Research Security Update 2026

Saul Sotolongo, JD, ECoP®(ITAR/EAR)
Director of Research Security and COI

UNIVERSITY OF NORTH CAROLINA
CHARLOTTE

Objectives

1. **Define research security and why it matters**
2. **Review new federal requirements (NIH, NSF, DOE, USDA)**
3. **Identify who must complete training and when**
4. **Review disclosure updates for PIs**
5. **Introduce research security data requirements**
6. **Share UNC Charlotte’s next steps and checklist**

What is Research Security?

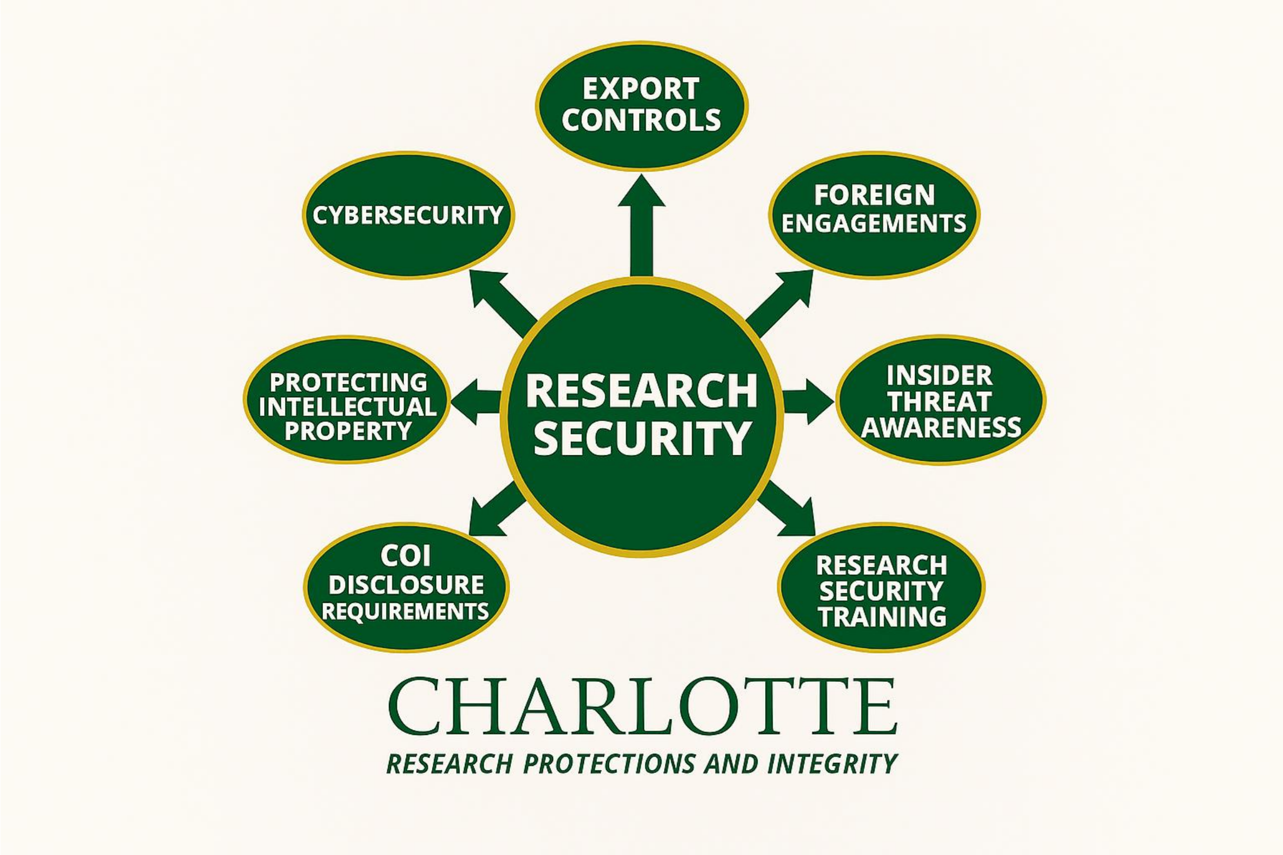
More than just cybersecurity

Goal: Preserve research integrity while enabling global engagement.

- Protecting UNC Charlotte’s research enterprise from misuse or foreign interference
- Safeguarding the data you generate and intellectual property you create
- Promoting transparency and compliance to maintain funding eligibility

On our website: [UNC Charlotte Research Security]()

[NATIONAL SECURITY PRESIDENTIAL MEMORANDUM – 33 - Jan 14, 2021]()


RESEARCH SECURITY
EXPORT CONTROLS
FOREIGN ENGAGEMENTS
INSIDER THREAT AWARENESS
RESEARCH SECURITY TRAINING
COI DISCLOSURE REQUIREMENTS
PROTECTING INTELLECTUAL PROPERTY
CYBERSECURITY
CHARLOTTE
RESEARCH PROTECTIONS AND INTEGRITY

The Regulatory Driver

NSPM-33 - *Jan 14, 2021*

National Security Presidential Memorandum 33 requires research institutions receiving over $50M in federal science support to operate a certified research security program.

CHIPS & SCIENCE ACT - *Codified into Law*

Codified many NSPM-33 requirements. Specifically prohibits participation in Malign Foreign Talent Recruitment Programs (MFTRP). Violation leads to

UNIVERSITY OF NORTH CAROLINA CHARLOTTE

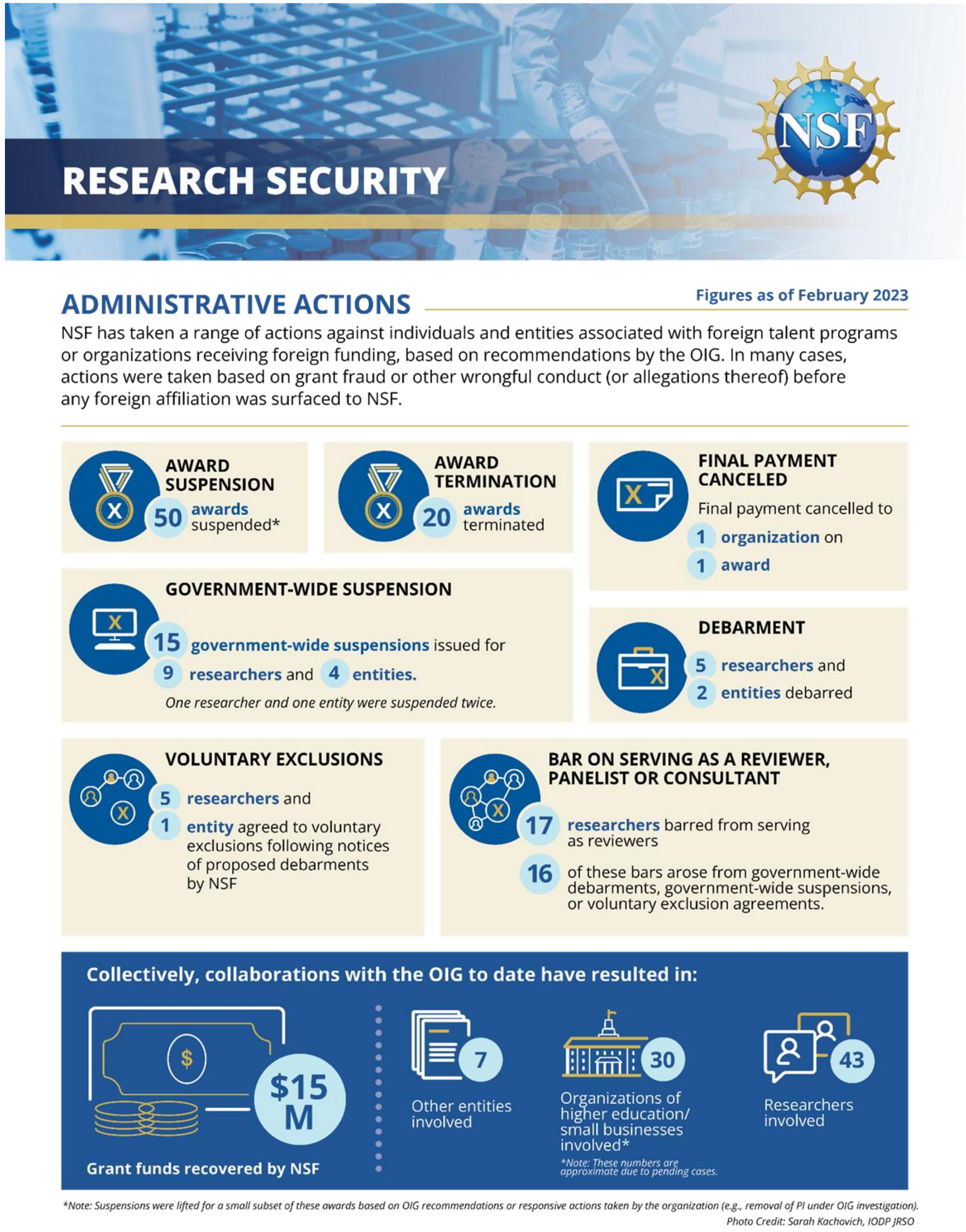
Why it matters now

From Advising to Enforcing

Federal agencies are raising expectations with new training certifications and increased audits. The risks include ineligible proposals and funding suspensions.

Protecting You

These regulations are designed to prevent the theft of your intellectual property and research data before you are ready to publish. Accurate disclosures protect your reputation and ensure you retain credit for your work.



RESEARCH SECURITY

NSF

ADMINISTRATIVE ACTIONS

Figures as of February 2023

NSF has taken a range of actions against individuals and entities associated with foreign talent programs or organizations receiving foreign funding, based on recommendations by the OIG. In many cases, actions were taken based on grant fraud or other wrongful conduct (or allegations thereof) before any foreign affiliation was surfaced to NSF.

AWARD SUSPENSION
50 awards suspended*

AWARD TERMINATION
20 awards terminated

FINAL PAYMENT CANCELED
Final payment cancelled to
1 organization on
1 award

GOVERNMENT-WIDE SUSPENSION
15 government-wide suspensions issued for
9 researchers and 4 entities.
One researcher and one entity were suspended twice.

DEBARMENT
5 researchers and
2 entities debarred

VOLUNTARY EXCLUSIONS
5 researchers and
1 entity agreed to voluntary exclusions following notices of proposed debarments by NSF

BAR ON SERVING AS A REVIEWER, PANELIST OR CONSULTANT
17 researchers barred from serving as reviewers
16 of these bars arose from government-wide debarments, government-wide suspensions, or voluntary exclusion agreements.

Collectively, collaborations with the OIG to date have resulted in:

$15 M
Grant funds recovered by NSF

7
Other entities involved

30
Organizations of higher education/ small businesses involved*
**Note: These numbers are approximate due to pending cases.*

43
Researchers involved

**Note: Suspensions were lifted for a small subset of these awards based on OIG recommendations or responsive actions taken by the organization (e.g., removal of PI under OIG investigation).*

Photo Credit: Sarah Kachovich, IODP JRSO

Recent Agency Updates

May 1, 2025

DOE
Research Security
Training

July 8, 2025

USDA
Research Security
Training

Oct 10, 2025

NSF
Research Security
Training

Jan 25, 2026

NIH
'Other Support'
Common Form

National Institute of Dental
and Craniofacial Research

MALIGN FOREIGN TALENT RECRUITMENT PROGRAMS

STRICTLY PROHIBITED

Programs sponsored by a foreign country of concern that compensate individuals in exchange for transferring knowledge or IP are banned for all federally funded researchers.

Who must be trained

- **Required: PIs, Co-PIs, Senior/Key Personnel**
- **Recommended: Other staff on federally funded projects**
- **Timing: Within 12 months of proposal submission or renewal**
- **UNC Charlotte will provide approved training and record completions centrally**

Training Timeline

Prior to Proposal

Many agencies require certification of training completion before submission of a proposal.

Annually

NSPM-33 guidance suggests an annual refresher to keep up with evolving threats.

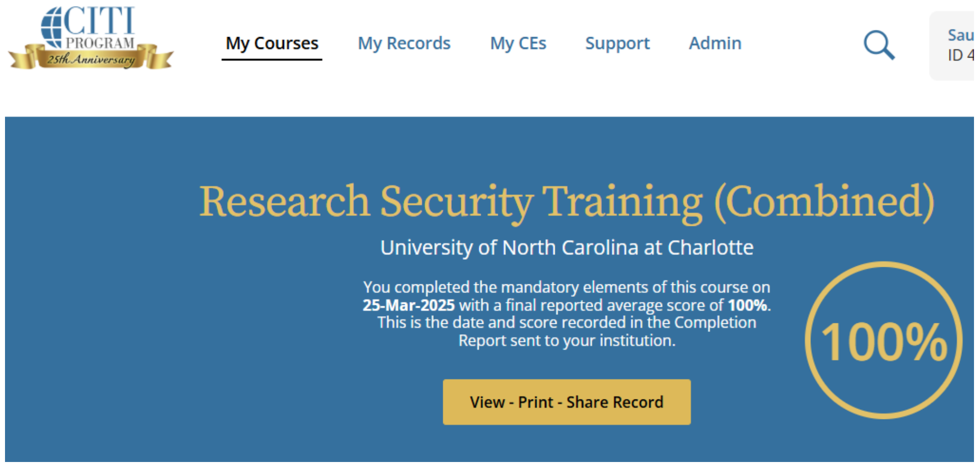
Within 30 Days

New personnel added to a project must complete training within 30 days of joining.

Training Content

1. Research security awareness & foreign influence prevention
2. Disclosure and 'Other Support'
3. Cybersecurity and data protection
4. Export control awareness
5. Safe international collaboration and travel

CITI PROGRAM



Research Security Training (Combined)

University of North Carolina at Charlotte

You completed the mandatory elements of this course on **25-Mar-2025** with a final reported average score of **100%**. This is the date and score recorded in the Completion Report sent to your institution.

Link: [Instructions: CITI Research Security Training]()

What is Foreign Influence Prevention?

- Foreign Influence = Efforts to divert or misuse U.S.-funded research
- Examples: Undisclosed foreign appointments, unauthorized data sharing, dual affiliations
- Prevent by: Full disclosure of all support, affiliations, and collaborations

REQUEST AN INTERNATIONAL ENGAGEMENT REVIEW

On our Website: Foreign Talent Recruitment Programs, Insider Threats

Insider Threat Awareness

What is an Insider Threat?

A threat that comes from within the organization, such as a researcher, student, or staff member who has authorized access but misuses it to harm the university or national security.

Behavioral Indicators

- Working unusual hours without a research justification.
- Attempting to access sensitive data unrelated to their specific project.
- Unreported foreign travel or unexplained affluence.
- Downloading large volumes of data to removable media (USBs).

The 3 Buckets Of Disclosure

CONFLICT OF INTEREST (COI)

Financial Focus: Consulting fees, equity, royalties, or ownership interests that could bias research.

CONFLICT OF COMMITMENT

Time Focus: Outside employment, appointments, or obligations that interfere with university duties.

OTHER SUPPORT

Resource Focus: All resources available for research, domestic or foreign, monetary or in-kind.

COI & Other Support Updates

- NIH NOT-OD-25-133 (July 17, 2025): institutions must provide training to Senior/Key Personnel on Other Support disclosure obligations; effective January 25, 2025.
- Other Support = all resources (financial and in-kind) supporting researcher’s research endeavors (active & pending) - broad scope.
- FCOI (PHS 42 CFR Part 50 Subpart F) remains core: report & manage significant financial interests; institutions must have policies and training.

On our Website: Conflict of Interest

DON'T FORGET "IN-KIND"

Many PIs miss non-monetary support. You must disclose:

- Visiting scholars funded by their home institution/government.
- Students or postdocs supported by external foreign fellowships.
- Access to high-value lab equipment or datasets provided by a foreign entity.
- Honorary titles at foreign universities.

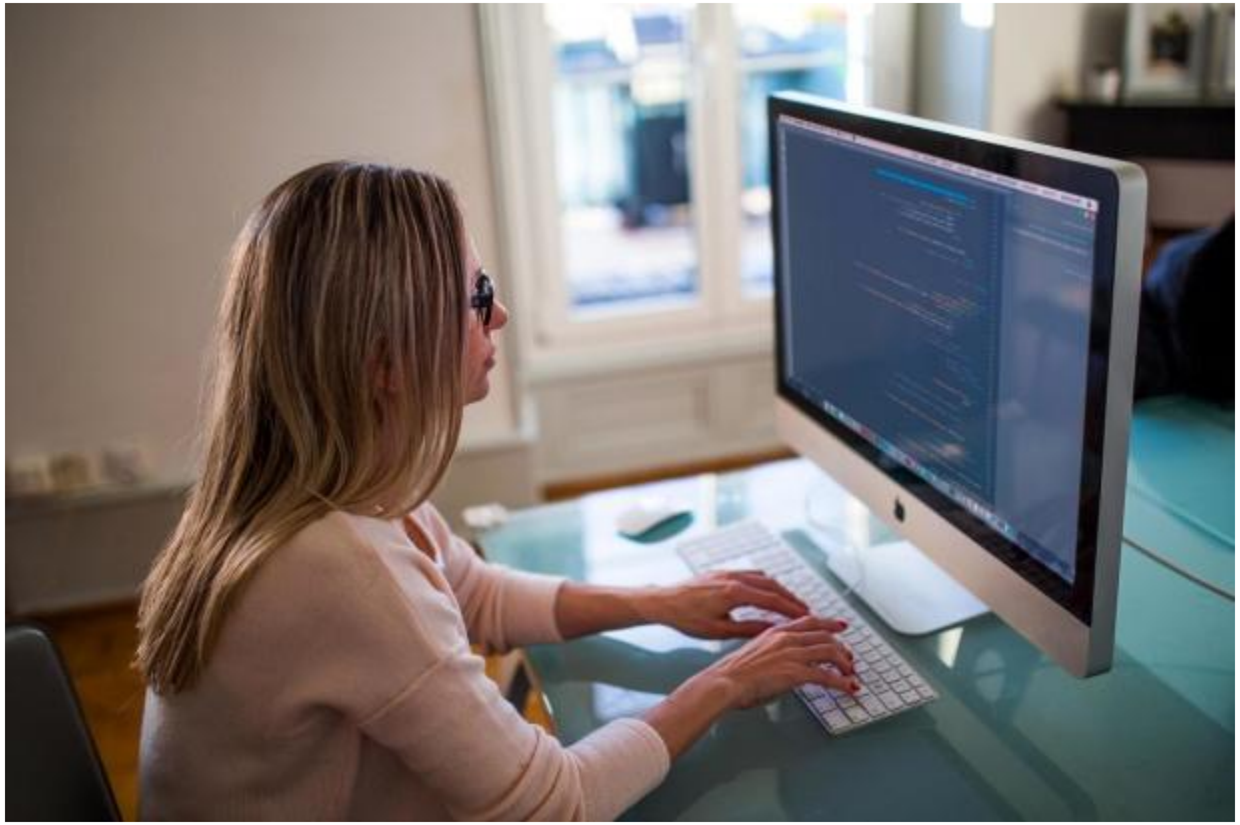
COI Update Triggers

THE 30-DAY RULE

You cannot wait for the annual disclosure cycle. You must update your COI disclosure within **30 days** of acquiring a new significant financial interest.

SPONSORED TRAVEL

Travel paid for by external entities (excluding US gov/universities) often requires disclosure.



NIH Data Security Requirements Update

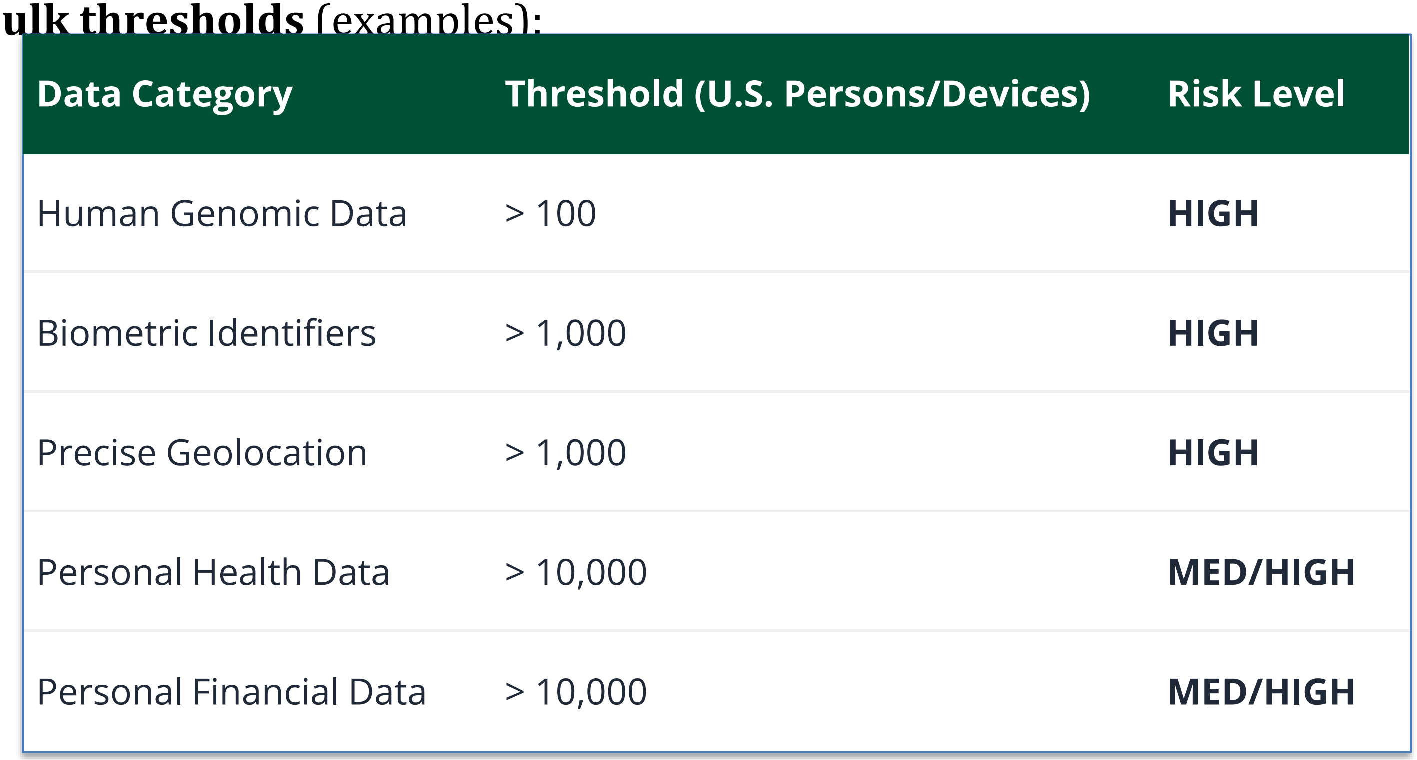
National Institutes of Health

NIH - Genomic Data Sharing (GDS) Policy

- Access to **controlled-access human genomic data** requires approval by an NIH **Data Access Committee (DAC)**.
- Users must agree to NIH **Data Use Certification** and **Genomic Data User Code of Conduct**.
- Systems used to store, process, or analyze controlled-access genomic data must comply with **NIST SP 800-171** security controls, as specified in NIH security best practices.
- Security compliance is **attested by the user/institution** and applies specifically to controlled-access data.

DOJ – National Security Division Data Security Program Update

- Regulates foreign access to **“bulk sensitive personal data”** of U.S. persons.
- **Bulk thresholds** (examples):



Data Category	Threshold (U.S. Persons/Devices)	Risk Level
Human Genomic Data	> 100	**HIGH**
Biometric Identifiers	> 1,000	**HIGH**
Precise Geolocation	> 1,000	**HIGH**
Personal Health Data	> 10,000	**MED/HIGH**
Personal Financial Data	> 10,000	**MED/HIGH**

- Transfers meeting these thresholds to **countries of concern*** or **covered persons** are regulated.
- Thresholds determine when data is treated as **“bulk”**; rules apply based on **recipient and destination**, not all transfers.

***Countries of Concern**: *China, Russia, Iran, North Korea, & Cuba. Transfers above these thresholds to these countries are restricted or prohibited.*

UNC Charlotte Research Faculty & Staff Checklist

- ✅ Complete required training (CITI module)
- ✅ Update Other Support & COI disclosures
- ✅ Review collaborators for export control flags
- ✅ Consult before international travel or visiting scholars
- ✅ Contact Research Security for any questions

Before engaging in international activity fill out this form International Engagement Questionnaire

Contacts

For inquiries or assistance regarding:

Research Security: Saul Sotolongo, Director of Research Security and COI at 704-687-1878

Export Control: Lacy Kitchin, Export Control Officer at 704-687-1877

Conflict of Interest: Sherry Loyd, Conflict of Interest Officer at 704-687-8270, or Jennifer Lewis, Sr. Research Integrity Administrator at 704-687-0688

Research Data Security: Kendra Raynor, Research Data Compliance Coordinator at 704-687-1357

UNIVERSITY OF NORTH CAROLINA CHARLOTTE