NSF SECURE Center Research Security Briefing

Vol. 1 No. 14: October 2, 2025

The SECURE Center distributes research security briefings and timely alerts **via** *its listserv. The Briefing provides a centralized resource for research security-related information, including new statutory and research funding agency requirements, new or updated federal and community resources, and significant news items and scholarly works. The Center will also assess and provide commentary, interpretation, or implementation considerations on new requirements, notices and resources, working with higher education associations, legal partners, or agencies as needed.*

Contents

Federal Agency News & Updates

Update: NIH Rescinds Notice on Implementation of Research Security Policies

In a September 29, 2025, notice (NOT-OD-25-161), the National Institutes of Health (NIH) rescinded the September 11, 2025, notice (NOT-OD-25-154) *Implementation of NIH Research Security Policies*. Per the notice, "NIH continues to work with the National Science Foundation and other Federal research agencies to finalize guidance on each of the required elements outlined in the Office of Science and Technology Policy (OSTP) *Guidelines for Research Security Programs at Covered Institutions*, and to develop a centralized process for recipients to certify compliance." The notice indicates that the implementation date for the requirements announced in NOT-OD-25-154 have not been finalized, the notice is therefore rescinded, and that "NIH will issue updated guidance on Research Security requirements in the coming months."

Required Security and Operational Standards for NIH Controlled-Access Data Repositories Notice Number: NOT-OD-25-159

On September 24, 2025, and effective immediately, NIH issued NOT-OD-25-159, establishing new security, operational, and transparency standards for controlled-access data repositories (CADRs) that store and manage sensitive human research data.

Key Points:

- Applies to NIH-funded repositories that manage long-term access to human participant data.
- Requires compliance with a new CADR Guidebook outlining data access, submission, and security protocols.
- Implementation deadlines:
    - **Now:** Registration and initial compliance steps.
    - **By Nov 1, 2025:** Document policies and access procedures.
    - **By Feb 25, 2026:** Full implementation of all standards.
- Noncompliant repositories may have to transfer data elsewhere.

This policy is intended to align with federal efforts to protect sensitive data from misuse, especially by foreign adversaries.

NIH Policy on Enhancing Security Measures for Human Biospecimens (NOT-OD-25-160)

Issued September 24, 2025, and effective October 24, 2025, NIH is implementing NOT-OD-25-160, a policy to enhance security for human biospecimens in NIH-funded research.

Key Points:

- Prohibits sharing NIH-funded human biospecimens with institutions in "countries of concern" as

determined under 28 CFR § 202.601 (i.e., China, Cuba, Iran, North Korea, Russia, and Venezuela)

- Exceptions allowed only in limited cases (e.g., legal obligations, unique expertise, or donor request), with documentation.
- Applies to all NIH-funded activities involving human biospecimens from U.S. persons.
- Does not apply to biospecimens already publicly or commercially available before the effective date.
- Must comply with U.S. export laws and recordkeeping requirements.

This policy is intended to protect human participants' "sensitive and personal health-related data from foreign adversary misuse," and to enhance U.S. security interests.

OMB and OSTP Fiscal Year (FY) 2027 Administration Research and Development Budget Priorities and Cross-Cutting Actions

On September 23, 2025, a memorandum was issued to the heads of executive departments and agencies from Russell Vought, Director of the Office of Management and Budget (OMB), and Michael Kratsios, Director of the Office of Science and Technology (OSTP). The memorandum lists five research and development budgetary priorities along with five high-priority, cross-cutting actions, including the implementation of Gold Standard Science as detailed in the OSTP memorandum from June 23, 2025, with an emphasis on innovation while maintaining research security. (more)

New NIH Application and Award Structure for NIH-Funded International Collaborations (Replacing Foreign Subawards)

On September 18, 2025, NIH released additional information regarding the agency's new application and award structure for international collaborations, previously announced on September 18, 2025 in NIH NOT-OD-25-155 (also see SECURE Briefing No. 12). In addition to summarizing impacts to proposing/recipient institutions, the announcement provides links to additional information for the four new Activity Codes (grant types) that will be used to facilitate the new application and award process:

- PF5: Collaborative International Research Project (awarded directly to domestic organization)
- UF5: Cooperative Agreement Equivalent
- RF2: Linked International Research Project (awarded directly to the foreign organization)
- UL2: Cooperative Agreement Equivalent

Professional Association Resources & Meeting Reports

Request for Community Feedback on Draft Cybersecurity Guidelines for Research Security Programs

Members of the Federal Demonstration Partnership (FDP) and EDUCAUSE Cybersecurity Guidelines and Demonstration Working Groups are requesting feedback from institutions on draft cybersecurity guidelines developed as part of an FDP demonstration project involving federal and institutional representatives. Intended recipients include the institution's or organization's Chief Information Security Officer and staff, research security lead, regulated data/information security staff, and other institutional stakeholders, as appropriate. Return of the draft as one single set of comments from each institution is requested by EOD Tuesday, October 21. The draft cybersecurity guidelines can be accessed for download and comment here. They should be submitted to ResearchSecurity@thefdp.org.

Consistent with National Security Presidential Memorandum-33 and the July 2024 White House Office of Science and Technology Policy-issued final research security program guidelines, agencies will be rolling out research security program requirements that include cybersecurity. To establish cybersecurity guidelines, federal agencies, including NSF, DOD, DOE, and the NIST developers of IR 8481 are working with the FDP Research Security Subcommittee, EDUCAUSE, other FDP committee and subcommittee chairs, higher education associations (e.g., Association of Public and Land-grant Universities, COGR), and other partners representing a spectrum of institution types to develop the desired guidelines through an FDP demonstration. Research funding agencies will ultimately put forward the requirements for research security programs to which institutions need to certify, including the research cybersecurity guidelines.

Comments will further inform the draft guidelines, with modifications made in response to community feedback. Individual institution/organization feedback will not be shared. An overview of comments in the aggregate may be shared to keep the community informed.

Reimagining Strategies for High-Impact International Collaborations

The University Industry Demonstration Partnership (UIDP) held a panel discussion on *Reimagining Strategies for High-Impact International Collaborations* at its annual meeting in Chicago, September 16-18, 2025. Launched in 2006, the UIDP is designed to enhance the value of collaborative partnerships between universities and industry in the United States. Panel speakers included: Husameddin Saleh Al-madani, King Fahd University of Petroleum and Minerals; Amanda Ferguson, Huron Consulting Group; Shakirah Akinwale, University College London; and Lisa Nichols, University of Notre Dame and SECURE Center. Following brief opening presentations, university and industry participants engaged in a discussion on collaboration dynamics, cultural and organizational considerations, operational and compliance challenges, case studies and examples, and the policy and security environment.

In terms of university engagement with industry, there was discussion on starting small and

developing relationships, including seed funding and fostering student engagement. There was discussion about student and research timelines being different across countries. Participants noted that in India students can complete three-month projects referred to as sprints. Projects may even be six-to-twelve weeks in duration.

In terms of the current geopolitical environment and engagement between universities and industry, a few topic areas surfaced. Disparities in funding, reductions in funding, and higher costs in the U.S. were raised, and the potential rethinking of cost models. The current unpredictability in the U.S. research environment was further noted, as well as different cost structures and intellectual property roles across countries. There was discussion of this leading to a reduction in engagement with U.S. institutions. It was noted that Europe is contributing funding that allows for industry engagement with academia, but at a lower cost to industry.

Updated COGR Research Security Resources

On September 30, 2025, COGR released updated versions of its "Matrix of Science & Security Laws, Regulations, and Policies" and "Quick Reference Table of Current & Upcoming Federal Research Security Requirements." Notably, the latest versions incorporate requirements outlined in:

- USDA's July 8, 2025 "America First Memorandum for USDA Arrangements and Research Security"
- NSF Important Notice 149 (July 10, 2025)
- NIH's 9/25/2025 notice, NOT-OD-25-161, rescinding the research security-related certification requirements previously released in NOT-OD-25-154 (also see above)

COGR Forum: Adapting to Change, Policy Shifts & Research Impact

As part of its ongoing series, the first hour of this month's COGR forum (held 9/30/2025) focused on research security. A brief poll on research security training implementation was conducted and results will be shared on the COGR website. COGR presented two slides detailing the research security landscape across multiple federal agencies over the past year, noting some documents are under revision or need additional clarification:

- DOE FAL 2025-02
- DOE FAL 2024-05
- DARPA/DOD Component Decision Matrix
- USDA Secretary's Memorandum 1078-014
- NSF Important Notice No. 149
- NIH Notice NOT-OD-25-133
- NIH Notice NOT-OD-25-154 (rescinded by NIH NOT-OD-25-161)

All of these federal notices or requirements can also be accessed through COGR's "Quick Reference Table of Current & Upcoming Federal Research Security Requirements," above.

COGR asked representatives from three universities to present on their current approach to implementation of NIH and other agencies' Research Security requirements:

- Carrie Kroll McMullan, Assoc. General Counsel and Deputy Chief Compliance Officer for International Activities, Johns Hopkins University (JHU)
- Deborah Motton, Executive Director Research Policy Analysis and Coordination, University of California System, Office of the President (UC)
- Lori Ann Shultz, Assoc. Vice President for Research, Colorado State University (CSU)

The pressing topics covered by all presenters focused on several key areas: their approach to Other Support training, whether a new Other Support policy was needed or already covered in the institution's existing policy; and how they were approaching research security training (given NIH's Notice NOT-OD-25-161 was issued the day before) along with other agencies' requirements.

Other Support training, NIH Notice NOT-OD-25-133:

- UC noted their need to "pivot" a bit on their homegrown system for research security training and added some clarifying Other Support disclosure information over the summer. UC noted a willingness to allow other institutions to adapt their research security training; an email request should be sent directly to Deborah.motton@ucop.edu.
- Johns Hopkins indicated they had started requiring the SECURE Condensed Training Module (CTM), downloaded into their Learning Management System (LMS), in advance of the May 1, 2025, Department of Energy (DOE) deadline, with confirmation occurring over summer 2025. Disclosure training information is embedded within the SECURE CTM.
- CSU indicated they have initiated an October 1, 2025 deadline for research security training completion, utilizing the SECURE CTM, accessed through CITI Program.

Other Support "Policy," NIH Notice NOT-OD-25-133:

- UC conducted an analysis to confirm that their existing policies met the criteria for the NIH notice through a combination of Academic Personnel Polices and the Contracts & Grants Manual.
- JHU has taken a holistic approach to confirm their policies over the course of the past year; its current policies appropriately address the NIH notice.
- CSU made the decision to create a new generalized Other Support disclosure policy that is currently under final review and will be issued shortly.

Research Security Training:

All three universities already require research security training for senior/key personnel in accordance with, or in anticipation of, DOE, USDA and NSF requirements. All indicated that, with the issuance of NIH Notice NOT-OD-25-161, their institutions are watching for additional guidance on this topic from NIH.

All three universities also confirmed the need to:

- Track this information at the sponsored program/pre-award office,

- Make decisions at the institutional level as to whether a proposal, JIT, or RPPR would be stopped from submission—which may be dependent on the specific federal sponsor,
- Track subrecipient information.

U.S. Congressional Activity

US House Select Committee on the CCP Releases Report, "From PhD to PLA"

Following investigations into six US institutions, on September 19, 2025, the U.S. House of Representatives Select Committee on the Strategic Competition between the United States and the Chinese Communist Party (CCP) released the report "From PhD to PLA." The report states that US universities are admitting "thousands of Chinese nationals with academic ties to the Chinese military and defense industrial base annually" and "channeling talent and cutting-edge research directly to the Chinese government." To address these concerns, the Select Committee suggests:

- Strengthening visa screening laws to "deny access to sensitive U.S. research and substantially reduce technology transfer risks,"
- Denying visas to applicants "affiliated with the PRC defense research and industrial base," participating in PRC talent recruitment programs, or programs supported by the Chinese Scholarship Council,
- Requiring "interagency national security review—led by DOD, DHS, and FBI—for all graduate student visa applications involving controlled fields or technologies,"
- Prohibiting "foreign adversary nationals affiliated with U.S. government blacklisted entities from participating in federally funded research projects," and
- Requiring "U.S. universities to submit regular reports to the federal government on foreign adversary country student affiliations, funding sources, and updates to research roles, and areas of study, to include major or intended major."

Research Security News & Reports

Please note, articles linked below may require a subscription to view.
NSF SECURE Center cannot distribute copies of subscription-based articles.

Iran's S&T Ecosystem: A Primer for Research Security Professionals, Advisory #2

(NSF Secure Analytics, September 2025)

The NSF Secure Analytics team has published its latest Advisory: an in-depth look at research relationships with Iran. The science and technology (S&T) ecosystem of the Islamic Republic of Iran (IRI) prioritizes research with defense applications, state control of research institutions, and circumvention of export controls and sanctions. Drawing on government documents and bibliometric datasets, this advisory provides a high-level overview of key features of that ecosystem, enhancing

situational awareness of potential research security risks for the US research community.

Key Takeaways:

- The US is the top international research partner of the Islamic Republic of Iran (IRI), as measured by the annual number of coauthored publications. From 2015 to 2024, that figure increased more than 250%, rising from 2,051 to 5,153 publications.
- These publications include IRI-based coauthors on US government sanctions lists. Some of the research in these publications received support from US funding agencies.
- Certain IRI academic institutions are directly affiliated with military or security organizations and align closely with the science and technology priorities of those organizations. They practice strict admissions and background screening, which favors students and faculty supportive of the regime.
- Civilian academics and university labs participate in military- and security-related S&T projects, often subtly embedding that work within their broader research portfolios and serving as the international face of these efforts.
- IRI military and security forces, along with their affiliated institutions, have been directly involved in coordinated cyberattacks on universities worldwide. In one notable case, hundreds of American universities were targeted over the course of 2013–2017.
- The IRI's arbitrary detention of visiting researchers, as well as its use of science and technology to suppress society, including through digital surveillance and internet censorship, raise serious concerns around human rights and duty of care.

The full report offers an extensive analysis useful to research security professionals tasked with assessing any research relationships. (more)

Two-thirds of CISA personnel could be sent home under shutdown (Cyberscoop, 9/30/2025)

Cyberscoop reports that, per a Department of Homeland Security document, nearly two-thirds of Cybersecurity and Infrastructure Security Agency (CISA) personnel could be sent home due to the federal government shutdown. This means 889 of CISA's 2,540 personnel would continue working. Additional details compare these numbers to previous federal shutdowns. The article also emphasizes that two major cybersecurity laws, one providing legal protections for cyber threat data sharing and another providing state and local grants, are set to expire shortly. (more)

University of Arizona Shutters Chinese Microcampuses (Inside Higher Ed, 9/26/2025)

"The University of Arizona is quietly shutting down its four microcampuses in China at the end of this semester, in response to a government report released earlier this month that criticizes branch campuses of U.S. institutions in China." (more)

Pulling Back the Curtain on China's Military-Civil Fusion

Center for Security and Emerging Technology (CSET), Georgetown University, September 2025

Cole McFaul, Sam Bresnick, and Daniel Chou from CSET provide an in-depth analysis of the growing intersection in China of the military and civilian entities, such as research institutions, and the leveraging of Artificial Intelligence (AI) information to create dual-use products, both civilian and military. The analysis explores the balance between preserving the openness essential for innovation while mitigating risks and protecting United States research. CSET is a policy research organization within Georgetown University's Walsh School of Foreign Service that provides data-driven analysis on the security implications of emerging technologies. (more)

International Research Security Policy & Resources

Research Security Blooms in South America

Glenn Tiffert, PhD, Distinguished Research Fellow; Co-Chair, Program on the US, China, and the World; Hoover Institution | Stanford University and Member of the SECURE Center Staff

For many in South America, research security is a novel concept, but the University of São Paulo (USP) in Brazil is working energetically to change that mindset. In 2023, USP established an Office of Research Integrity and Protection that seeks to identify risks and opportunities in research partnerships, assess alignment between the university and its partners, promote healthy relationships between researchers and external stakeholders, and ensure transparency. Notably, the spark came not from any governmental mandate, but rather from a recognition within the university itself of the core academic values at stake in research security, the university's position as a vital nexus for the tangible and intangible assets that fuel Brazil's knowledge economy, and a desire to participate in a global research security community populated by many of the university's key international partners.

What happens at USP carries weight across the region; USP is often ranked as South America's leading research university and it anchors the continent's top innovation cluster, with particular strengths in energy, automotives, the life sciences, and aerospace. USP also leads a growing South American Research Security Consortium (SARSeC), which includes institutions from Argentina, Brazil, Chile, and Peru. SARSeC aims to provide "robust standard operating procedures (SOPs), best practice guides, and training resources…to empower researchers and institutions to maintain the highest standards of research security."

South America's emerging research security community is connected to peers in North America and Europe, but developments in the region will inevitably reflect local conditions. The geopolitical orientations of South American countries, and their trade patterns and positions in critical technologies and value chains will shape local assessments of risk. Longstanding challenges regarding regulation and enforcement,

institutional capacity, research security consciousness, and IP protection mean there is much work to do. Even so, a widely felt desire to reinforce fidelity to common principles, and to protect and equitably benefit from the fruits of the continent's bounty of intellectual and natural resources, its biodiversity, its proximity to the Antarctic for polar research, the purity of its skies for astronomy; and the astounding genetic heterogeneity of its peoples make South America an exciting region to collaborate with on building the future of research security.

Research Security-Related Events & Conferences

COGR October Meeting: COGR October Meeting:
Registration is now open for our October 23-24, 2025 meeting in Washington D.C. at the Washington Marriott in Georgetown. Preliminary agenda topics include:

- Simplifying Research Regulations and Policies: Optimizing American Science: A NASEM Report
- Cybersecurity & Other Research Security Implementation Updates
- Legislative Update & Outlook

Save the Date for ASCE 2026:
Mark your calendars now for the 2026 Academic Security and Counter Exploitation Program. Next year is the 10th anniversary of the largest research security conference in the world: February 24 - 26, 2026. (more)

Looking to participate in NSF SECURE Center co-creation activities or contribute to weekly briefings?
Sign up Here!