal research security program (RSP). This readiness review outlines enhancements that can be executed before final guidance is issued[1].

The objectives of this audit were to determine whether cybersecurity controls required by NSPM-33 are designed and operating effectively in federally-funded research spaces across campus, and to assess UT Austin policies and procedures for alignment with NSPM-33 research security program elements (i.e., foreign travel security, research security training, and export control training).

## Conclusion

UT Austin partially aligns with NSPM-33 implementation guidance for creating a research security program. Policies, training, processes, and controls are present across the University, but gaps exist that may require organizational changes and additional resources to address.

## Audit Observations[2]

| Recommendation | Risk Level | Estimated Implementation Date |
|---|---|---|
| Develop a Research Security Program | High | August 2024 |
| Develop RSP cybersecurity requirements that align with UT Austin's IT Strategy | High | August 2024 |
| Designate Point of Contact | Medium | September 2023 |

## Engagement Team[3]

Ms. Autumn Gray, CIA, Assistant Director
Ms. Suzi Nelson, CPA, CIA, CISA, Senior Auditor
Ms. Abby Simpson, Auditor II
Mr. Matthew Stewart, CISA, IT Audit Associate Director
Ms. Laura Walter, IT Audit Consultant

[1] The final guidance from the Office of Science & Technology is anticipated to be released later in 2023.
[2] Each observation has been ranked according to The University of Texas System Administration (UT System) Audit Risk Ranking guidelines. Please see the last page of the report for ranking definitions.
[3] This project was co-sourced with EAG Gulf Coast, LLC.

# Detailed Audit Results

The Office of the Vice President for Research, Scholarship and Creative Endeavors (OVPR) is committed to developing an investigator-focused infrastructure that supports the needs of UT Austin's diverse research enterprise. Prior to the publication of NSPM-33, OVPR hired an Associate Director of Science Security and developed a Science and Security Compliance Plan. OVPR also utilized the work of an Open Source Intelligence Analyst, a research security risk mitigation position in the Information Security Office (ISO). These efforts demonstrate proactive attention to identifying opportunities and engaging resources in a research security environment.

## Observation #1 Develop Research Security Program and Designate Point of Contact

UT Austin does not have a comprehensive research security program that incorporates cybersecurity, foreign travel security, research security training and export control training (the elements) as outlined in the NSPM-33 for federally-funded research. However, some policies, process owners, and internal controls are in place across campus to address portions of the required elements. Table 1 outlines the summarized research security program assessment results.

**Table 1 – RSP Assessment Results**

| RSP Element/Detail | Element Detailed Examples | Status |
|---|---|---|
| Cybersecurity | NSPM-33 Cybersecurity Protocols & Procedures | ░ |
| | Training | ▒ |
| | Specialized research Information Technology support | ▒ |
| Foreign Travel Security | Foreign travel security policies | ░ |
| | Organizational record of travel | ░ |
| | Foreign travel disclosure and authorization | ░ |
| | Foreign travel pre-registration requirement | ░ |
| | Foreign travel electronic devices assistance | ▓ |
| | Security briefings | ▒ |
| Research Security Training | Security threat-awareness/identification training | ▒ |
| | New trainings incorporated into existing training | ░ * |
| | Research security incident training | ▒ |
| Export Control Training | Export control training | ▒ |
| RSP Point of Contact | Designated, public point of contact for RSP | ▓ |
| RSP Description | Maintain description of RSP | ▓ |
| RSP Compliance | Certify compliance of RSP to federal agency | ▓ ** |

* Federal agencies are in the process of creating research security training that can be incorporated into existing training on responsible and ethical conduct. UT Austin provides access to this training through the Collaborative Institutional Training Initiative (CITI).

** Federal agencies are in the process of creating the certification procedures for institutional RSPs. UT Austin does not currently have an RSP, thus would not be able to certify compliance.

| | |
|---|---|
| ░ | Requirements generally met |
| ▒ | Requirements are not fully met but resources are available |
| ▓ | Requirements are not currently met |

As the federal[4] and State of Texas[5] research security regulatory environment evolves, the need to provide institutional support and structure will increase. Specifically, additional attention is being given to areas like Controlled Unclassified Information (CUI) and data management. Without a cohesive structure to manage risks and compliance requirements related to research security, UT Austin is only partially ready to implement NSPM-33 requirements and respond to the changing regulatory environment.

Peer universities across the country are preparing for NSPM-33 and addressing research security program requirements in varied ways. We benchmarked UT Austin's preparedness against peer institutions that will be subject to the same requirements. UT Austin is in line with peer institutions in preparing a research security program that aligns with NSPM-33 (See Table 2).

**Table 2 - Benchmarking Results: NSPM-33 RSP Preparation Assessment**

| | Peer Institutions | | | | | |
|---|---|---|---|---|---|---|
| **Institutional Responses †** | The Ohio State University<br>**$1,236.1 ‡** | University of Wisconsin-Madison<br>**$1,380.1** | University of Michigan<br>**$1,639.6** | UCLA<br>**$1,454.8** | UC Berkley<br>**$846.8** | UT Austin<br>**$779.3** |
| Reorganizing Offices/Reporting Lines | ✓ | | ✓ | | | * |
| Hiring Research Security Staff | ✓ | | ✓ | | | ✓ |
| Forming Governing Committees | ✓ | ✓ | | | ✓ | |
| Socializing Idea on Campus | ✓ | | | ✓ | | * |
| Waiting to Make Big Decisions | | ✓ | ✓ | ✓ | ✓ | ✓ |

† Institutional responses were adapted for this review from a National Council of University Research Administrators (NCURA) presentation titled *National Security Presidential Memorandum-33: Best Practices and Lessons Learned.*

‡ 2021 R&D expenditures in millions (Source: https://ncsesdata.nsf.gov/profiles/site?method=rankingbysource&ds=herd)

*On August 22,2023, OVPR indicated progress has been made in these categories.

The benchmarking results demonstrate that, overall, institutions are responding to the requirements by making changes in governance, staffing, and campus awareness education. These high-level changes are necessary prerequisites before addressing specific institutional research security program gaps. UT Austin will need to address these high-level areas before addressing the program gaps observed during this assessment. UT Austin's current program gaps include the following:

[4] For example, the CHIPS and Science Act is a U.S. federal statute that may extend NSPM-33 requirements.

[5]The Texas Legislature signed SB 1565 into law on June 18, 2023. This act requires that governing bodies of institutions of higher education establish a policy framework to address research security.

*Cybersecurity*

There were no significant issues or cybersecurity control deficiencies noted for the research labs reviewed during this audit. While these labs operate in a decentralized information technology (IT) environment, they leverage institutional IT controls that provide reasonable assurance that research data is secure and monitored. Institutional controls include device procurement/registration through Information Technology Services (ITS), connecting devices to the network to allow for ISO visibility and monitoring, and utilization of data storage in approved locations (e.g., Texas Advanced Computer Center, University Data Center, and UT Box). Principal Investigators (PIs) who engage with ITS or Colleges, Schools, and Units' (CSU) IT resources are typically in alignment with basic safeguarding protocols and procedures outlined in NSPM-33 and are better positioned to protect their data.

However, the decentralized IT environment on campus affects PIs in varying degrees. Quality and quantity of service deliveries can impact the research process and cause some PIs to troubleshoot cybersecurity, IT, and data issues on their own or with fragmented resource services across campus. For example, IT and cybersecurity support are not fully integrated into current award/contract processes; therefore, ITS and CSU IT are not always aware of PI needs. Consequently, PIs may need to manage IT risks, thereby increasing administrative burdens and potentially increasing risks. This situation impacts the cybersecurity environment, as is evidenced in the following themes observed during testing:

- Inconsistent training requirements and completion by undergraduate research assistants.
- PIs expressed a desire for a more consultative partnership with ITS and CSU IT resources on campus, and for them to consistently assist PIs as subject-matter experts.
- Graduate assistants are tasked with IT support roles and are not properly trained or aware of institutional ITS policies and procedures.
- Confidential Data Control Plans are not monitored for accuracy and reliability.
- Personal devices are used to conduct research, including the transfer of data to conduct analysis.
- Shared passwords are used for some devices in the labs.
- Labs have limited physical security controls/mechanisms in place.
- Some PIs do not view data as sensitive; therefore, they do not think it needs protection.
- PIs generally do not consider impacts of production loss (e.g., time spent recreating lost or corrupted data and analysis) or loss of intellectual capital (i.e., ideas are stolen by other researchers).

*Foreign Travel Security*

Researchers do not receive security briefings that include risk mitigation strategies for protecting IT and research data during travel – including assistance with electronic devices (e.g., smartphones, loaner laptops) as appropriate.

*Research Security Training*
UT Austin does not have a formal research security training program, including threat awareness/identification and insider threat training.

*Export Control Training*
Researchers are not required to attend export control training. Assistance and training are provided upon request.

*Research Security Point of Contact*
UT Austin has not identified a person who will serve as the point of contact for the University's research security program.

**Recommendations:**

1. Develop a cohesive research security program that incorporates cybersecurity, foreign travel security, research security training, and export control training (the elements) as outlined in NSPM-33. Address gaps to the required elements by enhancing policies, assigning process owners, and strengthening internal controls.

   *Policies*
   - Develop a research security policy that includes all elements of a research security program.
   - Update UT Austin's Office of Research Support and Compliance's (RSC) Science and Security Compliance Plan to incorporate additional NSPM-33 research security program requirements.
   - Develop policies and procedures that address specific "containers" of research (e.g., classified, CUI, public).

   *Process Owners*
   - Identify key stakeholders on campus and organize a committee and/or governing body to create a research security program.
     - Utilize internal and external resources to bolster the planning for and implementation of a research security program at UT Austin.
     - Outline plans to address research security program operation, maintenance, monitoring, and compliance certification steps.[6]
   - Identify a Research Security Officer and additional staff needed to manage and monitor a research security program.

   *Internal Controls*
   - Develop a PI risk profile matrix (e.g., high, medium, low) to holistically assess risks related to cybersecurity, foreign travel, research security, export controls, and other research-related risks (e.g., Conflict of Interest, data management plans, etc.). Use the risk profile to determine the level of outreach, review, and technical support needed for PIs.

[6] The federal government has not published final compliance certification procedures yet, but leadership should begin identifying the processes and metrics that are acceptable from a risk mitigation perspective.

- Coordinate with relevant departments (e.g., Texas Global, Travel Office, ISO, etc.) to increase awareness and provide resources/guidance to international travelers including:
  - Security briefings
  - Assistance with electronic devices (e.g., smartphones, loaner laptops)
  - Protecting data and equipment during travel
- Utilize and incorporate training resources provided by external sponsors (e.g., NSF, NIH) to address security risks associated with data, cybersecurity, IT, foreign entities, export controls, and research.
  - Require export control training for PIs (and research assistants) that are subject to that requirement.
  - Identify training needs during the creation and submission of the required Technology Control Plan.
  - Create training to address research security incidents and incorporate lessons learned.
- Require graduate and undergraduate research assistants involved in federally-funded research, who are considered covered individuals per NSPM-33, to complete appropriate trainings related to research security program elements.

2. Develop research security program cybersecurity requirements that align with UT Austin's IT Strategy.
   a. Coordinate efforts with campus IT leaders to align research security program cybersecurity requirements with IT Strategy.
   b. Partner with appropriate stakeholders within the new IT governance model to identify ways to address PI IT support needs.
   c. Integrate IT/cybersecurity support into the research support infrastructure to reduce PI administrative burden and help PIs manage risks.
   d. Review and monitor data/technology agreements (e.g., Technology Control Plans, Confidential Data Control Plans).

3. Identify a single point of contact for the research security program. To enhance the effectiveness of the program, this person should be knowledgeable of the elements, partner with campus stakeholders to mitigate program risks, and support compliance with NSPM-33.

**Management's Corrective Action Plan:**
OVPR acknowledges the need for establishment of a robust research security program which meets the requirements of NSPM-33 and other relevant legislation. We will use the recommendations as outlined above as our management action plan. We look forward to establishing a research security officer in the near term, and working to develop a structured program, backed by a new policy, with appropriate educational, training and engagement activities for the researcher community in the coming fiscal year. Likewise, OVPR looks forward to collaborating with ITS and ISO to ensure cybersecurity requirements are appropriately accounted for in the research security program.

**Responsible Person:**
Associate Vice President / Director, Research Support & Compliance
Chief Information Security Officer (Recommendation 2 only)
Assistant Vice President for Information Technology Services (Recommendation 2 only)

**Planned Implementation Date:**
Recommendation 1: August 2024
Recommendation 2: August 2024
Recommendation 3: September 2023

## Conclusion

UT Austin partially aligns with NSPM-33 implementation guidance for creating a research security program. While behind several peer institutions in terms of planning for and instituting a research security program, there are some policies, process owners, and controls in place to address and incorporate the elements of a research security program as identified in NSPM-33.

Establishing a cohesive research security program may require organizational changes and additional resources. However, it will allow UT Austin to address process gaps, provide comprehensive customer service to the research enterprise on campus, reduce administrative burden on PIs, and enhance research security.

**Table: Controls Assessment**

| Audit Objective | Controls Assessment |
|---|---|
| Objective 1. Determine whether cybersecurity controls required by NSPM-33 are designed and operating effectively in federally-funded research spaces across campus. | Satisfactory with Medium Risk Opportunity |
| Objective 2. Assess UT Austin policies and procedures for alignment with NSPM-33 research security program elements (i.e., foreign travel security, research security training, export control training). | Partial Alignment with High Risk Opportunity |

## Background

In January 2021, NSPM-33 directed a national response to safeguard the security and integrity of federally-funded research. Research institutions that receive federal science and engineering support in excess of $50 million per year must establish, operate, and certify a research security program. Implementation guidance for this directive was subsequently published by the National Science and Technology Council's (NSTC) Joint Committee on the Research Environment (JCORE) in January 2022. While federal agencies, including the National Science Foundation (NSF) and National Institutes of Health (NIH), are still in the process of developing additional instructions and training to assist research organizations, many institutions have begun planning for the five key areas addressed in the memorandum:

- Disclosure Requirements and Standardization
- Digital Persistent Identifiers
- Consequences for Violation of Disclosure Requirements
- Information Sharing
- Research Security Programs

In Fiscal Year 2022, NSF awarded UT Austin $110.5 million[7], and in Fiscal Year 2020, UT Austin ranked first in NSF research expenditures, totaling more than $144 million[8].

Throughout this assessment, we considered the decentralized operating environment, diverse needs of the research community, and efforts to reduce PI administrative burdens. Risks vary significantly across UT Austin's vast research enterprise, and this assessment does not attempt to cover all campus research-related risks. Instead, this review covers a smaller population of campus research (i.e., NSF and NIH awards). NSPM-33 provides institutions flexibility in applying research security programs in a manner to address their diverse research communities and operating environments. Although the detailed audit results are attributable to a sample population, lessons learned during the engagement can be considered for the larger research population to optimize research security at UT Austin and serve the research enterprise holistically.

## Scope, Objectives, and Methodology

This audit was conducted in conformance with The Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing*. Additionally, we conducted the audit in accordance with Generally Accepted Government Auditing Standards and meet the independence requirements for internal auditors. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions on our audit objectives.

The scope of this review includes active NSF- and NIH-funded research in fiscal year 2023.

Specific audit objectives and the methodology to achieve the objectives are outlined in the table below.

[7] Source: https://dellweb.bfa.nsf.gov/AwdLst2/default.asp

[8] Source: https://news.utexas.edu/2022/01/18/ut-austin-no-1-in-nsf-funding-in-united-states/ and https://ncses.nsf.gov/pubs/nsf22311/table/63

**Table: Objectives and Methodology**

| Audit Objective | Methodology |
|---|---|
| Objective 1. Determine whether cybersecurity controls required by NSPM-33 are designed and operating effectively in federally-funded research spaces across campus. | • Interviewed a sample of ten PIs within the defined scope<br>• Interviewed IT support staff for the sampled PIs respective CSUs<br>• Reviewed award documentation and relevant terms, conditions, and policies<br>• Examined labs and IT equipment set-ups<br>• Assessed status of relevant cybersecurity controls within sampled labs |
| Objective 2. Assess UT Austin policies and procedures for alignment with NSPM-33 research security program elements (i.e., foreign travel security, research security training, export control training). | • Reviewed relevant policies<br>• Interviewed personnel in each research security program element area<br>• Reviewed select peer institutions' related policies and procedures<br>• Interviewed individuals from peer institutions<br>• Compared UT Austin to select peer institutions' approach to NSPM-33 |

## Criteria

- National Security Presidential Memorandum 33 (NSPM-33) Section 4(g)
- Guidance for Implementing National Security Presidential Memorandum 33 (NSPM-33) on National Security Strategy for United States Government-Supported Research and Development

## Observation Risk Ranking

Audit observations are ranked according to the following definitions, consistent with UT System Audit Office guidance.

| Risk Level | Definition |
|---|---|
| Priority | If not addressed immediately, has a high probability to directly impact achievement of a strategic or important operational objective of UT Austin or the UT System as a whole. |
| High | Considered to have a medium to high probability of adverse effects to UT Austin either as a whole or to a significant college/school/unit level. |
| Medium | Considered to have a low to medium probability of adverse effects to UT Austin either as a whole or to a college/school/unit level. |
| Low | Considered to have minimal probability of adverse effects to UT Austin either as a whole or to a college/school/unit level. |

In accordance with directives from UT System Board of Regents, Internal Audits will perform follow-up procedures to confirm that audit recommendations have been implemented.

## Report Submission

We appreciate the courtesies and cooperation extended throughout the audit.

Respectfully Submitted,

Sandy Sutton Jansen

Sandy Jansen, CIA, CCSA, CRMA, Chief Audit Executive

## Distribution

Dr. Jay C. Hartzell, President
Mr. Cameron Beasley, Chief Information Security Officer
Mr. Mark Featherston, Chief of Staff, Office of the Vice President for Research, Scholarship and Creative Endeavors
Mr. Jeffery Graves, Chief Compliance Officer, University Risk and Compliance Services
Ms. Monica Horvat, Director Presidential Priorities
Mr. Trice Humpert, Assistant Vice President for Information Technology Services
Dr. Daniel Jaffe, Vice President for Research
Mr. Jeff Neyland, Chief Strategist for IT Transformation
Dr. Catherine Stacy, Chief of Staff, Office of the Executive VP & Provost
Dr. Daniel Slesnick, Interim Vice President and Chief Financial Officer
Dr. Michelle Stickler, Associate Vice President, Office of Research Support & Compliance
Dr. Sharon Wood, Executive Vice President and Provost

The University of Texas at Austin Institutional Audit Committee
The University of Texas System Audit Office
Legislative Budget Board
Governor’s Office
State Auditor’s Office