NSF SECURE Center Research Security Briefing

Safeguarding the Entire Community in the U.S. Research Ecosystem (SECURE)

Issue 1 - June 25, 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 Updates

New NSF Annual Malign Foreign Talent Recruitment Program Certification for PIs/co-PIs

The CHIPS and Science Act of 2022 prohibits participation in a malign foreign talent recruitment program (MFTRP) by covered individuals (senior/key personnel) involved with federal research and development (R&D) awards. The Act directs federal research funding agencies to establish a policy that requires each covered individual (CI) listed in an R&D proposal to certify that they are not a party to a MFTRP in the proposal submission and annually thereafter for the duration of the award.

The National Science Foundation (NSF) was the first federal agency to implement this certification via the common federal biosketch and current and pending support forms in May 2024. NSF is now implementing the annual certification requirement in compliance with the CHIPS Act. Additional agencies are expected to implement these requirements in the coming months.

NSF began rolling out the annual certification on June 7, 2025, for all PIs and co-PIs named on an NSF award made on or after May 20, 2024, and is working to expand the requirement to all senior/key personnel roles at a future date. Those with more than one active award made on or after May 20, 2024, are only required to certify once annually.

Research.gov users with applicable roles on an active NSF award made on or after May 20, 2024, will be prompted to complete the MFTRP annual certification each year after the date of award when they log-in to Research.gov and must complete the certification before they can submit annual project reports or conduct other Research.gov activity. NSF is making sample contracts available that meet the parameters of a MFTRP. Contract examples and frequently asked questions can be found on the NSF website **here** under MFTRPs.

DoD Publishes Revised Matrix to Inform Fundamental Research Proposal Review and Mitigation Decisions

The Department of Defense (DoD) published the 2025 Decision Matrix to Inform Fundamental Research Proposal Mitigation Decisions on May 9, 2025, effective for proposals submitted on or after that date. The matrix updates the initial version published in June 2023 to inform DoD components (Army, Navy, etc.) conducting risk-based proposal reviews and institutions and researchers submitting proposals. It identifies prohibited actions, and conditions where mitigation is required, expected, or suggested.

While prohibitions on participation in malign foreign talent recruitment programs (MFTRPs) remain as required by the CHIPS and Science Act, the matrix no longer requires institutions to have a policy prohibiting participation. The revised matrix also prohibits DoD funding for "Collaborations for the specific purpose of fundamental research" which refers to research proposed to be funded by DoD that include collaboration with an academic institution that appears on the 1286 list or FY 2019 NDAA list. Per the revised guidance it is defined as, "research that is identified in the fundamental research project proposal that is to be conducted with an

entity that is included on the most recent version of the list developed pursuant to section 1286 of the NDAA for FY 2019, as amended, or to any employees of such entities." Engagement with entities on this list would otherwise be treated as indicated for the different categories in the matrix (i.e., mitigation measures required, expected or suggested).

The updated matrix and guidance clarify that co-authorships with restricted entities or individuals in MFTRPs should not be the basis for the denial of an award but may result in requests for mitigation measures. This is an important clarification as many institutions have submitted proposals that appeared to have been rejected based on co- authorship in the past. Per DoD, "Co-authorship and patents are both useful in providing a full picture of a fundamental research project's risks but are not, on their own, sufficient cause to deny funding for a fundamental research project proposal. International collaboration is an important mechanism for participating in the global scientific commons and promoting progress in fundamental research."

In other changes of note, the category "mitigation measures recommended" has been changed to "Mitigation Measures Expected" which may suggest DoD is setting stronger expectations for risk mitigation under this category for indicators occurring after publication of DoD's October 10, 2019 "Letter to Academia." During the FDP meeting, DoD noted that the Department took steps in the current version to emphasize that co-authorships are considered "affiliations," but cannot be used as the sole basis for denying an award. The Matrix previously differentiated between "associations" and "affiliations," with "affiliations" involving remuneration. The current version uses only the term "affiliation," regardless of whether the activity is paid or unpaid.

Updated NIH Policy on Foreign Subawards

Guide notice NOT-OD-25-104 prospectively updates NIH policies and practices for utilizing foreign subawards. Per the notice, "NIH is establishing a new award structure that will prohibit foreign subawards from being nested under the parent grant. This new award structure will include a prime [with independent linked awards] that will allow NIH to track the project's funds individually while scientific progress will be reported collectively by the primary institution under the Research Performance Progress Report."

In comments made during a June 5 Council on Governmental Relations (COGR) meeting session, NIH Director Dr. Jay Bhattacharya noted that with institutions responsible for the oversight and discipline of subawardees under the previous/existing structure, NIH has little direct control or insight into these organizations. Dr. Bhattacharya suggested that under the new structure, foreign collaborators will be like a direct grantee, drawing funds and having oversight from NIH.

The guide notice indicates that "NIH anticipates implementing the new award structure by no later than September 30, 2025, prior to Fiscal Year 2026." The policy further indicates that "NIH continues to support direct foreign awards" and plans to expand this policy to domestic subawards in the future, for consistency.

Per the notice, NIH will not issue awards to domestic or foreign entities, whether new, renewal or non-competing continuation, that include a subaward to a foreign entity and will no longer accept prior approval requests to add a new foreign component or subaward to an ongoing

project. NIH will allow Institutes, Centers and Offices to renegotiate awards to remove subawards to foreign entities and, "where the work can be performed domestically, allow the funds to be rebudgeted for use by the prime recipient (domestic or foreign) or a domestic subrecipient. If a project is no longer viable without the foreign subaward, NIH will work with the recipient to negotiate a bilateral termination of the project, taking into consideration any need to support patient safety and/or animal welfare."

A related May 7 article indicates that NIH "will continue to fund foreign components, as long as they are structured as independent subprojects rather than subawards."

Notice of Information: NIH SBIR and STTR Foreign Disclosure Post-Award Requirements for Active SBIR and STTR Awardees (NOT-OD-25-102) (4/29/2025)

Effective immediately the SBIR and STTR Foreign Disclosure and Risk Management Requirements described in NOT-OD-23-139 and NOT-OD-24-029 may be applied to all active SBIR and STTR awards regardless of the due date the competing application was submitted. Recipients with active awards that did not undergo foreign risk assessment at the time of their original application may be required to disclose all funded and unfunded relationships with foreign countries, using the Required Disclosures of Foreign Affiliations or Relationships to Foreign Countries Form.

If the recipient reports a covered foreign relationship that meets any of the risk criteria prohibiting funding, NIH may deem it necessary to terminate the award for material failure to comply with the federal statutes, regulations, or terms and conditions of the federal award.

U.S. to 'Aggressively Revoke' Visas Held by Chinese Students (AIP, 5/30/3025)

On May 28, 2025, "Secretary of State Marco Rubio announced ... that the U.S. will 'aggressively revoke' visas held by Chinese students, 'including those with connections to the Chinese Communist Party or studying in critical fields.' All future visa applications from China will also be subject to additional scrutiny, he added." [A State Department spokesperson indicated] "... that the decision is partly tied to concerns about technology transfer to China, saying the U.S. 'will not tolerate the CCP's exploitation of U.S. universities or theft of U.S. research intellectual property or technologies to grow its military power, conduct intelligence collection, or repress voices of opposition.'" (more)

Education Department Releases New Foreign Gifts Data (5/14/2025)

American institutions of higher education reported $290 million in foreign gifts and contracts between last July and this February, according to the latest data from the U.S. Department of Education (more). Some institutions are checking the published data for consistency with the data submitted, suggesting that there have been significant errors in the past.

Professional Association Meetings & Resources

FDP May 2025 Virtual Meeting

The Federal Demonstration Partnership's (FDP) May 2025 virtual meeting included several research security-related sessions. Research security highlights included:

Update on Federal Research Security Program Requirements

Moderator/Host: Lisa Nichols, Executive Director, Research Security, University of Notre Dame

Federal Agency Updates

The National Science Foundation (NSF) - Sarah Stalker-Lehoux, Acting Chief of Research Security, Strategy and Policy); Department of Defense (DoD) – Jason Day, Research Policy Director; and Department of Energy (DoE) – Julie Anderson, Director, Office of Research, Technology, and Economic Security presented.

Federal research funding agencies continue to work to coordinate the implementation of NSPM-33 research security program (RSP) requirements, working through an Interagency Memorandum of Agreement (MOA). The goal is to make something publicly available within approximately 6 months. The MOA establishes a common government-wide process and location for covered institutions (CIs) (those with >$50 million in annual federal funding) to annually certify their RSPs, possibly through research.gov. NSF will maintain a list of CIs and monitor certification. Agencies will provide feedback on the MOA by June 6 and coordinate implementation with the White House Office of Science and Technology Policy (OSTP). Agencies anticipate that research security training will be required within 12 months prior to proposal submission (i.e., *not* at time of award) consistent with language in the CHIPS and Science Act.

- NSF anticipates issuing a notification in June 2025 about their implementation plans for research security training, which they expect to be required sometime in the fall of 2025 (90 days from issuance of the notice).
- DoE has already implemented a research security training requirement (effective May 1, 2025) and will likely align with NSF regarding training options that satisfy the requirement (e.g., a new condensed training module – see below).
- DoD is still evaluating when it will implement required research security training. Details on training implementation have not yet emerged from other agencies.

Regarding RSP requirements, DoD added that the Department is considering the use of foreign travel reporting as part of a risk mitigation measure for use across all DoD Components.

Effective May 9, 2025, PIs and Co-Is on NSF awards made on or after May 20, 2024, must complete an annual process recertifying they are not party to a malign foreign talent recruitment program (MFTRP).

- PIs/Co-Is will be prompted to complete the recertification when they log into research.gov (e.g., to complete their annual progress report). Additional Senior/Key Personnel roles will be added in the future. Recipient institutions will not be able to see when PIs/Co-Is have completed the recertification
- On June 6, NSF is making sample MFTRP contracts available.

- Foreign Financial Disclosure Reporting (FFDR):
    - The 2025 reporting period is now July 1, 2024, through June 30, 2025.
    - The 2025 submission period is now September 1 through October 31, 2025.
    - There will not be a grace period.

FDP Cybersecurity Demonstration

Jarret Cummings, Senior Advisor, Policy and Government Relations, Educause and Lisa Nichols, Executive Director, Research Security, University of Notre Dame/NSF SECURE Center/FDP RSS Co-chair

- The Research Security Subcommittee is leading an FDP cybersecurity demonstration in partnership with Educause, working with other FDP committees, federal agencies and other organizations. Project deliverables include:
    - An overview of current and emerging cybersecurity risks to fundamental research at recipient institutions as a foundation for a risk-based approach.
    - A cybersecurity framework including fundamental principles and elements for institutions to assess and address risks and implement flexible solutions as part of their research security program.
    - A plan for a potential implementation of a pilot demonstration.
- A Cybersecurity Demonstration Working Group (WG) will include representatives from several FDP committees and subcommittees, Educause and other higher education association partners, and Federal partners, including NIST, NSF, DoD, and other agencies to provide direction for the full demonstration process.
- A Cybersecurity Framework Working Group, will include Chief Information Security Officers, compliance, researchers, and others from different types and sizes of research institutions and other partners (i.e., Trusted CI and RRCoP). This WG will develop a fundamental cybersecurity risk management approach that is consistent with NIST guidance and supports individual institutional assessment of risks of their research portfolio and the flexibility to develop a calibrated approach that reflects and reasonably manages risks and protects research assets.
- The Demonstration WG will consult with federal research funding agencies prior to delivering a final product to the FDP Executive Committee. Following FDP approval, the WG will deliver the framework and any related materials to NSF and the federal interagency in support of federal RSP cybersecurity requirements.
- The working group plans to deliver the framework and related materials in approximately six months.

Condensed Training Module (CTM) 1.0

Lisa Nichols, University of Notre Dame/SECURE Center

- The CHIPS and Science Act requires that each covered individual listed on the application for a R&D award certify that they have completed research security training within one year of application. The training requirement is therefore broadly applied and not just part of the federal NSPM-33 research security program requirements.
- The SECURE Center has released a condensed version of the four NSF research security training modules originally funded by NSF, NIH, DOD and DOE and developed through cooperative agreements with institutions and other non-federal entities. The module used as a foundation the condensed version generated by SECURE Center staff at the University of

Michigan collaboratively with the Ohio State University, Stanford University and Duke University.

- Condensed training module 1.0 (CTM 1.0) is an approximately one-hour training module that also incorporates several updates. Information on malign foreign talent recruitment programs is expanded in this module and examples of contract language are provided. In addition, information on agency risk reviews of fundamental research proposals, internal risks, and elicitation have been added and the foreign travel security section has been expanded. For consistency with the CHIPS Act, a brief section on cybersecurity has also been added. The module has been redesigned to provide a consistent look and feel across the different sections and improve usability.
- The CTM 1.0 file can be found on the **SECURE Center website** and downloaded for use in institution's learning management system. It will also be made available to CITI for CITI users. The webpage provides background on federal training requirements and agency implementation to date.
- The SECURE Center will periodically update the training as new information and federal requirements evolve. The Center will continue to incorporate user feedback for continuous improvement.

Perspectives on Managing Foreign Travel Security Risks
Moderator/Hosts: Steven Post, University of Arkansas for Medical Sciences; Mark Haselkorn, University of Washington; Lee Stadler, University of Missouri Kansas City

In a joint session, the Federal Demonstration Partnership's (FDP) FACT (Faculty Administrator Collaboration Team) and the SECURE Center teams, with the help of FDP attendees, examined the different perspectives of faculty and research administrators related to the requirements and perceived risks associated with foreign travel security. In breakout sessions the teams walked through several foreign travel security risk scenarios for smaller group discussions. Faculty expressed interest in clear information that would allow them to gain a better understanding of what they need to know and report.

Examples include infographics, one-page overviews, and scenarios that might occur while they are traveling that could necessitate additional reporting. Session facilitators suggested that both faculty and administrators are seeking information, often from each other. Faculty are looking for guidance and administrators details to assist with guidance.

Expanded Clearinghouse/Research Security/Subawards Subcommittees Joint Session

Moderator/Hosts: Amanda Hamaker, Purdue University; Robert Prentiss, Yale University; Jennifer Rodis, University of Wisconsin-Madison; Jennifer McCallister, Duke University; Stuart Politi, Mount Sinai School of Medicine; Doug Backman, University of Central Florida; and Mark Sweet, University of Wisconsin-Madison

This joint session of subcommittees focused on the potential to enhance existing FDP tools to incorporate data elements that will be required and/or useful to institutions as Federal funding agencies implement research security program requirements. For example, the subcommittees noted that one potential approach could be to:

1. Add fields to the FDP Expanded Clearinghouse related to institutional requirements for research security programs and/or research security training requirements.
2. Add a certification to the FDP Sample Letter of Intent (LOI) related to prohibitions on Malign Foreign Talent Recruitment Programs (MFTRPs)

The joint subcommittees proposed that a working group be formed, specifically focused on the community's needs regarding institutional certifications for non-participation in MFTRPs. Multiple attendees volunteered to participate.

Foreign Influence Working Group (FIWG) – Federal Panel

Moderators/Hosts: Jim Luther, FIWG Co-Chair, Yale University; Pamela Webb, FIWG Co- chair, University of Minnesota

This session included a summary of recent federal activities as well as updates from federal partners on research security topics of interest.

Julie Anderson (DOE) emphasized that DOE is committed to aligning with other agencies in implementing RSP requirements via an MOA, but noted that there may be some differences across agencies due to differing missions and statutory requirements. Anderson also noted that DoE is supportive of many options to meet their research security training requirement (effective May 1, 2025). When new Senior/Key Personnel are added to an existing DoE project, the agency expects them to certify to their completion of research security training within 30 days. Anderson also highlighted DoE's use of the Transparency of Foreign Connections Disclosure and Certification that includes updated instructions to clarify which questions must be completed by institutions of higher education (IHEs).

Sarah Stalker-Lehoux (NSF) reviewed several of the NSF topics covered during the previous day's Update on Federal Research Security Program Requirements (see above) but also highlighted the work underway through NSF's two complementary cooperative agreements to fund the SECURE Center and SECURE Analytics. In addition, Stalker-Lehoux called attention to NSF's Research on Research Security (RoRS) Program (PD 25- 275Y) that is currently accepting proposals.

Michelle Bulls (NIH) was unable to attend the session, but provided slides that highlighted, 1) NIH's delay in adopting the Common Forms for Biosketches and Current & Pending (Other) Support documentation, and 2) NIH's continued participation in the Interagency Working Group, led by NSF, to coordinate agencies' implementation of RSP requirements.

Jason Day noted that DoD recently issued an updated version of the agency's Decision Matrix applicable for all proposals submitted on or after May 9, 2025. Day also noted that DoD has adopted use of the Common Forms, though not via SciENcv yet. DoD has not implemented their research security training requirement but anticipates aligning with other agencies. In addition, an updated 1286 list will be released soon.

Case Studies with Data Integration using ORCID

Moderators/Hosts: Lori Schultz, Assistant Vice President, Research Administration, Colorado State University; Shawna Sadler, ORCID

Three universities of different sizes presented examples of how their institutions have been integrating ORCiD into their administrative process, especially research. Topics included researcher adoption, connecting with existing systems, and navigating the campus landscape, with a focus on synthesizing Biosketches and/or Current & Pending (Other) Support documents. This information both supports faculty workflows and informs research security efforts. Presenters are willing to discuss their efforts with interested university colleagues.

- Augusta University: Jennifer Putnam Davis (Scholarship and Data Librarian, Asst. Professor) and Vonny Nogales (Library Systems Analyst)
- Northwestern University: Kim Griffin (Dir. Research Analytics) and Karen Gutzman (Head Research Assessment & Communications
- University of Florida: Kevin Hanson (Assoc. Director Information Services)

National Academies Research Security Workshop

The National Academies of Sciences, Engineering, and Medicine held a workshop May 22-23, 2025, to consider 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.

Workshop sessions included:

- The US Department of Defense, Research, and the Research Security Environment
- Research Security Policies and Requirements - Scope and Measures of Effectiveness
- The Impact of Research Security Policies and Requirements on the Research Ecosystem
- Advancing Research Security in the Research Community
- The Path Forward for the U.S. Department of Defense and Other Funding Agencies

Video of the event will be available soon. SECURE Center team members Amanda Humphrey and Lisa Nichols serve on this National Academies Working Group and team members Lori Schultz and Jason Owen-Smith served on panel sessions.

COGR Updates Research Security Resources

COGR included several research security-related items in its May 2025 Update, including:

- Updates to COGR's comprehensive matrix of science and security laws, regulations and policies.
- Updates to COGR's Quick Reference Table of Current and Upcoming Federal Research Security Requirements.

U.S. Congressional Activity

House Committee Chairs Send Letters to Universities on the Risk of CCP Infiltration into SBIR and STTR Programs (5/20/25)

"Congressman Roger Williams (R-TX), Chairman of the House Committee on Small Business; Congressman Brian Babin (R-TX), Chairman of the Committee on Science, Space, and

Technology; Congressman Tim Walberg (R-MI), Chairman of the Committee on Education and Workforce; and Congressman John Moolenaar (R-MI), Chairman of the Select Committee on the Chinese Communist Party (CCP), sent letters to the to the [sic] State University of New York (SUNY) and the University of California (UC) urging the university systems ensure that innovation developed by American small businesses stays out of the hands of our foreign adversaries, like the People's Republic of China." (more)

House committee leaders encourage Duke University to end partnership with China's Wuhan University (5/15/25)

The heads of two House committees have written a letter to the president of Duke University advising the North Carolina school to end its partnership with Wuhan University in China. Rep. John Moolenaar (R-Mich.), the chair of the Select Committee on the Chinese Communist Party, and Rep. Tim Walberg (R-Mich.), the chair of the House Education and Workforce Committee, sent the letter Wednesday, May 14, 2025, regarding concerns about China gaining access to U.S. research. (more)

Research Security-Related Reports and Resources

Federal Research Security Policies: Background and Issues for Congress

The Congressional Research Service (CRS) issued a report on May 20, 2025, summarizing federal research security policy efforts to date, and providing options Congress might consider to address perceived gaps or deficiencies while also remaining cognizant of the potential increase to administrative burden they would present.

Proposed options discussed include:

- Expanding sources of foreign support researchers are required to disclose beyond those that involve the design, conduct of reporting of research,
- Broadening the scope of who is required to disclose Current and Pending (Other) Support (i.e., beyond senior/key personnel),
- Increasing the frequency of post-award updates to Current and Pending (Other) Support,
- Expanding agency requirements when reviewing disclosed information to include the identification of potential security vulnerabilities,
- Focusing risk assessment activities more narrowly (e.g., increasing focus on research involving critical and emerging technologies),
- Expanding agencies' requirements to report to congress on: research security violations; mitigation measures required; status of the implementation of requirements; or tasking a nongovernmental entity (e.g., the SECURE Center) with compiling this information to report to Congress.

Upcoming Research Security-Related Events & Conferences

NCURA Annual Meeting

Registration is open for the 67th annual NCURA meeting in Washington DC, August 10 - 13, 2025. The event includes several research security-related offerings, including concurrent sessions and a pre-meeting workshop. (more)

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)

Other Research Security News

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

In Reversal, Trump Says Chinese Students Are Welcome

(*Inside Higher Ed*, 6/13/2025)

"President Trump said that Chinese international students would be welcome in the U.S. in a post on Truth Social on Wednesday announcing the terms of a pending trade agreement with China. In exchange for shipments of rare earth metals, the U.S. 'WILL PROVIDE TO CHINA WHAT WAS AGREED TO, INCLUDING CHINESE STUDENTS USING OUR COLLEGES AND UNIVERSITIES (WHICH HAS ALWAYS BEEN GOOD WITH ME!),' Trump posted (capital letters his)."(more)

Harvard's China Ties Become New Front in Battle with Trump

(*Wall Street Journal*, 6/8/2025)

In his war with Harvard, President Trump has sought to withhold billions of dollars in federal funding from the school and strip its tax exemptions, measures the White House initially tied to perceived antisemitism at the school amid Israel's war in Gaza. In recent weeks, long-simmering Republican anger over Harvard's links to China has increasingly gained traction. In escalating calls to punish the school, a training event two years ago in the Chinese city of Kunming has emerged as Exhibit A. (more)

Penn included in foreign-funds probe (*The Chronicle of Higher Education*, 5/14/2025)

The University of Pennsylvania is the latest institution to be investigated by the Trump administration over foreign-funds disclosures. In a letter, the Department of Education asked Penn to provide an accounting of foreign gifts, donations, and contracts from individuals or entities abroad for the past eight years. It accused the university of possible "incomplete, inaccurate, and untimely disclosures." Similar investigations have already been opened into Harvard University and the University of California at Berkeley. (more)

'Second chance': convicted US chemist Charles Lieber moves to Chinese university (*Nature*, 5/7/2025)

The prominent US chemist Charles Lieber, who was convicted of hiding his research ties to China from US federal agents, has joined the faculty of a Chinese university. On 28 April, Lieber became a full-time professor at Tsinghua Shenzhen International Graduate School (SIGS), according to a SIGS press release. The institution was established by Tsinghua University and the Shenzhen local government in 2001. (more)

Trump Scrutinizes Foreign Gifts, Raising the Stakes for Colleges

(*The Chronicle of Higher Education*, 5/5/2025)

"Colleges and universities should brace for another round of federal funding attacks as President Trump targets colleges that fail to report possible "foreign influence," higher education experts warn. Late last month, Trump directed the Department of Education to ensure it is enforcing Section 117 of the Higher Education Act—which requires institutions to disclose certain international gifts—as part of an executive order aimed at ending "the secrecy surrounding foreign funds." (more)

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

Sign up Here!

NSF SECURE Center

NSF SECURE Center Research Security Briefing

Safeguarding the Entire Community in the U.S. Research Ecosystem (SECURE)

Issue 2 - July 10, 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 Updates

Department of Defense (DoD) Publishes Updated 1286 List

On June 24, 2025, the DoD published its annual (FY24) update to the 1286 list. DoD reaffirmed the FY23 list of foreign talent recruitment programs that pose a threat to national security. The lists are required under the FY19 National Defense Authorization Act. Per the introduction, "Caution is advised for any researcher or institution engaging with institutions" on the 1286 list. The list is one of several DoD, DOE and NSF use in risk reviews of fundamental research proposals.

NSF Updates to Research Security Policies

The National Science Foundation issued Important Notice 149, *Updates to NSF Research Security Policies*, on June 30, 2025. The notice includes NSF implementation of six requirements in alignment with the CHIPS and Science Act and National Security Presidential Memorandum 33.

1. Research Security Assessment and Required Recipient Documentation – Effective October 1, 2025 – "NSF proposers and recipients are required to maintain supporting documentation, including copies of contracts, grants, or any other agreements specific to foreign appointments, employment with a foreign institution, participation in a foreign talent recruitment program and other information reported as current and pending (other) support for all senior/key personnel that must be available to NSF upon request," as previously required, and to have reviewed it for compliance with NSF terms and conditions.

2. Research Security Training – Effective: October 1, 2025 – Individuals identified as a senior/key person must certify that they have completed research security training (RST) within 12 months prior to proposal submission. The Department of Energy previously implemented this requirement effective May 1, 2025.

   The notice notes the four research security training modules made available on the NSF website as a resource to awardee organizations. The notice indicates that the SECURE Center has developed an updated and condensed version of the four modules designed to meet the government-wide training requirement in the CHIPS and Science Act. Per the notice, NSF, NIH, DOE, and DOD all recognize completion of the condensed module as compliant with their respective RST requirements. Consistent with previous guidance, the notice indicates that "Proposers may utilize *any training* [emphasis added] that addresses cybersecurity, international collaboration, foreign interference, and rules for proper use of funds, disclosure, conflict of commitment, and conflict of interest."

   Institution's Authorized Organizational Representative (AOR) must also certify that all individuals identified as senior/key personnel have completed the requisite research security training and that the institution has a plan to provide appropriate training and oversight in the responsible and ethical conduct of research that meets the CHIPS Act requirements.

3. Malign Foreign Talent Recruitment Program Prohibition (MFTRP) – In Effect – Individuals who are a current party to a MFTRP are not eligible to serve as a senior/key person on an NSF proposal or any award made after May 20, 2024.

4. MFTRP Certification – In Effect – NSF requires MFTRP certifications from proposers (AORs) and individuals identified as senior/key personnel at the time of proposal and annually by individuals serving as a PI or co-PI on an active NSF award made on or after May 20, 2024 via Research.gov. See the description in the June 25 SECURE Center RS briefing.

5. Foreign Financial Disclosure Reporting (FFDR) – In Effect – This requirement became effective in July 2024. The current reporting period is from July 1, 2024 through June 30, 2025. However, per the notice, "to provide sufficient time for finalization and submission of the requisite information, the FFDR reporting portal on Research.gov will open for report submissions September 1, 2025, and the report must be submitted by October 31, 2025." In taking this approach, we note that NSF is maintaining consistency with the Higher Education Act Section 117 reporting period while allowing institutional staff to submit the report at a later date to avoid additional reporting during fiscal year end.

   The notice indicates that "The institution will maintain a copy of the relevant records subject to the disclosure requirement until the latest of:
   - the date that is four years after the end date of the award;
   - the date on which the agreement terminates; or
   - the last day of any period that applicable State public record law requires a copy of such agreement to be maintained."

   The notice also indicates that "upon review of a submitted disclosure, NSF may request that copies be submitted of any contracts, agreements, or documentation of financial transactions associated with disclosures submitted under this section."

6. Certification Regarding IHEs Hosting or Supporting Confucius Institutes – Effective October 1, 2025 – Details can be found in the notice. Currently IHEs are not hosting or supporting Confucius Institutes.

Professional Association Meetings & Resources

Video Recordings Now Available from National Academies May 2025 Workshop: Assessing Research Security Efforts in Higher Education

Video recordings are now available from the National Academies of Sciences, Engineering, and Medicine workshop held May 22-23, 2025, to consider 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.

Workshop sessions included:
- The US Department of Defense, Research, and the Research Security Environment
- Research Security Policies and Requirements - Scope and Measures of Effectiveness

- The Impact of Research Security Policies and Requirements on the Research Ecosystem
- Advancing Research Security in the Research Community
- The Path Forward for the U.S. Department of Defense and Other Funding Agencies

SECURE Center team members Amanda Humphrey and Lisa Nichols serve on this National Academies Working Group, and team members Lori Schultz and Jason Owen-Smith served as session panelists.

Research-Security Related Sessions at Upcoming NCURA Annual Meeting

The National Council of University Research Administrators (NCURA) will hold its 67th Annual Meeting in Washington DC, August 10-13, 2025.

Research-security related sessions include:

- Research Security and Export Controls for the Research Administrator
- Research Security Programs: Agency Implementations and the Road to Compliance
- Managing Compliance in the Proposal Process
- Leveraging ORCID in Research Administration
- Building Capacity to Manage RISC: Investing in Research Integrity, Security, and Compliance at Mid-Sized and Smaller MSIs and HBCUs

Additional details and meeting registration information are available here.

U.S. Congressional Activities

House Committee Chairs Send Letters to University of Michigan, NSF, NIH Following Arrest of Chinese Nationals

Following two separate incidents involving Chinese nationals with ties to the University of Michigan (UM), the Chairs of three US House of Representatives Committees recently issued records request letters to both UM and the heads of NIH and NSF.

On June 3, 2025, the Justice Department announced charges against two Chinese nationals, Yunqing Jian and Zunyong Liu, accusing the pair of conspiracy, smuggling goods into the United States, false statements, and visa fraud. According to the complaint, Mr. Liu smuggled *Fusarium graminearum*—a fungus that causes "head blight" in wheat and other grains — into America to further study the pathogen at the UM lab where Ms. Jian worked as a research fellow.

In a separate incident, Chenxuan Han — also a Chinese national — arrived at Detroit Metropolitan Airport on June 8, 2025, to begin work at UM as a visiting scholar from the College of Life Science and Technology in the Huazhong University of Science and Technology (HUST) in Wuhan, China, where she is pursuing her PhD. Upon arrival in Detroit, Han was arrested and charged with smuggling goods into the US and making false statements. According to the complaint, from 2024 to 2025 Han sent four packages addressed to recipients at UM that contained concealed biologic material. On June 18, 2025, US House of Representatives Committee Chairs John Moolenaar (Select

Committee on the CCP), Tim Walberg (Committee on Education and Workforce), and Brian Babin (Committee on Science, Space, and Technology) sent a letter to NIH Director Jay Bhattacharya and NSF Interim Director Brian Stone. The letter expresses concern about the incidents and, in particular, Jian, Liu, and Han's alleged ties to the Chinese Communist Party (CCP). It also poses several questions to NIH and NSF regarding the funding the agencies provided in support of professors Libo Shan and Ping He, the faculty members with whom Jian and Liu worked while at UM.

The letter requests NIH and NSF to "conduct a full review of all grants awarded to the UM's Molecular Plant-Microbe Interaction Laboratory, including Professors He and Shan, to determine whether any restrictions or prohibitions—pursuant to grant terms and conditions, agency policy and regulations, or federal statutes—have been violated." The letter also requests that the agencies respond to specific questions regarding:

- The agencies' due diligence risk analysis for awards to Professors Shan and He
- Proposal and program review documents for awards to Professors Shan and He
- The agencies' knowledge or review of the faculty members' potential dual affiliations with China Agricultural University while simultaneously holding positions at Texas A&M University
- Travel expenses paid by the agencies for Jian or Liu, and any travel to China by Professors Shan and He during the time that Jian or Liu worked under them

In addition, the letter poses broader questions to the agencies regarding:

- Compliance, monitoring, and additional due diligence pre-award, post-award, and during the period of performance
- Dual use research of concern (DURC) and potential weaponization of fundamental research Protection of intellectual property and scientific expertise
- Coordination/information-sharing across federal agencies

On the same day, the Committee Chairs sent a similar letter to UM President Domenico Grasso. The letter to UM requests information and documentation in response to a series of 24 questions covering many of the same topics included in the letter to NIH and NSF. However, the UM letter also includes topics specific to UM's policies, processes, and procedures regarding:

- Physical access and security, including how potential biohazards may arrive on campus
- Vetting of visiting scholars/researchers
- Review and approval of dual appointments
- Disclosure requirements, including consequences for noncompliance
- Compliance, monitoring, and additional due diligence on faculty during their employment
- The status of the university's establishment of a research security program office as outlined in the Guidelines for Research Security Programs at Covered Institutions
- If and how UM shares information with external entities including federal agencies and the US Intelligence Community

In addition to the Chairs, the letters were co-signed by 22 other Members of Congress from the three committees.

Congress requests GAO report on Research Security Program implementation
On June 24, 2025, the House Committee on Science, Space and Technology sent a letter to the Government Accountability Office (GAO) Comptroller General. The letter requests that GAO conduct a review of federal agencies' and research institutions' implementation of research security guidelines, as well as agencies efforts to measure the effect of research security requirements.

Upcoming Research Security-Related Events & Conferences

NCURA Annual Meeting: Registration is open for the 67th annual NCURA meeting in Washington DC, August 10 - 13, 2025. The event includes several research security-related offerings, including concurrent sessions and a pre-meeting workshop. (more)

FDP Virtual Meeting: Registration is now open for the Federal Demonstration Partnership (FDP) Virtual September 2025 meeting, taking place Monday, September 15th (11 AM ET – 5 PM ET), Tuesday, September 16th (11 AM ET – 5 PM ET) and Wednesday, September 17th (11 AM ET - 2 PM ET). (more)

COGR October Meeting: Registration is now open for the October 23-24, 2025 meeting in Washington D.C. at the Washington Marriott in Georgetown. (more)

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. Proposals are being accepted through noon (CST) on August 31, 2025 (more)

Other Research Security News

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

How Harvard's Ties to China Helped Make It a White House Target (***New York Times***, 7/7/2025): "Harvard turned to international donors, including China, as one way to help save it from financial troubles. That money is dwindling, but Republicans are questioning the relationship." (more)

Grand Jury Indicts Russian Scientist on Smuggling Charges (***New York Times***, 6/25/2025): "A federal grand jury in Boston on Wednesday indicted Kseniia Petrova, a Russian researcher who works in a laboratory at Harvard Medical School, on criminal charges of smuggling goods into the United States and lying to customs officials." (more)

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

NSF SECURE Center Research Security Briefing

Safeguarding the Entire Community in the U.S. Research Ecosystem (SECURE)

Vol. 1 No. 3: July 17, 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 Updates

NSF Updates *Important Notice 149*

On June 30, 2025, the National Science Foundation (NSF) issued *Important Notice 149*, described in detail in the July 10, 2025, *SECURE Center Research Security Briefing* Volume 2.

On the same day *Briefing* Volume 2 was published, NSF issued an updated version of *Important Notice 149*, now dated July 10, 2025. The comparison below outlines the material changes made between the two versions. The revised *Notice* also included some additional minor edits for clarity and formatting.

Effective dates

The effective dates have been changed from October 1, 2025, to October 10, 2025, for three areas:

- Research Security Assessment and Required Recipient Documentation
- Research Security Training
- Certification Regarding IHEs Hosting or Supporting Confucius Institutes

No other changes were included in these sections. As listed in the *Important Notice 149*, all other areas covered by NSF Research Security Polices are in effect.

Foreign Financial Disclosure Report (FFDR), Public Release

Under this section, guidance on the information regarding the ability for an Institution of Higher Education to request an opt-out for the name and address of a foreign source has been removed. Previously, NSF indicated they were working on a mechanism for such requests.

As it has in prior guidance, in the July 10, 2025, the updated version of *Important Notice 149,* NSF states:

"While it is NSF's intention to make public the information provided or collected in the FFDR disclosures, certain data elements will be treated as confidential to the extent required or permitted under applicable Federal law."

USDA's *National Farm Security Action Plan*

On July 8, 2025, the US Department of Agriculture announced the release of its *National Security Action Plan*

Per the press release, the *Action Plan* builds upon prior efforts including the May 5, 2025, Executive Order "Improving the Safety and Security of Biological Research," as well as NSPM-33-related policies and guidance. Seven topical areas are identified:

- Secure and Protect American Farmland
- Enhance Agricultural Supply Chain Resilience
- U.S. Nutrition Safety Net Must be Protected from Fraud, Abuse, and Foreign Adversaries
- Enhance Research Security
- Evaluate USDA Programs to Ensure America First Policies
- Safeguard Plant and Animal Health
- Protect Critical Infrastructure

New initiatives are described in these areas. It is anticipated USDA will issue further guidance on these topics.

U.S. Congressional Activities

House Select Committee on the CCP urges U.S. universities to cut ties with the China Scholarship Council

On July 9, 2025, the House Select Committee on China sent letters to seven universities calling on them to reconsider joint programs associated with the China Scholarship Council (CSC). Letters to the universities including Dartmouth College; Temple University; University of California, Davis; University of California, Irvine; University of California, Riverside; University of Notre Dame; and the University of Tennessee are linked in the press release.

Per the letters, *"Unlike other international student programs, the CSC has faced increasing scrutiny and criticism due to concerns over academic freedom, surveillance of students, ideological control, and potential espionage. For example, CSC mandates that sponsored students return to the PRC upon completing their studies and serve the PRC for at least two years,"* and *"Additionally, CSC requires these sponsored students to submit a report to PRC embassies or consulates every three months, detailing their academic progress, laboratory work, research outputs, and publications. PRC diplomatic missions are tasked to monitor the 'ideological and academic progress' of CSC-sponsored students."*

The letters include a series of questions for the institutions, with responses due by July 22, 2025. Among the information requested are:

- All documents regarding the contractual relationships between the institution and CSC;
- A list of which Chinese entities CSC-sponsored students came from between May 2020 and May 2025;

- A list of those that came to the institution under a non-STEM program and subsequently switched majors to a STEM program;
- Whether any CSC-funded students worked on research funded by any U.S. government entity or funds used from any government entity were used to support CSC sponsored students and scholars;
- Whether CSC-sponsored students are currently studying or doing research in STEM fields at the university;
- Whether any CSC-sponsored students in STEM fields stayed at the institution for postdoctoral research after completing their Ph.D. and whether federal funding has been used to support their post-doctoral research.

Research Security News and Reports

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

After Northwestern scientist questioned for China ties died by suicide, family sues and speaks out (NBC News, 7/12/2025)

"The Wu family suit, filed on June 23, says that the school's treatment of [faculty member Jane Wu], including its alleged efforts to oust her, her physical eviction from her office and forced hospitalization, was a 'substantial and decisive factor in her decision to end her life.'" (more)

Canada's Leap Forward in Research Security (*Minerva*, 7/8/2025)

The authors highlight key events over the past decade that have played a significant role in shaping Canada's current research security posture and posit that the country's responses to them — including those from the federal government, individual provinces, and academia — illustrate a distinct change in Canada's position on the securitization of research. The authors assert that, prior to 2024, Canada's research security efforts were focused primarily on education and awareness-raising. However, the federal government's recent adoption of more assertive policies, including the January 2024 implementation of the Policy on Sensitive Technology Research and Affiliations of Concern (STRAC), indicates a transition from a position of "Scientific Globalism" to one more representative of "Scientific Nationalism." (more)

NIH restores grants to South Africa scientists, adds funding option for other halted foreign projects (*Science*, 7/3/2025)

"The National Institutes of Health (NIH) has softened a controversial change to its foreign funding policy that had put many clinical trials abroad in limbo. Staff guidance dated 30 June maintains that grant renewal and new applications including a foreign subaward submitted after 1 May will not be reviewed until the new tracking system is in place. But the document

describes an exception for human subject research in applications submitted earlier, and for ongoing human studies. As a temporary measure, NIH grants staff can convert the subawards within these projects to special 'supplements' to the main grant that will go directly to the foreign collaborator, the document says." (more)

Upcoming Research Security-Related Events & Conferences

NCURA Annual Meeting

Registration is open for the 67th annual NCURA meeting in Washington DC, August 10 - 13, 2025. The event includes several research security-related offerings, including concurrent sessions and a pre-meeting workshop. (more)

Research-Security Related Sessions at Upcoming NCURA Annual Meeting:

- Research Security and Export Controls for the Research Administrator
- Research Security Programs: Agency Implementations and the Road to Compliance
- Managing Compliance in the Proposal Process
- Leveraging ORCID in Research Administration
- Building Capacity to Manage RISC: Investing in Research Integrity, Security, and Compliance at Mid-Sized and Smaller MSIs and HBCUs

Additional details and meeting registration information are available here.

FDP Virtual Meeting

Registration is now open for the Federal Demonstration Partnership (FDP) Virtual September 2025 meeting, taking place Monday, September 15th (11 AM ET – 5 PM ET), Tuesday, September 16th (11 AM ET – 5 PM ET) and Wednesday, September 17th (11 AM ET - 2 PM ET). (more)

COGR October Meeting

Registration is now open for our October 23-24, 2025 meeting in Washington D.C. at the Washington Marriott in Georgetown. (more)

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. through noon (CST) on August 31, 2025. Proposals are being accepted through noon (CST) on August 31, 2025 (more)

NSF SECURE Center Research Security Briefing

Vol. 1 No. 4: July 24, 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 Updates

Updated Implementation Guidance of NIH Policy on Foreign Subawards for Active Projects (Notice Number: NOT-OD-25-130, issued July 18, 2025)

In keeping with its goals related to research security, NIH provided this updated guidance on the policy for existing projects and submitted applications related to the implementation of the NIH Policy on Foreign Subawards (see NOT-OD-25-104).

This updated guidance creates an alternative, short-term approach for existing grants and cooperative agreements involving human subjects research (e.g., clinical trials and clinical research) with foreign sites. The alternative approach involves removing a foreign sub-award from the primary award and having it issued as a foreign supplement award. It is noted that each foreign supplement award can only be issued to a single foreign entity.

By choosing this pathway, and so that NIH can ensure its financial management and reporting obligations:

> *...both the primary award and foreign supplement(s) will be removed from the streamlined non-competing award process (SNAP) and automatic carryover authority. The primary award and each foreign supplement will be issued with a distinct document number and will need to submit separate annual Federal Financial Reports (FFR, SF-425).*

No re-budgeting will be allowed between the primary award and supplements within a budget period. As indicated in the prior notice, prime awardees can use the annual RPPR process to request a reallocation of funds across the entire project, provided the total cost does not increase.

NIH was careful to point out:

> *This supplement option is in addition to, and not in lieu of, the other options outlined in NOT-OD-25-104; namely, ICOs may renegotiate with the primary recipients to move activities to a domestic organization, remove the scope of the foreign component from the overall project scope, or bilaterally terminate the award. Additionally, this supplement option is meant to be a short-term solution, permitted only for the current competitive segment, and it does not replace the new award structure announced in NOT-OD-25-104 that will apply to upcoming applications, including any planned renewals.*

NIH Announces a New Policy Requirement to Train Senior/Key Personnel on Other Support Disclosure Requirements

On July 17, 2025, NIH issued NOT-OD-25-133, a new policy requirement to train senior/key personnel on the requirement to disclose all research activities and affiliations in Other Support. The training requirement is effective October 1, 2025, and notes the availability of the federal research security training (RST) modules on the NSF website.

NSF's July 10, 2025 Important Notice No. 149, referencing the NSF-funded SECURE Center's condensed version of the federal RST modules, indicated that "NSF, NIH, DOE, and DOD all recognize completion of the condensed module as compliant with their respective RST requirements." NSF is leading the coordination of federal research funding agency implementation of research security requirements under a memorandum of agreement, working with these and other agencies. The training includes extensive information on federal disclosure requirements for biosketches and current and pending support.

Per the NOT-OD-25-133, "recipients must implement trainings in addition to maintaining a written and enforced policy on requirements for the disclosure of other support to ensure Senior/Key Personnel fully understand their responsibility to disclose." Additional information and clarification on these requirements will be included in future briefings as they become available.

U.S. Department of Education Opens Foreign Funding Investigation into the University of Michigan

Following two separate incidents involving criminal charges against Chinese nationals with ties to the University of Michigan (UM), on July 15, 2025, the US Department of Education (ED) opened a foreign funding investigation into the university. In a letter sent to UM Interim President Domenico Grasso, ED requests a variety of documents pertaining to UM's compliance with Higher Education Act Section 117 the university's international research collaborations, and research security program. Since April 2025, similar records requests have been sent to Harvard University, the University of California-Berkeley, and the University of Pennsylvania.

US Secretary of Agriculture Issues *America First Memorandum for USDA Arrangements and Research Security*

On July 8, 2025, US Secretary of Agriculture Brooke Rollins issued the ***America First Memorandum for USDA Arrangements and Research Security***. The memorandum came on the same day that the US Department of Agriculture (USDA) issued its *National Farm Security Action Plan*.

In the memo, Secretary Rollins directs USDA to undertake initiatives intended to "place America First in provisioning all USDA funds, regardless of source and in accordance with any statutory or legal requirements," and to prevent "the expenditure of American taxpayer funds to help foreign competitors out-produce, out-compete, and out-innovate the United States." Directives include a number of research security-related measures that will impact institutions that are recipients of USDA funding and individuals involved in the design, conduct, or reporting of USDA-funded efforts (i.e., covered individuals).

Agency Review of Existing Arrangements and Justification of New Arrangements

- Within 30 days, all USDA Mission Areas, Agencies, and Offices must conduct a comprehensive review of all current USDA awards and subawards "with any foreign person or entity or any U.S. citizen or entity subject to foreign ownership, control, or influence," including justification as to why a US recipient was not selected for all applicable awards/subawards. USDA Mission Areas, Agencies, and Offices must submit lists of applicable awards/subawards for review by the Office of Homeland Security, Office of the General Counsel, and Office of the Chief Scientist. After review, these offices will make recommendations to the Secretary on which awards, if any, "should be terminated due to potential risks to American agriculture."
- Effective immediately, prior to issuing any awards/subawards "with any foreign person or entity or any U.S. citizen or entity subject to foreign ownership, control, or influence," all USDA Mission Areas, Agencies, and Offices must provide justification for the arrangement to Office of Homeland Security, the Office of General Counsel, and the Office of the Chief Scientist and receive the approval of those offices prior to executing the arrangement.

Impacts on Applicants

Similar to requirements that have been implemented by other federal funding agencies, the memo requires USDA research and development (R&D) and science and technology (S&T) awards to include a number of research security-related terms and conditions for applicants. While not specifically defined in the memo, it is presumed that "applicants" has a definition similar to that of "covered individual" in NSPM-33 and other federal agency guidance (i.e., an individual who significantly contributes to the scientific development or execution of a research and development project funded or proposed for funding by the U.S. government).

Applicants are required to:

- Complete the Common Forms for Biographical Sketches and Current and Pending (Other) Support, and provide updated information annually throughout the duration of the award,

- Certify that research security training has been completed not more than one year prior to the date of application. Per the memorandum, USDA is requiring an annual recertification.
- Certify they are not a participant in a malign foreign talent recruitment program (MFTRP), and recertify annually.

Unlike research security-related requirements implemented by other federal funding agencies, USDA will also require applicants to:

- "Certify that they are not contracting, entering into arrangement with, or otherwise providing material or non-material benefit through the provision of funded or unfunded work to any foreign person or entity or any U.S. citizen or entity subject to foreign ownership, control, or influence by a country of concern or other foreign adversary unless appealed to and approved by the Secretary of Agriculture." "Certify that they are not party to utilizing forced labor, or partnering with universities who are party to utilizing forced labor;"
- "Complete a disclosure (updated annually) of contracts associated with participation in programs sponsored by foreign governments, foreign instrumentalities, or foreign entities including FTRPs;"
- "Seek approval from USDA to subaward any portion of a funded arrangement, including but not limited to university students, post-doctoral fellows, [and] visiting researchers."

Impacts on Employing Entities

The Secretary's memo includes requirements for certifications from "Employing Entities" like those implemented by other federal funding agencies, including certification of applicants' completion of research security training and awareness of the requirements outlined in the memo.

Unlike requirements from other federal funding agencies, the USDA memo also requires that Employing Entities:

- "Prohibit applicants who either are currently or have in the past 10 years participated in malign FTRPs from working on projects supported by R&D and S&T awards." The 10-year timeframe of this requirement may necessitate that Employing Entities collect data from their faculty from a period that *predates* widespread national awareness of malign foreign talent recruitment programs (MFTRPs). Since most Employing Entities did not become aware of or begin requiring specific disclosure information regarding MFTRPs until roughly 2019 and, per the USDA requirement, Employing Entities must prevent *past* participants in MFTRPs back to 2015 from working on USDA projects, then those entities may need to implement mechanisms to collect this specific information (i.e., request "retroactive" disclosure of MFTRP participation).

- "Provide any supporting documentation, including copies of contracts, grants, or any other agreement, specific to foreign appointments, employment with a foreign institution, participation in a FTRP, and other information reported as current and pending support for all applicants in an application." To date, only the National Institutes of Health (NIH) have required that this type of supporting documentation be provided as part of the application process. Other agencies, such as NSF, require that it be provided on request.
- "Review any documents required under this memorandum for compliance with USDA award terms and conditions, including guidance on conflicts of interest and conflicts of commitment."

Regarding implementation, per the memo, "Each Mission Area, Agency, or Office that administers arrangements shall be responsible for implementing and ensuring compliance with all aspects of this memorandum."

Research Security News and Reports

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

UT Knoxville Cuts Chinese Scholarship Program Under Pressure From House (*Inside Higher Ed*, 7/22/2025): "Under threat from Republican lawmakers, the University of Tennessee, Knoxville ended a scholarship partnership for Chinese students. (more)

US farm agency fires 70 foreign researchers following national security review (Reuters, 7/18/2025): Reuters reports the USDA stated it had fired 70 foreign contract researchers as part of its efforts to secure the US food supply. The contractors, mostly post-docs, had worked at the Agricultural Research Service within the USDA. (more)

Danish universities reject foreign researchers amid espionage fears (Euronews, 7/17/2025): Danish universities are conducting a higher scrutiny of proposed foreign researchers focusing on Russia, Iran and China, with Aarhaus University rejecting 24 researchers so far this year. (more)

Upcoming Research Security-Related Events & Conferences

NCURA Annual Meeting:

Registration is open for the 67th annual NCURA meeting in Washington DC, August 10 - 13, 2025. The event includes a number of research security-related offerings, including concurrent sessions and a pre-meeting workshop. (more)

Research-Security Related Sessions at Upcoming NCURA Annual Meeting:

- Research Security and Export Controls for the Research Administrator
- Research Security Programs: Agency Implementations and the Road to Compliance
- Managing Compliance in the Proposal Process
- Leveraging ORCID in Research Administration
- Building Capacity to Manage RISC: Investing in Research Integrity, Security, and Compliance at Mid-Sized and Smaller MSIs and HBCUs

Additional details and meeting registration information are available here.

FDP Virtual Meeting:

Registration is now open for the Federal Demonstration Partnership (FDP) Virtual September 2025 meeting, taking place Monday, September 15th (11 AM ET – 5 PM ET), Tuesday, September 16th (11 AM ET – 5 PM ET) and Wednesday, September 17th (11 AM ET - 2 PM ET). (more)

COGR October Meeting:

Registration is now open for our October 23-24, 2025 meeting in Washington D.C. at the Washington Marriott in Georgetown. (more)

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. through noon (CST) on August 31, 2025. Proposals are being accepted through noon (CST) on August 31, 2025 (more)

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

Sign up Here!

NSF SECURE Center Research Security Briefing

Vol. 1 No. 5: July 31, 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

Cadence Design Systems Agrees to Plead Guilty and Pay Over $140 Million for Unlawfully Exporting Semiconductor Design Tools to a Restricted PRC Military University

On July 28, 2025, the U.S. Department of Justice issued a press release regarding Cadence Design Systems' agreement to plead guilty to resolve charges of export control violations. The charges came as the result of the San Jose, California, company's sale of electronic design automation intellectual property technology to the National University of Defense Technology, a Chinese university included on the U.S. Department of Commerce's Entity List. (more)

U.S. State Department Investigating Harvard University Participation in the Exchange Visitor Program

In a July 23, 2025, press statement, Secretary of State Marco Rubio announced the opening of an investigation into Harvard University's eligibility to continue participating in the Exchange Visitor Program. While the statement notes that "All sponsors participating in this program are required to fully comply with exchange visitor regulations, transparency in reporting, and a demonstrated commitment to fostering the principles of cultural exchange and mutual understanding upon which the program was founded," it does not provide any details or specific allegations of infractions on the part of the university. In a related story, *The New York Times* reported that the Secretary's letter "gave Harvard a one-week deadline to produce a lengthy list of university records related to the student visa program."

Research Security News

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

How China's bold talent recruitment has shaped science (*Nature*, 7/29/2025):

"Over the past three decades, thousands of Chinese researchers who studied or worked abroad have returned to the country through…talent-recruitment [programs]. These recruits — who often receive substantial funding and benefits — have largely had a positive influence on China's research landscape and contributed to its global competitiveness, say scientists." (more)

U.S. Warns Montenegro Over University's Cooperation with Sanctioned Chinese Center (Radio Free Europe/Radio Liberty, 7/25/2025): "The United States has expressed concern over reports of the University of Montenegro's cooperation with a

scientific center controlled by the Chinese military's leading scientific and engineering research institution." (more)

Upcoming Research Security-Related Events & Conferences

NCURA Annual Meeting:

Registration is open for the 67th annual NCURA meeting in Washington DC, August 10 - 13, 2025. The event includes a number of research security-related offerings, including concurrent sessions and a pre-meeting workshop. (more)

Research-Security Related Sessions at Upcoming NCURA Annual Meeting:

- Research Security and Export Controls for the Research Administrator
- Research Security Programs: Agency Implementations and the Road to Compliance
- Managing Compliance in the Proposal Process
- Leveraging ORCID in Research Administration
- Building Capacity to Manage RISC: Investing in Research Integrity, Security, and Compliance at Mid-Sized and Smaller MSIs and HBCUs

Additional details and meeting registration information are available here.

FDP Virtual Meeting:

Registration is now open for the Federal Demonstration Partnership (FDP) Virtual September 2025 meeting, taking place Monday, September 15th (11 AM ET – 5 PM ET), Tuesday, September 16th (11 AM ET – 5 PM ET) and Wednesday, September 17th (11 AM ET - 2 PM ET). (more)

COGR October Meeting:

Registration is now open for our October 23-24, 2025 meeting in Washington D.C. at the Washington Marriott in Georgetown. (more)

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. through noon (CST) on August 31, 2025. Proposals are being accepted through noon (CST) on August 31, 2025 (more)

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

Sign up Here!

NSF SECURE Center Research Security Briefing

Vol. 1 No. 6: August 7, 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

Professional Association Resources & Meeting Reports

COGR Letter to USDA Regarding America First Memorandum

On July 31, 2025, COGR President Matt Owens sent a letter on behalf of COGR and its member institutions to US Secretary of Agriculture Brooke Collins regarding the secretary's July 8 memorandum, America First Memorandum for USDA Arrangements and Research Security. In the letter, Owens requests Secretary Collins to provide clarification on several points, including:

- **USDA's use of the terms "Arrangements" and "Sub-arrangements,"**
- **USDA's intended use of the term "Foreign Ownership, Control, or Influence" (FOCI) as applied to one of the new certification requirements for applicants,**
- **Confirmation that completion of the SECURE Center's Consolidated Training Module will fulfill the agency's research security training requirement, and clarification on whether this requirement applies to all senior/key personnel associated with a proposal, or only the individual applicant,**
- **USDA's prohibition of applicants who have participated in malign foreign talent recruitment programs in the past 10 years from working on projects, which deviates from the statutory language at 42 U.S. Code § 19231.**

Additional information regarding USDA's America First Memorandum can be found in the SECURE Center's July 24, 2025, Research Security Briefing No. 4.

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.

Securing American Innovation by Improving Research Security

(Foundation for American Innovation, 07/31/2025): Posted by a non-profit think tank, this article scopes the importance of research security and makes recommendations for federal government steps to ensure security and innovation. (more)

Building a Wall Around Science: The Effect of U.S.-China Tensions on International Scientific Research

(National Bureau of Economic Research, revised May 2025): A working paper (originally issued in June 2024) discussing the status and impact of the US-China relations across measures of trainee mobility, cross-border knowledge flows, and researcher productivity. (more)

Research Security-Related Events & Conferences

NCURA Annual Meeting:

Registration is open for the 67th annual NCURA meeting in Washington DC, August 10 - 13, 2025. The event includes a number of research security-related offerings, including concurrent sessions and a pre-meeting workshop. (more)

Research-Security Related Sessions at Upcoming NCURA Annual Meeting:

- Research Security and Export Controls for the Research Administrator
- Research Security Programs: Agency Implementations and the Road to Compliance
- Managing Compliance in the Proposal Process
- Leveraging ORCID in Research Administration
- Building Capacity to Manage RISC: Investing in Research Integrity, Security, and Compliance at Mid-Sized and Smaller MSIs and HBCUs

Additional details and meeting registration information are available here.

FDP Virtual Meeting:

Registration is now open for the Federal Demonstration Partnership (FDP) Virtual September 2025 meeting, taking place Monday, September 15th (11 AM ET – 5 PM ET), Tuesday, September 16th (11 AM ET – 5 PM ET) and Wednesday, September 17th (11 AM ET - 2 PM ET). (more)

COGR October Meeting:

Registration is now open for our October 23-24, 2025 meeting in Washington D.C. at the Washington Marriott in Georgetown. (more)

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. through noon (CST) on August 31, 2025. Proposals are being accepted through noon (CST) on August 31, 2025 (more)

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

Sign up Here!

NSF SECURE Center Research Security Briefing

Vol. 1 No. 7: August 14, 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

U.S. Congressional Activity

House Committee Chairs Request Documentation of Harvard's Ties to People's Republic of China and Chinese Communist Party

On July 30, 2025, U.S. Representatives John Moolenaar (R-MI, Chairman, Select Committee on the CCP), Tim Walberg (R-MI, Chairman, Committee on Education and Workforce), and Elise Stefanik (R-NY) sent a letter to Harvard President Alan Garber requesting that the university provide documentation related to its alleged connections to the People's Republic of China (PRC) and the Chinese Communist Party (CCP). The request includes all documents related to Harvard's formal and informal engagements, partnerships, or collaborations with entities "subordinate to or controlled or directed by" the PRC or CCP, as well as a list of all monies and non-monetary benefits received from such entities. (more)

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.

Voices: We can't afford to be passive about China. As a representative of Utah, I won't be. (Salt Lake Tribune, 8/7/2025): Opinion Editorial from Representative, Mike Kennedy (R-UT), member of the House Science, Space and Technology Committee, regarding national security threats related to universities, businesses, national labs. (more)

Class dismissed: The quiet collapse of US-China university partnerships (ThinkChina, 7/29/2025): As many U.S. institutions of higher education are sunsetting joint educational programs with Chinese entities—particularly in STEM-related fields—China is looking to other countries for partnerships. (more)

China Refocuses Its Science and Technology Ecosystem on Innovation and Security (Hoover Institution Press, 6/26/2025): "The government of China is overhauling its science and technology (S&T) ecosystem in ways that are sharpening geostrategic rivalry and impacting the risk portfolios managed by research security professionals. This overhaul aims to integrate basic science in priority fields with state-led mobilization of capital and S&T assets to enhance China's global influence as an innovation hub; and advance policy goals such as self-reliance, economic and defense strength, and comprehensive national power." (more)

Research Security-Related Events & Conferences

FDP Virtual Meeting:

Registration is now open for the Federal Demonstration Partnership (FDP) Virtual September 2025 meeting, taking place Monday, September 15th (11 AM ET – 5 PM ET), Tuesday, September 16th (11 AM ET – 5 PM ET) and Wednesday, September 17th (11 AM ET - 2 PM ET). (more)

COGR October Meeting:

Registration is now open for our October 23-24, 2025 meeting in Washington D.C. at the Washington Marriott in Georgetown. (more)

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. through noon (CST) on August 31, 2025. Proposals are being accepted through noon (CST) on August 31, 2025 (more)

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

Sign up Here!

NSF SECURE Center Research Security Briefing

Vol. 1 No. 8: August 21, 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

DoD Fundamental Research Guidance

The Department of Defense (DoD) published Fundamental Research Guidance on August 4, 2025. The Guidance provides background on Fundamental Research (FR) as defined by National Security Decision Directive – 189 (NSDD-189) and DoD's implementation of the Directive via the May 24, 2010 "Carter Memo". The Guidance notes that "under the Carter Memo, research funded by 6.1 budget activity or 6.2 research conducted on a university campus is fundamental. For other research categories, the Department must be deliberate when deciding that a particular research topic is appropriate for openly published fundamental research" the availability of a FR Review to assist S&T Managers with determining whether a particular research topic should be developed as fundamental.

The Guidance notes the benefits of FR and that "transformative technologies generally come from unrestricted research conducted by the most talented researchers in a collaborative, open environment." It incorporates Considerations for Program Managers and Contracts and Grants Officers, including:

- Refraining from imposing publication review of research that has been formally designated as fundamental;
- For awards with multiple performers, considering whether some portion of the work should be designated as FR even if much of the award is not; and,
- Avoiding flowing down restrictions to awardees performing FR that are inappropriate for FR.

In addition, apart from Risk-Based Security Reviews of Fundamental Research, that no security vetting should be done on personnel engaged in fundamental research and "no preapproval conditions for the addition of researchers such as students, postdoctoral fellows, laboratory technicians, or other persons not labeled as senior/key personnel by the research performer should be placed on awards for fundamental research."

Considerations for Prime Awardees include that in cases where a subawardee requests a FR designation, prime awardees are encouraged to contact the Program Manager and request such a designation. Taken together, the guidance has the potential to 1. significantly limit restrictions on fundamental research that can preclude the participation of some institutions and 2. foster the open-exchange of scientific information.

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.

CISA 2015 Expires September 30th

From Cyberscoop, a summary of possibilities or pathways regarding the pending Cybersecurity Information Sharing Act (CISA), set to expire at the end of September 2025. Congressional authorization is needed before that date for organizations to continue sharing threat data, including

with the federal government. The Cybersecurity Information Sharing Act of 2015 is a US federal law designed to improve cybersecurity by encouraging the sharing of cyber threat information between government agencies, private companies, and other non-federal entities. (more)

International Research Security Policy & Resources

Major University in Denmark Increases Research Security Procedures

Announced online, the University of Copenhagen is taking additional steps to protect its research from foreign influence. The University will have "new procedures aimed at screening potential collaborators, employees, and students with ties to countries identified as posing a heightened espionage risk." (more)

Research Security-Related Events & Conferences

National Academies "Assessing Research Security Efforts in Higher Education - Meeting of Experts 2":

Thursday, September 4th, 1-4:30pm. Convened by the Department of Defense, subject matter experts from universities and federal agencies will gather to discuss research security efforts, including potential measures of effectiveness and institutional perspectives. Conducted in person in Washington DC or some portions available via a webcast (registration required). (more)

FDP Virtual Meeting:

Registration is now open for the Federal Demonstration Partnership (FDP) Virtual September 2025 meeting, taking place Monday, September 15th (11 AM ET – 5 PM ET), Tuesday, September 16th (11 AM ET – 5 PM ET) and Wednesday, September 17th (11 AM ET - 2 PM ET). (more)

COGR October Meeting:

Registration is now open for the October 23-24, 2025, meeting in Washington D.C. at the Washington Marriott in Georgetown. Hotel reservations under the COGR block can now also be made. (more)

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. **Proposals are being accepted through noon (CST) on August 31, 2025.** (more)

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

Sign up Here!

NSF SECURE Center Research Security Briefing

Vol. 1 No. 9: August 28, 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

Federal Agencies Issue *Safeguarding Academia* Bulletin (August 25, 2025)

The Office of the Director of National Intelligence's National Counterintelligence and Security Center released the bulletin *Safeguarding Academia*, in partnership with the Federal Bureau of Investigation, the National Science Foundation, the Department of Education, and other federal agencies. The bulletin, aimed at the U.S. academic community, outlines potential threats posed by foreign adversaries, particularly foreign intelligence entities, to U.S. research, innovation, and talent within higher education institutions. Highlights include:

- Case studies providing real-life examples of the current risk environment, including talent poaching, transnational repression, talent recruitment programs, foreign research collaborations, and recruitment for espionage
- Information on indicators of potential threats, including elicitation, insider threats, and cyber threats
- Risk mitigation strategies for institutions and individuals

In addition to the bulletin, quick-reference guides are available for both institutions and researchers.

Professional Association Resources & Meeting Reports

COGR Updates to Research Security Quick Reference Table

On August 22, 2025, COGR announced its most recent update to the "Quick Reference Table of Current & Upcoming Federal Research Security Requirements." The latest version includes updates to reflect:

- The Department of Defense's (DOD's) updated "Component Decision Matrix to Inform Fundamental Research Proposal Mitigation Decisions"
- Updates to the Department of Energy (DOE) FAQ for required research security training
- The National Institutes of Health (NIH) announcement of required training on Other Support disclosure for all senior/key personnel
- Requirements included in the National Science Foundation's (NSF's) Important Notice No. 149, including: maintaining supporting documentation for activities included in researchers' current and pending (other) support; research security training (satisfied by the SECURE Center Consolidated Training Module) and certification by senior/key personnel and proposing institutions
- The United States Department of Agriculture (USDA) "America First Memorandum for USDA Arrangements and Research Security" (for additional information, see SECURE Center Briefing No. 6, August 7, 2025)

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.

MD Anderson Researcher Accused of Stealing Cancer Data, Trying to Take it to China
(Houston Chronicle, 8/25/2025) "Yunhai Li, 35, was charged with theft of trade secrets, a felony, and tampering with a government record, a misdemeanor, according to the Harris County District Attorney's Office. Li began working for MD Anderson in 2022. He was in the U.S. on a research scholar visa and was conducting breast cancer vaccine research funded by the National Institutes of Health and the Department of Defense." (more)

International Research Security Policy & Resources

ASPI Announces Tracker Update

The Australian Strategic Policy Institute (ASPI) announced they will be releasing an updated version of their widely referenced and used "China Defense Universities Tracker." From the announcement: "Developed by ASPI's Cyber, Technology & Security Program, the Tracker is a global reference tool for governments, research institutions and companies seeking to understand the military, security and technology risks linked to Chinese universities and research bodies." Release is anticipated in September 2025. (more)

Research Security-Related Events & Conferences

National Academies "Assessing Research Security Efforts in Higher Education - Meeting of Experts 2"

Following a two-day public workshop in May 2025, the National Academies will be holding its second "Assessing Research Security Efforts in Higher Education – Meeting of Experts" on Thursday, September 4, 2025, from 1:00-4:30pm. Convened by the Department of Defense, subject matter experts from universities and federal agencies will gather to discuss research security efforts, including potential measures of effectiveness and institutional perspectives. The meeting will be held in-person in Washington DC, with some portions available via webcast (registration required). (more)

FDP Virtual Meeting September 2025:

Monday, 9/15 - Wednesday, 9/17, 2025. Registration is now open for the Federal Demonstration Partnership (FDP) Virtual September 2025 meeting, taking place Monday, September 15th (11 AM ET – 5 PM ET), Tuesday, September 16th (11 AM ET – 5 PM ET) and Wednesday, September 17th (11 AM ET - 2 PM ET). (more)

COGR October Meeting 2025:

Thursday, 10/23 - Friday 10/14, 2025. Registration is now open for October 23-24, 2025 COGR meeting in Washington D.C. at the Washington Marriott in Georgetown. (more)

Save the Date for ASCE 2026:

Tuesday 2/24 - Thursday 2/26, 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. **Proposals are being accepted through noon (CST) on August 31, 2025** (more)

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

Sign up Here!

NSF SECURE Center Research Security Briefing

Vol. 1 No. 10: September 4, 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

Maximizing and Safeguarding NIH's Investment in Foreign Collaborations:

On August 25, 2025, National Institutes of Health (NIH) Director, Dr. Jay Bhattacharya issued a statement delineating the agency's mission in the context of international activities, specifying that NIH "conducts and supports international research because responsible global collaboration can drive scientific progress. However, NIH is not a foreign aid organization and support of international research should deliver both scientific and taxpayer value, as NIH is also tasked with being good stewards of U.S. taxpayer dollars." Therefore, NIH is adopting two fundamental principles regarding research activities conducted outside the U.S.:

1. “All research supported at international sites should have a clear scientific rationale to be conducted in a foreign country rather than in the United States.”

2. “All research supported at international sites should have direct potential to generate knowledge applicable to understanding, improving, or protecting the health of Americans.”

Professional Association Resources & Meeting Reports

NCURA Annual Meeting Reports

At the 67th annual NCURA meeting in Washington DC, August 10 - 13, 2025, several events involved or were related to research security. Presenters from these sessions have provided a post-meeting summary.

Building Capacity to Manage RISC: Investing in Research Integrity, Security, and Compliance at Mid-Sized and Smaller MSIs and HBCUs

Presenters:

- Dr. Melissa Harrington, PhD, Assoc. Vice President for Research, Delaware State University
- LaKeisha Harris, PhD, Dean, School of Graduate Studies, University of Maryland Eastern Shore
- Michael Miller, Asst. Director of Research Security and Integrity, Office of Research Protections & Compliance, University of Maryland Baltimore County
- Keyshawn Moncrieffe, PhD, Special Assistant (Business & Public Affairs), Research & Economic Development, Morgan State University

Summary provided by the panelists along with Christine Mallinson, PhD, Assistant Vice President for Research and Scholarly Impact, University of Maryland Baltimore County, Grant Principal Investigator.

“Building Capacity to Manage RISC: Investing in Research Integrity, Security, and Compliance at UMBC through Practices, Processes, and Partnerships” is a project funded by a 5-year award from the National Science Foundation. In a partnership among the University of Maryland, Baltimore County (UMBC), University of Maryland, Eastern Shore (UMES), Morgan State University (MSU) and Delaware State University (DSU), the project is developing best practices, guidance and training resources for building compliant yet flexible research security programs for smaller to mid-sized universities.

Following an overview of the federal regulatory landscape, the four partnering institutions discussed how they are implementing compliance protocols to meet federal requirements. For example, MSU described their phased implementation plan—cybersecurity, export controls, foreign travel, and research security—emphasizing project management structures and communication strategies. Each institution emphasized a need for charting clear goals for training and policy alignment and working with other units.

The presenters also identified several key issues facing smaller to mid-sized universities and colleges in today’s challenging regulatory environment, including challenges tied to international collaborations, export controls, and travel oversight. Both DSU and UMES discussed barriers and

opportunities for compliance infrastructure at smaller HBCUs. For example, although resource constraints and complex regulatory changes are a common challenge, opportunities lie in cross-institutional collaboration, in developing adaptable materials and training resources, and in building strong regional and national networks, all of which are key goals of the current collaborative project.

Navigating Security, Openness, and Inclusion in Global Research

Presenters:

- Lori Schultz, Asst. VP for Research Administration, Colorado State University (in-person)
- David Ribes (virtual)

This session explored how universities and researchers can balance the demands of research security, open science, and inclusive collaboration in an increasingly global research environment. David's contributions focused on strategies for navigating security and openness, developing new languages for inclusion, and supporting both domestic and international partnerships. Lori focused on how research administrators help researchers navigate both policies and laws that inform openness and security like data management and sharing, export control, research security, and federal/institutional anti-discrimination requirements. Drawing from policy analysis and case studies, we examined how institutions can uphold integrity and compliance while fostering equitable and collaborative research practices. Participants spanned research organizations and institutions of higher education in the United States and in other countries. A lively Q&A followed in which participants expressed interest in the SECURE Values Areas and appreciation for the weekly briefings. Attendees also discussed their concerns about how the current federal landscape will change what makes research work: funding, inclusion of international partners, student enrollment, and more.

Research Security Programs: Agency Implementations and the Road to Compliance

Presenters:

- Elizabeth Peloso, Sr. Vice Provost & Sr. Assoc. Vice President for Research at the University of Pennsylvania
- Kristin West, Director for Research Ethics & Compliance at COGR

A session on recent research security updates and institutional efforts in establishing research security programs was provided. The presentation covered the following new agency requirements:

(a) NSF's new research security training and research security assessment/recipient supporting documentation requirements from Important Notice 149 [also see SECURE Center Research Security Briefing No. 3];

(b) NIH's new disclosure requirements training set forth in NOT-OD-25-133 [also see SECURE Center Research Security Briefing No.4]; and

(c) the research security requirements in USDA's "America First Memorandum for USDA Arrangements and Research Security" [also see SECURE Center Research Security Briefing No.4].

Presenters also discussed research security implications of the Department of Justice's recent

regulations on the transfer of U.S. persons' bulk sensitive personal data to countries of concern and Covered Persons and the Executive Order on Improving the Safety and Security of Biological Research. The presenters and the audience then engaged in a robust discussion of challenges academic institutions face in this area stemming from lack of agency harmonization and a continuing/worsening lack of resources, as well as concerns about whether the federal government is truly supportive of continuing international collaborations and institutions' willingness to engage in such collaborations given the ever-increasing barriers to participation.

Research Security and Export Controls for the Research Administrator

Presenters:

- Jessica Buchanan, Senior Director of Research Security and Export Compliance at the University of Pennsylvania
- John Jenkins, Director of Research Security at Princeton University
- Elizabeth Peloso, Sr. Vice Provost & Sr. Assoc. Vice President for Research at the University of Pennsylvania

A workshop was conducted in which participants explored the overlap between Export Controls and Research Security as well as where they diverge. In addition to describing the elements of Research Security programs, the workshop participants explored their role, as a research administrator, in maintaining research security at their institutions. Participants also joined in discussions on how best to leverage existing practices and resources at their institution to support fledgling Research Security programs, as well as discussion of roles and responsibilities across the institution for implementing Research Security programs. With participants from both research-intensive institutions as well as small, primarily undergraduate institutions, the workshop included discussions around practices and strategies research administrators can use to assist in supporting research security at their institutions.

Additional NCURA details and meeting program information are available here.

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.

The National Academies Releases the Report, *Simplifying Research Regulations and Policies: Optimizing American Science*, Addresses Research Security

The National Academies Committee on Improving Regulatory Efficiency and Reducing Administrative Workload to Strengthen Competitiveness and Productivity of U.S. Research published its report, *Simplifying Research Regulations and Policies: Optimizing American Science* on September 3, 2025. The Committee "conducted an expedited study to examine federal research regulations and identify ways to improve regulatory processes and administrative tasks, reduce or eliminate unnecessary

work, and modify and remove policies and regulations that have outlived their purpose while maintaining necessary and appropriate integrity, accountability, and oversight."

The report highlights "a dramatic rise in regulations, policies, and requirements over time" and "excessive, uncoordinated, and duplicative policies and regulations surrounding research" that "are hampering progress and jeopardizing American scientific competitiveness". Many options are presented for the federal government to address these growing requirements and issues with coordination and duplication, as well as the pros and cons of each option.

Topics addressed include:

- Grant Proposals and Management
- Research Misconduct
- Financial Conflict of Interest in Research
- Protecting Research Assets, which includes Research Security, Export Controls, and Cybersecurity and Data Management
- Research Involving Biological Agents
- Human Subjects Research and,
- Research Using Nonhuman Animals

Overarching options to address issues include:

- Establishing a permanent career role in OMB [Office of Management and Budget] that is charged with coordinating cross-agency requirements that affect federally funded academic research and has the authority to ensure agency coordination, working collaboratively with OIRA [Office of Information and Regulatory Affairs], OSTP [Office of Science and Technology Policy], and using the NSTC [National Science and Technology Council] to institute harmonization.
- Reauthorizing the creation of a Research Policy Board within OIRA, granting it similar composition and authorities to those outlined in the 21st Century Cures Act.
- Using the Federal Demonstration Partnership (FDP) to explore innovative ideas and practices through pilot programs, establishing low-risk processes for testing innovative approaches to increase harmonization and use of approaches that are tiered to risk.

Among the options to protect research assets are:

- Implement the National Security Presidential Memorandum-33 (NSPM-33) common disclosure forms and disclosure table, without deviation, as the primary means to identify and address Conflicts of Commitment (COCs) and develop federal-wide FAQs via the interagency working group; in addition, use the Science Experts Network Curriculum Vitae (SciENcv) system, persistent identifiers (PIDs), and application programming interfaces (APIs) across research funding agencies.

- Establish common principles for agency research security risk reviews for fundamental research.
- Continue prior efforts, chiefly the Export Controls Reform Initiative, to streamline and clarify export controls and reduce associated administrative work, with representation from the academic research community and expedite licensing processes for low-risk controlled research.
- Adapt cybersecurity requirements for university settings: direct NIST (National Institute of Standards and Technology], in collaboration with OSTP and the broader research community, to undertake a comprehensive review of cybersecurity controls as they apply to institutions of higher education and make appropriate modifications to ensure alignment with the academic research environment.

The report notes the efforts of the SECURE Program, Center and Analytics, including that "This organization, established in September 2024 and now known as the SECURE Program, including the SECURE Center and SECURE Analytics, serves to connect the research community and collectively design and develop resources and tools to address research security risks and federal agency research security requirements. Although it is relatively new and its evaluation is ongoing, the SECURE Center could be a model for community codesigned resources that facilitate coordinated implementation across institutions." Related to the Center, the report includes the following option:

- Use the Safeguarding the Entire Community of the U.S. Research Ecosystem (SECURE) Center as an interactive research security information hub to keep the community current on the latest information and provide resources to facilitate consistent implementation of research security requirements across institutions.

And within the option to "Amend the CHIPS and Science Act to allow for 'just-in-time' research security training," that to reduce the annual training hours required by current policies, agencies could subscribe to the SECURE Center's condensed research security training module and broadly accept and apply an investigator's completion of said module as satisfying the agency's security training requirement. The full report can be found here.

NSF SECURE Analytics Releases Webinar on China's Science & Technology Shift

(August 8, 2025): "The government of China is overhauling its science and technology (S&T) ecosystem in ways that are sharpening geostrategic rivalry and impacting the risk portfolios managed by research security professionals. A new NSF SECURE Analytics Advisory outlines the geopolitical and security stakes for the United States. (more)

Research Security-Related Events & Conferences

National Academies "Assessing Research Security Efforts in Higher Education -Meeting of Experts 2"

Following initial meetings in September 2024 and a two-day public workshop in May 2025 and a meeting in September 2024, the National Academies will be holding another "Assessing Research Security Efforts in Higher Education – Meeting of Experts" session on Thursday, September 4, 2025. Convened by the Department of Defense, subject matter experts from universities and federal

agencies will gather to discuss research security efforts, including potential measures of effectiveness. The meeting will be held in-person in Washington DC, with some portions available via webcast (registration required). (more)

FDP Virtual Meeting:

Registration is now open for the Federal Demonstration Partnership (FDP) Virtual September 2025 meeting, taking place Monday, September 15th (11 AM ET – 5 PM ET), Tuesday, September 16th (11 AM ET – 5 PM ET) and Wednesday, September 17th (11 AM ET - 2 PM ET). While the agenda is still being finalized, potential sessions include:

- Federal Research Security
- Research Security – Update on Cybersecurity Framework
- Updates from the NSF SECURE Center

COGR October Meeting:

Registration is now open for our October 23-24, 2025 meeting in Washington D.C. at the Washington Marriott in Georgetown. **"Early Bird" registration price is available until September 16th**. (more) Preliminary agenda topics include:

- Simplifying Research Regulations and Policies: Optimizing American Science: A NASEM Report (also see above)
- 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. through noon (CST) on August 31, 2025. **Proposal deadline extension: Proposals are now being accepted through September 12, 2025** (more)

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

NSF SECURE Center Research Security Briefing

Vol. 1 No.11: September 11, 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

NIH Issues Notice on Implementation of Research Security Policies

On September 11, 2025, the National Institutes of Health (NIH) issued NOT-OD-25-154, "Implementation of Research Security Policies." The notice provides information on NIH's implementation of requirements for covered institutions and individuals regarding research security programs (RSPs), research security training (RST) and the prohibition of malign foreign talent recruitment programs (MFTRPs), in alignment with National Security Presidential Memorandum-33 (NSPM-33) and the CHIPS and Science Act of 2022.

Effective January 25, 2026:

Research Security Programs

- Covered institutions (i.e., participants in the U.S. R&D enterprise receiving federal science and engineering support "in excess of $50 million per year) must certify to the NIH that the institution has established and operates a research security program (RSP). RSPs must include the four elements required under NSPM-33: (1) cybersecurity; (2) foreign travel security; (3) research security training; and (4) export control training, as appropriate.

This is an interesting update because agencies have indicated that they are working on coordinated implementation of the RSP requirements under a memorandum of agreement and have not yet released the requirements for e.g., foreign travel security or cybersecurity or coordinated implementation of training requirements. Cybersecurity guidelines are currently being developed cooperatively with federal agencies and the research community via a Federal Demonstration Partnership cybersecurity demonstration. Clarification will need to be sought as to how institutions will certify that they have an established and operational RSP that meets the NSPM-33 requirements by January 25, 2026, as requirements have not yet been published, and institutions will need time for implementation.

Research Security Training

Regarding the research security training, the notice indicates that:

- "NIH fully supports the NSF online research security training (RST) modules which includes a condensed version of the four modules at the SECURE Center." Per the notice, applicant institutions may utilize any training that addresses cybersecurity, international collaboration, foreign interference, and rules for proper use of funds, disclosure, conflict of commitment, and conflict of interest (the CHIPS Act requirements). The SECURE Center's condensed module meets these requirements.
- Proposing institutions must certify that all senior/key personnel in the proposal have completed RST within the 12-months prior to submission of the application. This certification will be provided to NIH via an electronically signed PDF uploaded to the proposal at the time of submission.
- NIH is also including Annual Certification at the time of the Research Performance Progress Report (RPPR). Per the notice, "Individuals serving as senior/key personnel must continue to

certify annually that they have completed training within the past 12 months." At this time, this annual requirement for active awards has not been implemented by other federal agencies.

This notice does not reference NOT-OD-25-133 issued July 17, 2025. This 9/11/2025 notice could be seen as superseding that initial communication. NIH has communicated in presentations and informal communications that their training requirements do not deviate from those of NSF. This presumes the January 25, 2026, implementation date replaces the previously indicated October 1, 2025, implementation date, although this is not explicitly stated. Further clarification will be required.

Malign Foreign Talent Recruitment Programs

- Proposing institutions must certify that all senior/key personnel have been made aware of the MFTRP requirement, and certified that their personnel are not a party to an MFTRP.
- Per NIH, senior/key personnel will continue to certify via the Biosketch that they are not party to an MFTRP. At the time of the annual RPPR, senior/key personnel will recertify that they are not a party to an MFTRP.

Preview of NIH Common Forms for Biographical Sketch and Current and Pending (Other) Support Coming Soon to SciENcv

On September 4, 2025, the National Institutes of Health (NIH) issued notice NOT-OD-25-152, informing the community that the agency plans to release *preview* versions of NIH's Common Forms for Biographical Sketches (Biosketches) and Current and Pending (Other) Support in the Science Experts Network Curriculum Vitae (SciENcv) system.

Access to the preview versions is purely for informational purposes and applicants/recipients may not submit documents to NIH that were created using the preview functionality. Applicants/recipients must continue to use the current NIH Biosketch and Other Support forms until NIH officially implements its Common Forms, which the agency anticipates will occur in November 2025. (more)

NSF Issues First Round of Research on Research Security (RORs) Awards

The National Science Foundation (NSF) recently issued its first round of awards through the agency's Research on Research Security Program (RORs). The awards were issued to 12 recipients in 10 different states and include examples of three types of proposals accepted by RoRs for fiscal year 2025:

- EArly-concept Grants for Exploratory Research (EAGERs)
- Planning proposals to support initial conceptualization, planning and collaboration Activities
- Workshops and conferences

NSF's RORs Program "supports interdisciplinary, evidence-based research to enhance understanding of security risks, practices and policies to safeguard the U.S. research enterprise and foster a strong

academic field in research security."

DoD Publishes Federal Rule for DFARS CMMC 2.0 Standards

In the September 10, 2025, Federal Register, the Department of Defense (DoD) issued a final rule amending the Defense Federal Acquisition Regulation Supplement (DFARS) to incorporate contractual requirements related to the final Cybersecurity Maturity Model Certification (CMMC) program rule. The new rule will formalize the ability of the DoD to include CMMC requirements as a condition of contract award, to include either Federal Contract Information (FCI), Controlled Unclassified Information (CUI), or both. The latter in particular will require demonstrated compliance with the NIST 800-171 standard, as well as organizational attestation to ongoing compliance maintenance. In the short term, a self-assessment may be acceptable, but requirements for third-party assessment are possible and will become a requirement when Phase 2 of the rule starts next year.

Professional Association Resources & Meeting Reports

National Academies Meeting of Experts and Workshop Proceedings on Research Security Requirements

The National Academies convened a Meeting of Experts on September 4, 2025 to build upon and conclude previous discussions on Assessing Research Security Efforts in Higher Education that included input from the broader community through a two-day workshop in May. The proceedings of the May workshop are now available here.

The meeting and workshop series considered the impacts of research security requirements on U.S. research and development, including global leadership in the key technology areas where research protections are often sought, and identification of potential measures of effectiveness and impact and the data needed to assess this. The September 4 meeting, a continuation of proceedings from May, brought together leaders in the research security space from federal research funding agencies and academia for a discussion on measures and data identified during the workshop and how the Department of Defense, other federal research funding agencies, and the broader research community might proceed in assessing the near- and long-term impact of the research security requirements and processes that have and continue to be implemented.

Participants noted that the situation is becoming more complex and discussed measuring changes in culture, including a culture of responsible international collaboration and data sharing, and how to measure these changes through available data and using automated means for collection that don't unnecessarily increase administrative workloads. There was discussion on capturing the flow and collaboration of people engaged in U.S. research and development at all levels, changes in trends, and why these trends are occurring, as well as sources of existing data and where additional data might be collected. As an example, the National Center for Science and Engineering Statistics, Science and Engineering Indicators was mentioned as a key source of information.

The SECURE Center was mentioned several times as a potential source of data to measure the effectiveness of research security efforts, as well as providing possible methods for reducing the

burden associated with security efforts and enhancing consistency across government and academic partners. The SECURE Center was represented by Lori Schultz (Southwest Center Director), Lisa Nichols (Senior Advisor), and Amanda Humphrey (Northeast Center Director).

The meeting concluded with a sense of the need for ongoing discussions in this space.

AIRI Meeting Report, September 2025

SECURE Center Senior Advisors Jim Luther and Lisa Nichols led two sessions at the September 8, 2025, Association of Independent Research Institutes meeting. The first focused on the Center's community-centered design approach and the resources and products being developed to support the research community. Products from year 1, the upcoming release of the Shared Virtual Environment, and a number of resources including travel briefings and checklists and risk analysis tools were discussed and previewed. Non-profit research institutions are specifically identified in the CHIPS and Science Act legislation to co-develop these solutions.

Federal agency research security leaders including Sarah Stalker-Lehoux, Acting Chief of Research Security, Strategy and Policy, NSF and Jeannette Singsen, Senior Advisor, Office of Research, Technology, and Economic Security, DOE, provided agency-specific updates and perspectives on research security. Although Michelle Bulls, Director, Office of Policy for Extramural Research Administration, National Institutes of Health, NIH was unable to participate. An NIH presentation was provided.

NIH noted plans to launch preview versions of the NIH Common Forms within Science Experts Network Curriculum Vitae (SciENcv) by September 15, 2025. Per the presentation materials, these are not the official final versions. NIH will issue a subsequent Guide Notice to announce the final version once clearance is obtained from the Office of Information and Regulatory Affairs.

The presentation materials also *indicated that NIH will issue a guide notice this week* on the requirement for senior/key personnel to complete Research Security Training (RST). Consistent with DOE's implementation and NSF's planned implementation, the requirement will include certification that each senior/key personnel has completed RST within 12 months of application submission. NIH previously indicated that the implementation date for training will be October 1, 2025. Per NIH, annual certification will be required in the RPPR. An annual certification has not been proposed by other agencies at this time.

NSF noted the agency's planned October 10, 2025, implementation of mandatory research security training and that, per NSF's Important Notice 149, NSF, NIH, DOE, and DoD recognize the SECURE Center's one-hour condensed training module as meeting the agencies RST requirements. NSF has also linked to the condensed module on their training webpage. Sarah Stalker-Lehoux noted that USDA will also recognize the condensed training module as meeting their requirements and that while the four longer modules currently remain on the NSF website, they will not be updated. NSF also noted its Annual Certification Requirement Regarding Prohibition on Participation in Malign Foreign Talent Recruitment Programs is now In Effect. NIH is also implementing this requirement.

Jeannette Singsen indicated that DOE anticipates implementing the Common Current and Pending Support and biosketch forms via SciENcv in October for all NOFOs and awards. Covered individuals

(senior key personnel) will need to certify that they have taken research security training within the last 12 months and that they are not currently participating in a malign foreign talent recruitment program. Regarding transparency of foreign connections, DOE has a new suggested (but optional) template. The template can be found here.

U.S. Congressional Activity

Fox In the Henhouse: the U.S. Department of Defense Research and Engineering's Failures to Protect Taxpayer-Funded Defense Research

On September 5, 2025, the U.S. House of Representatives Select Committee on the Chinese Communist Party (CPP) and the Committee on Education and the Workforce issued a report, "Fox In the Henhouse: the US Department of Defense (DOD) Research and Engineering's Failures to Protect Taxpayer-Funded Defense Research." The report suggests that:

> *The persistent occurrence of joint publications by DOD-funded personnel with Chinese defense-affiliated entities suggests systemic failures in research security oversight, grant due diligence, risk mitigation within federally funded research programs, and compliance and monitoring post-award during research grants' period of performance. This underscores an urgent need for strengthened research security measures, standardized risk assessments, and prohibitions against collaborations with foreign military-industrial entities in federally funded research.*

In addition to a large number of case studies, the report includes 14 recommendations—mainly directed toward DOD's research security policies, processes, and systems. The report also recommends adoption of the *Securing American Funding and Expertise from Adversarial Research Exploitation Act of 2025 (SAFE Research Act)*, proposed by Rep. John Moolenaar (R-MI), Chairman of the Select Committee on the CPP. The proposed legislation is linked under Appendix A of the report.

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.

CISA pushes final cyber incident reporting rule to May 2026 (Cyberscoop, 9/8/2025) According to a report on the Office of Management and Budget (OMB) website, the Cybersecurity and Infrastructure Agency (CISA) is delaying finalization of terms for cyber incident reporting until May 2026. The rule affects a variety of industries and further input is being sought by the agency. (more)

NASA bans Chinese nationals from working on its space programmes (BBC, 9/11/2025) According to a report from the BBC, as of September 5, 2025, they lost all access to NASA system and facilities on the basis of national security concerns.(more)

Research Security-Related Events & Conferences

FDP Virtual Meeting:

Registration is now open for the Federal Demonstration Partnership (FDP) Virtual September 2025 meeting, taking place Monday, September 15th (11 AM ET – 5 PM ET), Tuesday, September 16th (11 AM ET – 5 PM ET) and Wednesday, September 17th (11 AM ET - 2 PM ET). While the agenda is still being finalized, research security-related sessions tentatively include:

- Expanded Clearinghouse Subcommittee - Research Security & SubAwards: 9/16, 2:30 – 3:40 PM ET
- FDP Demonstration to Develop Cybersecurity Guidelines for Federal Research Security Program Requirements: 9/16, 3:55 – 5:00 PM ET
- GRANTED Session presenting on two projects related to research administration workforce development and research security: 9/16, 3:55 – 5:00 PM ET
- Federal Research Security Panel: 9/17, 11:00 AM – 12:15 PM ET
- Simplifying Research Regulations and Policies: Optimizing American Science, from recently released National Academies Report – includes options for assessing administrative workloads associated with research security requirements: 9/17, 1:45 – 3:00 PM ET
- The SECURE Center: Solutions and Initiatives to Empower the Research Security Community: 9/17, 3:15 – 4:15 PM

COGR October Meeting:

Registration is now open for our October 23-24, 2025 meeting in Washington D.C. at the Washington Marriott in Georgetown. **"Early Bird" registration price is available until September 16th**. Preliminary agenda topics include:

- Simplifying Research Regulations and Policies: Optimizing American Science: A NASEM Report (also see above)
- 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. through noon (CST) on August 31, 2025. **Proposal deadline extension: Proposals are now being accepted through September 12, 2025** (more)

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

Sign up Here!

NSF SECURE Center Research Security Briefing

Vol. 1 No. 12: September 18, 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

New Application Structure for NIH-Funded International Collaborations

On September 12, 2025, the National Institutes of Health (NIH) issued NOT-OD-25-155, "New Application Structure for NIH-Funded International Collaborations," providing additional information on the agency's new process for handling foreign components, as NIH announced in NOT-OD-25-104 that the agency would not issue awards for proposals that include subawards to foreign entities.

Under the process described in NOT-OD-25-155, competing applications that include one or more foreign components must submit to a Notice of Funding Opportunity (NOFO) that supports a complex mechanism activity code, including two new international project "parent" activity codes that NIH is creating: PF5 for grants and UF5 for cooperative agreements.

- NIH anticipates the new application structure being available for the January 2026 application submission cycle.
- Applications will be submitted and reviewed as a whole.
- For those applications being considered for funding, the international components will be disaggregated, and each will be assigned its own grant number with an activity code of RF2 (for grants) or UL2 (for cooperative agreements). Each RF2/UL2 will be considered its own applicant/recipient for the associated grant or cooperative agreement.
- NIH will request Just-In-Time (JIT) information from the domestic "parent" entity and any foreign components independently. If not already completed, the international project components must verify registration in SAM.gov, grants.gov, and eRA Commons.
- Each recipient organization will be responsible for its own financial reporting.
- Additional details regarding progress reporting (e.g., RPPRs) and terms and conditions of the Notice of Award will be forthcoming.
- For existing submissions, NIH is looking into a system-based mechanism of converting applications to fit the new structure, but resubmission by applicant organizations is a possibility.
- NIH will be providing additional resources, FAQs, and training for the new activity codes and application structure.

Department of Education OIRA Posting Signals HEA 117 Rule Change

The Department of Education recently posted a notice on the Office of Information and Regulatory Affairs reginfo.gov website indicating that the "Department intends to propose regulations covering institutions' reporting of statutorily defined gifts, contracts, and/or restricted and conditional gifts or contracts from or with defined foreign sources, pursuant to the requirements of section 117 of the Higher Education Act of 1965, as amended (HEA)."

Professional Association Resources & Meeting Reports

The SECURE Center and AIRI: Partnering with Nonprofit Research Institutions

In a session at the Association of Independent Research Institutes, SECURE Center Senior Advisors Jim Luther and Lisa Nichols shared community feedback gathered from AIRI's June Discovery Co-creation Stakeholder Activities (CSAs), which engaged fifteen member institutes. The session was moderated by Rosemary Madnick, Vice President for Research Administration, Lundquist Institute for Biomedical Innovation. Additional insights were gathered in a follow-up discussion with participants to further inform the next phase of resource development.

Several AIRI session participants agreed with the need for guidance expressed in the earlier CSAs on how to approach research security for faculty who are affiliated with multiple U.S. based research entities. Researchers have academic appointments through universities and research institutes and may have multiple appointments, making it challenging to track completion of requirements such as training. Tracking training through the SECURE Center's Shared Virtual Environment would help to reduce the burden associated with these arrangements. There was discussion on how to consolidate training to reduce burden, and participants echoed interest in free tools similar to Visual Compliance. There was discussion on the federal Consolidated Screening List Search Engine which participants were not aware of, but also that this free tool wouldn't provide dynamic (continuous) screening. Participants expressed that step by step guidance on how to be at least minimally compliant would be helpful as well as other free resources including in relation to foreign travel.

These discussions will help inform the SECURE Center's year 2 planning for the design and development of new resources and tools. Opportunities for continued engagement were discussed.

FDP Virtual Meeting, September 15-17

Reports from the Research Security-related sessions at the September 2025 Federal Demonstration Partnership (FDP) virtual meeting will be provided in next week's Briefing, Vol 1, No 13.

U.S. Congressional Activity

U.S. House Committees Report: Joint Institutes, Divided Loyalties

On September 11, 2025, the U.S. House of Representatives Select Committee on the Chinese Communist Party (CPP) and the Committee on Education and the Workforce issued a report, "Joint Institutes, Divided Loyalties." The report, written largely in follow-up to the Committees' September 2024 report, "CCP on the Quad," suggests that:

> *U.S.-PRC joint institutes are entities based in China that pair American universities with PRC institutions and serve as key technology transfer points. These joint institutes operate under PRC law, are run by Chinese majority boards, and are aligned with the CCP's national strategy, including its military buildup.*

Similar to the Committees' other recent report, "Fox in the Henhouse: the U.S. Department of

Defense Research and Engineering's Failures to Protect Taxpayer-Funded Defense Research," this report also recommends adoption of the *Securing American Funding and Expertise from Adversarial Research Exploitation Act of 2025 (SAFE Research Act)*, proposed by Rep. John Moolenaar (R-MI), Chairman of the Select Committee on the CPP (also see Research Security Briefing No. 11).

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.

Former Defense Contractor Sentenced to Over 10 Years in Prison for Attempted Espionage (U.S. Department of Justice, 9/15/2025)

John Rowe Jr., a former defense contractor who acted as an insider threat, used his nearly 40 years of experience and access to highly classified U.S. military information to attempt to share sensitive national defense secrets with someone he believed to be a Russian agent. Rowe pleaded guilty to multiple charges of attempted espionage, including delivering and willfully communicating classified information. Despite his trusted position and security clearances, he repeatedly betrayed U.S. national security, exchanging over 300 emails and disclosing classified details in meetings with an undercover FBI agent. Rowe was sentenced to 10 years in prison. (more)

Trump administration escalates space race with China, banning visa-holding scientists from working at NASA (CNN, 9/11/2025)

CNN reports that, effective September 5, 2025, "NASA has banned Chinese citizens with US visas from participating in agency programs… [and] are no longer allowed to have physical access to NASA facilities, to join Zoom calls with their NASA colleagues or access the agency's supercomputing resources." (more)

Alien from Wuhan, China Sentenced for Smuggling Biological Materials into the U.S. for Her Work at a University of Michigan Laboratory and For Lying About the Shipments (U.S. Attorney's Office, 9/10/2025)

On September 10, 2025, Chengxuan Han was sentenced to time served (3 months) after pleading guilty to smuggling charges and making false statements to U.S. Customs and Border Protection Officers. Ms. Han will also be removed from the United States and barred from re-entry. Han, a citizen of the People's Republic of China (PRC) and a PhD student at the Huazhong University of Science and Technology, Wuhan, sent packages from the PRC containing concealed biologic material related to roundworms, addressed to individuals associated with a lab at the University of Michigan. Han was arrested on June 8, 2025, after arriving at Detroit Metropolitan Airport on a J1 visa. (more)

Russian scientists' international collaborations to be vetted by security services under new law (*Science*, 7/17/2025)

"Russian universities and research institutions will soon be obliged to report all scientific collaborations with foreign citizens to the country's security services, who will have the ultimate say over whether those projects can go ahead.

The government says the new law, signed by President Vladimir Putin on 24 June, will allow the Russian Federal Security Service (FSB) to prevent the unauthorized transfer of scientific results outside of the country, 'without violating the freedom of scientific creativity and without creating obstacles for organizations to engage in scientific activities.'" (more)

International Research Security Policy & Resources

Recent Updates to Japanese and South Korean Research Security Policy

Japan and Korea are making great strides in research security. Stung by recent, well-publicized cases of foreign misappropriation of research in academia and industry, both countries have initiated multi-stakeholder processes to raise domestic awareness of research security risk, strengthen regulations, formulate best practices, and build analytical and administrative capacity. They are sending representatives to global research security conferences, inviting international experts to local workshops to exchange perspectives, and studying developments in Australia, North America, and Europe with care. In addition, research security features in the bilateral and multilateral (e.g. G7 and OECD) consultations between the Japanese and Korean governments and their key partners on critical and emerging technologies, scientific collaboration, export controls, and international security.

Korea is explicitly adopting a whole-of-government approach to research security. Its 2023 Industrial Technology Protection Act empowers the Ministry of Trade, Industry, and Energy to protect competitiveness and national security in core technologies and other products and services. Supporting legislation prioritizes twelve national strategic technologies. In 2024, the Ministry of Science and ICT released a Blueprint for National S&T Sovereignty that defines proactive measures for technological security as a key objective. The Blueprint calls for the establishment of research security guidelines for researchers, strengthened research security systems conducive to global joint research, and robust strategic partnerships with like-minded countries. Academic research security programs are now beginning to pilot the implementation of these initiatives in coordination with government. Japan has been a member of the G7 SIGRE (Security and Integrity of the Global Research Ecosystem) Working Group since 2021. It's Ministry of Education, Culture, Sports, and Technology (MEXT) will soon pilot an analogue to the NSF TRUST program in the areas of quantum and semiconductor technology to screen proposals for risks and promote tailored mitigation measures. MEXT is also establishing regional research security contact points for universities in coordination with other government departments, as well as training programs to raise awareness across universities and researchers. Meanwhile, Japan's Cabinet Office is preparing draft guidelines on research security that

will focus on sensitive research and a national contact point to support implementation. Finally, the Ministry of Economy, Trade, and Industry (METI) is enhancing Japan's export control regime.

These are just a few of the research security initiatives being pursued in both nations. Each regards balancing openness and security in alignment with its key international partners as paramount. Together, they promise to set new standards for the region.

Safeguarding Western Tech Startups: Exploitation of International Pitch Competitions (Government of Canada, 09/08/2025)

On September 8, 2025, the Canadian Security Intelligence Service in the Canadian Government posted information on potential concerns related to international pitch competitions, with a focus on those affiliated with the Chinese government or the Chinese Communist Party (CCP), and the associated risks to startup companies. They identify primary risks such as losing intellectual property, misuse of data, or having talented individuals recruited away along with other potential risks. Specific case examples are provided along with mitigation efforts that companies can take. (more)

Research Security-Related Events & Conferences

COGR October Meeting:

Registration is open for the COGR 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!

NSF SECURE Center Research Security Briefing

Vol. 1 No. 13: September 25, 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.

SECURE Center Updates & Resources

SECURE Center Consolidated Research Security Training Webpage and Updates

The SECURE Center has created a dedicated webpage for the consolidated research security training (RST) module. Information on the webpage has been updated to reflect current federal RST requirements and updated files and materials have been made available, including:

- An updated version of the module, condensed training module (CTM) 1.1, includes additional accessibility improvements for better compliance with Web Content Accessibility Guidelines Level AA standards.
- Changes were made to address potential completion tracking issues on interactive slides to accommodate slower server/client processing speeds for those who were experiencing challenges.
- CTM 1.1 has been made available for direct training on the website and provides a certificate of completion.
- Versions of the training with 4 and 6 customizable university-specific pages have been made available in response to stakeholder requests.

The Center will continue to update this webpage with the latest research security training requirements and resources.

Federal Agency News & Updates

Dr. Jon Lorsch Named NIH Deputy Director for Extramural Research

On September 18, 2025, Dr. Jay Bhattacharya, NIH Director, announced that Dr. Jon Lorsch has been confirmed as the NIH Deputy Director for Extramural Research (DDER). Dr. Lorsch has served in this role in an acting capacity since April 2025. He will advise the NIH Director on multiple issues related to NIH's extramural research program and administration. This office oversees NIH's research security efforts. (more)

Professional Association Resources & Meeting Reports

Federal Demonstration Project (FDP) September 2025 Meeting: Research Security Highlights

FDP Session: Federal Agency Updates

Presenters:
Stephanie vonFeck, Chief, Federal Assistance Planning Branch, Division of Grants Policy, HRSA
Priyanga Tuovinen, Senior Grants Policy Analyst, Office of Extramural Research, NIH
Mary Sladek, Senior Program Director, Science Mission Directorate, NASA

Kimberly Whittet, Senior Policy Advisor, NIFA
Laura Givens, Policy Branch Chief, Office of Grants and Financial Management, NIFA

Moderator: Michelle Bulls, Director, Office of Policy for Extramural Research Administration, NIH

National Institutes of Health (NIH)

Per NOT-OD-25-155, NIH has implemented a new application and award structure for applications requesting funding for a foreign component (FC). Competing applications with one or more FCs must submit applications to a complex mechanism notice of funding opportunity (NOFO) that supports International Project component type. Applications will be reviewed as a whole; however, Just-in-time (JIT) information will be requested separately, and separate—but linked—awards will be issued to the various components. Also see SECURE Briefing No. 12.

National Aeronautics and Space Administration (NASA)

NASA has adopted the format of the Common Forms for Biosketches and Current and Pending (other Support), which are available for download on the Agency's Grants Policy and Compliance site. For further training on NASA's use of these forms, an instructional video is available. NASA does not currently have an agreement in place to make these forms available via SciENcv.

FDP Session: Demonstration to Develop Cybersecurity Guidelines for Federal Research Security Program Requirements

On September 16, 2025, FDP held a session on a current Demonstration to Develop Cybersecurity Guidelines for Federal Research Security Program Requirements. The session was moderated by SECURE Center Senior Advisor Lisa Nichols, Executive Director of Research Security, University of Notre Dame, FDP Research Security Subcommittee Co-chair, and Cybersecurity Demonstration Lead. Speakers included:

- Sarah Stalker-Lehoux, Acting Chief of Research Security Strategy and Policy, NSF, and FDP RSS Co-chair
- Jarret Cummings, Senior Advisor, Policy and Government Relations, Educause
- Michael Corn, Former CISO, University of California San Diego, and Former Cybersecurity. Advisor for Research Infrastructure, NSF

Sarah Stalker-Lehoux provided background on cybersecurity requirements for fundamental research under the National Security Presidential Memorandum – 33 research security program (RSP) requirements, which apply to institutions receiving more than $50 million in federal awards. Per the White House Office of Science and Technology Policy July 2024 final guidelines, institutions will need to implement a cybersecurity program one year after publication of the final NIST cybersecurity resource (IR 8481: Cybersecurity for Research). The question for agencies was, what would institutions certify to?

Through an FDP demonstration, the Research Security Subcommittee, partnering with Educause, is

leading an effort to develop flexible, risk-based guidelines to address cybersecurity threats to research as part of federal RSP requirements. The guidelines are being developed collaboratively with community and federal agency partners and the engagement of knowledge experts representing a broad array of research organizations, programs, and roles.

Jarret Cummings provided an overview of what is covered in the research cybersecurity plan, including roles and responsibilities across institutional stakeholders, risk assessment (e.g., how to conduct, frequency) and mitigation. Implementation of the NSF Critical Controls Set was reviewed by Mike Corn. They include 14 basic controls such as multi-factor authentication, anti-malware, data backups, and others. Exceptions and compensating controls would be implemented as needed at the institutions' discretion. Additional information on the controls can be found here.

The working group anticipates sharing the draft guidelines with the broader FDP community later this month and providing the opportunity for feedback. The intent is to deliver the final guidelines to NSF and the federal interagency in the late-November/early-December timeframe.

FDP Session: Expanded Clearinghouse Subcommittee - Research Security & Subawards

Presenters:
Amanda Hamaker, Purdue University
Robert Prentiss, Yale University
Jennifer Rodis, University of Wisconsin-Madison
Taren Ellis Langford, University of Arizona
Jennifer Ford, University of California San Diego

The Expanded Clearing House (ECH) Subcommittee presented an overview on the purpose of the ECH (to reduce burden for commonly shared institutional data) as well as recent updates for the fdpclearinghouse.org institutional profiles. They noted there are currently 376 profiles in the database: 216 FDP members and 159 non-members (whose participation is fee-based). As context for the discussion, the Subcommittee presented background on:

- National Security Presidential Memorandum - 33
- Research Security Program requirements (noting the pending federal guidance on three of four areas: cybersecurity, foreign travel, and export control)
- The malign foreign talent recruitment program (MFTRP) prohibition in the CHIPS and Science Act of 2022
- A summary of the NSF SECURE Center

The ECH Subcommittee described its activities and its overlap with the Subawards Committee and the Subawards Committee's standardization initiatives for FDP membership.

Introductions were made to the 15 members of the Research Security & Subawards Working Group, co-chaired by Taren Ellis Langford, University of Arizona and Jennifer Ford, University of California San Diego. The purpose of the Working Group is to review the intersection of research security with ECH's areas, partnering with the Subawards and Research Security committees as needed. Initial focus

areas for this group include current requirements, a sustainable approach, the changing landscape, and identification of covered institutions.

The group presented on its goal to implement a new field in the ECH institutional profile to indicate NSPM-33 "covered institutions." Implementation is planned for January 2026. Discussion included possible identification of these institutions using the three-year average in the NSF Survey of Federal Science and Engineering Support to Universities, Colleges, and Nonprofit Institutions 2023 and pre-population by the FDP into existing ECH profiles. Many audience members agreed that this would be beneficial and reduce administrative burden, rather than having each institution populate the field. Attendees raised additional questions, including how to certify research security training for individuals, and concerns about smaller subawardees providing certification. A suggestion was made to revise the Letter of Intent (LOI) template to include text about research security and the MFTRP prohibition. The Committee chairs noted that, due to the variety of stakeholders involved in the LOI template review process, changes to the LOI template could take about a year and these suggestions were tabled for further consideration and possible updates at the January FDP meeting.

FDP Session: Recent Insights from NSF's GRANTED Program September 2025

Moderator/Hosts:
Susan Anderson, ERI Committee Co-Chair, College of Charleston
Dina Stroud, Program Director, Growing Research Access for Nationally Transformative Economic Development, National Science Foundation (NSF)

This session consisted of presentations from two GRANTED Project Teams:

- RISC and GRANTs Made: University of Maryland-Baltimore County (UMBC) Scholarly Impact
- Filling the Gap: University of South Alabama

Dina Stroud, NSF Program Director, began the session with an overview of the research enterprise, challenges faced, and where the GRANTED Program seeks to fill those gaps. The GRANTED Program provides funding opportunities for ideas that will: generate scalable models of sustainable capacity; create new collaborations and communities; increase the range of leadership and institutions funded; and strengthen engagement across the research enterprise. These funding opportunities are ongoing. Proposals should directly relate to the research support and service infrastructure ecosystem. The GRANTED themes and program descriptions were presented as well as an overview of past awards. Engagement with NSF staff during their office hours, to discuss potential proposal submissions, is strongly encouraged.

The University of Maryland-Baltimore County (UMBC) leadership team of Karl Steiner, Vice President for Research and Creative Achievement, and Christine Mallinson, Assistant Vice President for Research and Scholarly Impact, presented a summary of their grant, *Building Capacity to Manage RISC: Investing in Research Integrity, Security and Compliance at UMBC through Practices, Processes & Partnerships*. The goal of the project is to build scalable knowledge for research security infrastructure, which started at their own institution, including the development of materials and an institutional self-assessment to identify gaps. The extension of their partnership work with the

University of Maryland Eastern Shore, Delaware State University, and Morgan State University was highlighted. As part of their current year of funding they are conducting a survey to understand how institutions are addressing the evolving research security requirements. They invite compliance professionals from other institutions to visit their website to complete a brief survey.

The UMBC team also presented their work on *GRANTS MADE at Scale: Implementing a Regional Research Administration Student Internship Program in Maryland and Delaware* which create opportunities at several partnering institutions resulting in 52 interns trained by 2029 in research administration (one dedicated to research security), and where the interns will be connected with the NCURA Region 2 professional community in the course of their professional development.

Filling the Gap: Establishing an Undergraduate Program in Research Administration and Grant Management was presented by the team from the University of South Alabama (USA): Lynne Chronister, former Vice President for Research (retired), Project Director; Keone Fuqua, Program Manager Curriculum Design; and overall project leadership from Chris Brown, Vice President of Research at University of Alabama Birmingham (UAB). The program is designed to prepare the next generation of research administration professionals through the creation of an academic curriculum in research administration that forms the basis for a minor, concentration, or certificate, in conjunction with an undergraduate degree. A Research Administration and Management (RAM) curriculum has been developed and launched. Several key collaborators/ subawardees are assisting in development and/or assessment of the curriculum. At the time of the presentation, the University of Southern Alabama had accepted 19 out of its 25 anticipated partner institutions to implement the RAM curriculum at their institutions. To ensure content consistency and sustainability, the Society of Research Administrators International (SRAI) hosts the modules and then provides the technical files for incorporation into each institution's learning management system. The team noted that, after the grant period, SRAI will own and maintain the curriculum. For implementation, the team profiled some of the challenges to be addressed by each institution, including an institutional approval process, faculty credentials, state level approvals (if needed), and accrediting bodies. The University of Alabama Birmingham successfully launched the initial program for Fall Semester 2025 with 20 students in the cohort.

FDP Session: Federal Research Security Panel

On Wednesday, September 17, 2025, the FDP Federal Research Security (RS) session was moderated by SECURE Center Senior Advisors Jim Luther, Yale University, and Lisa Nichols, University of Notre Dame. Speakers included:

- Michelle Bulls, Director, Office of Policy for Extramural Research Administration, NIH, and Lead FDP Federal Representative
- Steve Ellis, Program Officer, Office of the Chief of Research Security Strategy and Policy, NSF
- Jeannette Singsen, Senior Advisor, Office of Research, Technology, and Economic Security, DOE

The session covered the latest updates from federal partners on RS topics of interest, including the implementation of the Research Security Program (RSP) standards, updates on agency- specific

activities, and other topics.

National Institutes of Health (NIH)

Common Forms

NIH has launched preview versions of the Common Forms within SciENcv (Science Experts Network Curriculum Vitae). These are not the final official versions. The goal is to allow users to preview the new functionality and instructions. NIH will issue a subsequent Guide Notice announcing the final versions once clearance is obtained from the Office of Information and Regulatory Affairs. That "uber" notice will include a great deal of information.

Training on Disclosure

Michelle Bulls provided further clarity regarding NOT-OD-25-133, *New Policy Requirement to Train Senior/Key Personnel on Other Support Disclosure Requirements*. Per the notice and presentation, institutions' internal controls (e.g., policies and procedures) for Other Support disclosure must include training for senior/key personnel on these policies and procedures. Although the notice does not relate to research security programs and is applicable to all NIH recipient institutions, NIH noted that NSF's research security training modules, the Secure Center's condensed training module (CTM) (endorsed by NIH and other agencies), or an institution's own training that meets the CHIPS Act and notice requirements can be used for Other Support disclosure training. The SECURE Center notes that additional blank slides have been made available at the end of the CTM (2, 4, or 6 slides) for institutions to include their specific policies, guidance, procedures, contacts and other relevant information. All are available on the SECURE Center's CTM webpage. Per Michelle Bulls, effective October 1, 2025, training on Other Support must be taken by all senior/key personnel at the time of research performance progress report (RPPR) or just in time (JIT) submissions.

Research Security Program Policy

The NIH presentation included the September 11, 2025, notice NOT-OD-25-154, *Implementation of NIH Research Security Policies*. NIH clarified that the agency is participating in a Memorandum of Agreement with NSF and other federal research funding agencies to develop a centralized process for recipients to certify compliance with the yet-to-be-published RSP requirements. NIH will issue more information on the central certification process and timing as it becomes available.

Effective January 25, 2026, NIH will require that institutions and senior personnel submitting applications for NIH funding certify that Research Security (RS) training has been completed within the previous 12 months. There was discussion during the session that the RS training and the malign foreign talent recruitment program requirements are not just part of the RS Program requirements but, separately, a requirement of the CHIPS and Science Act. Therefore, both requirements and certifications are applicable to all applicants or recipients of federal science and engineering awards, regardless of whether institutions meet the $50 million threshold for the RSP requirements, including subrecipients.

National Science Foundation (NSF)

Steve Ellis of NSF noted the agency's planned October 10, 2025 implementation of mandatory RS training and that, per NSF's Important Notice 149, NSF, NIH, DOE, and DoD recognize the SECURE Center's one-hour CTM as meeting the agencies' RS training requirements. USDA has also indicated the CTM will meet their requirements. Steve noted that while the four longer RS training modules currently remain on the NSF website, these modules will not be updated and recipients are encouraged to use the SECURE Center's CTM. NSF also noted its Annual Certification Requirement Regarding Prohibition on Participation in Malign Foreign Talent Recruitment Programs is now In effect.

Department of Energy (DOE)

Jeannette Singsen indicated that DOE anticipates implementing the Common Forms for Biosketches, Current and Pending (Other) Support and via SciENcv in October for all Notices of Funding Opportunities (NOFOs) and awards. There will also be a supplemental disclosure form for a subset of projects that will be built into SciENcv as well. Applicability for the supplemental disclosure form is based on the sensitivity of the technology. The supplemental disclosure focuses on foreign country of concern (FCOC) connections, with questions related to past FCOC support; past FCOC incentives, past collaborations at FCOC sites (excluding routine workshops or conferences hosted in FCOCs), patent applications filed in an FCOC without a companion US patent application, and FCOC military or intelligence service. If required, it will be indicated in the NOFO. Jeannette suggested DOE is taking a risk-based approach in terms of whether Current and Pending (Other) Support, the supplemental disclosure, and/or the transparency of foreign relations form are required.

Covered individuals (Senior/Key Personnel) will need to certify that they have taken RS training within the last 12 months and that they are not currently participating in a malign foreign talent recruitment program. New covered individuals added to the project after award/selection are required to certify they have taken the RS training within 30 days of joining the project. As indicated by other agencies, institutions can use their own RS training provided it meets the requirements in the CHIPS Act. There was discussion about whether other agencies would require the RS training annually, as NIH has stated. Jeannette indicated that it was likely, though not yet established, that the RS training would be required annually in association with Research Security Programs, but not for institutions with less than $50 million in federal science and engineering funding.

Regarding transparency of foreign connections (TFC), DOE has a new suggested (but optional) template which the agency indicates can make it easier to disclose. The template can be found here. Per the DOE presentation, updated TFCs must be submitted if information changes. For some awards, an updated TFC will be required as part of the continuation application.
Per statute, DOE continues to have a prohibition on individuals or entities on the 1260H or Commerce BIS Entity lists from participating on DOE proposals and awards. DOE recipients are encouraged to do due diligence to ensure collaborators are not on these lists. More information on DOE requirements and FAQs can be found on the DOE's RTES website.

FDP Session: Simplifying Research Regulations and Policies: Optimizing American Science

The FDP September 15-17, 2025, meeting included a briefing of the recently released National

Academies report, *Simplifying Research Regulations and Policies: Optimizing American Science* which presents options for federal actions to improve regulatory efficiency affecting researchers and their institutions. Alex Helman, Study Director, National Academies of Sciences, Engineering, and Medicine, served as the moderator. Speakers included committee members Lisa Nichols, University of Notre Dame, Stacy Pritt, Texas A&M University System, and Christopher Viggiani, Oregon State University.

The session provided an overview of past efforts to reform research regulations and policies, and cross-cutting principles, including harmonizing agency requirements, tiering them to risk, and using technology to simplify compliance. Several overarching options were presented to facilitate reform, including:

- Establishing a permanent function within the Office of Management and Budget, an *Assistant Director for Institutional Research Coordination and Community Engagement*, with the authority to coordinate cross-agency requirements
- Appointing a Federal Research Policy Board as previously authorized in the 21st Century Cures Act
- Using FDP to explore innovative ideas and practices through pilot programs. As agencies develop new models and innovative approaches, they could work directly with FDP to test and refine them before formal launch.

The report includes options covering a broad array of research administration and compliance areas. The FDP session covered recommendations on grant proposals and management, including: introducing a federal-wide, two-stage pre-award (letter-of-intent) process; eliminating expectations for filing financial disclosure statements at every transaction; and a centralized financial disclosure system. In the area of conflict of interest, creating a uniform federal FCOI in research policy or reverting to the previous $10,000 Public Health Services threshold.

In the area of protecting research assets, Federal-wide implementation of the NSPM-33 common disclosure forms and pre- and post-award table without deviation as the primary means to identify conflicts of commitment; using the SECURE Center as an interactive research security information hub; renewing the Export Control Reform Initiative with input from academia; and, adopting a risk-tiered approach to export controls.

The report explores ways to streamline research misconduct proceedings including the creation of a single, flexible federal misconduct policy to which all funding agencies defer, or the option to more clearly designate a lead agency to coordinate cases involving multiple funders.

The report also highlights the complexity of regulations governing research with biological agents and toxins. Leveraging successful oversight frameworks, it provides options for a more centralized, coordinated federal approach to biosafety oversight, through a single agency that registers and empowers institutional biosafety committees. The report also offers an alternative that would shift responsibility for identifying DURC and gain-of-function research to federal funders.

The session highlighted several options provided in the report to enable the USDA and NIH Office of Laboratory Animal Welfare (OLAW) to harmonize, streamline, and modernize their oversight

processes, including for NIH OLAW to adopt an online platform and streamlined approach for its Animal Welfare Assurance process.

The options presented aim to improve regulatory administrative processes and modify or eliminate policies and regulations that have outlived their purpose while maintaining necessary and appropriate integrity, accountability, and oversight.

FDP Session: The SECURE Center -- Solutions and Initiatives to Empower the Research Security Community

Moderator/Host: Steve Post, University of Arkansas for Medical Sciences

Speakers:
Mark Haselkorn, University of Washington
Sonia Savelli, University of Washington
Robert Nobles, Emory University
Lee Stadler, University of Missouri Kansas City

Sonia Savelli, SECURE Center Creation Director, led a demonstration of the SECURE Center's Shared Virtual Environment (SVE) and various research security resources related to foreign travel and travel-sensitive topics, including: Basic and High-Risk Travel Checklists, A Travel Resource Guide, and a Sample Travel Briefing to support the activities of both researchers and research security professionals.

On September 15, 2025, the SVE had its initial release for testing, marking the beginning of a Use Feedback Refine (UFR) process. UFR is an iterative approach designed to gather user insights that guide the development and refinement of the SVE. During the first week, 27 users, who are designated Research Security Officers for their institutions, participated in guided sessions to provide feedback on the SVE and its products. Their input is helping the SECURE Center Co-Creation teams refine the SVE ahead of broader release and onboarding. The UFR process will continue even after the SVE is broadly released to ensure continued relevance and user-friendly functions.

Following the presentation, discussion ensued with SECURE Center members, regarding the features demoed in the SVE and particularly when the system would be available. As the UFR process has started, several items needing resolution have been identified. Once items are successfully resolved, the SVE will be opened to interested users.

Questions were also raised about the availability of the web-based Consolidated Training Module for RS training. The SECURE Center webpage and materials have been updated. It was noted that a certificate of completion can now be downloaded on successful completion of the training.

As shared during the session, the capabilities of the SVE will continue to expand over time, providing resources that bolster the research ecosystem through the shared perspectives of a wide stakeholder base. Engagements between the FDP and the SECURE Center have become a vital channel of contribution to understanding the multi-faceted nature of research security.

U.S. Congressional Activity

House Republicans Express Concern Over Theft of Research Information

On September 18, 2025, U.S. House of Representatives Science, Space, and Technology Committee Chair Brian Babin (R-TX) and Investigations and Oversight Subcommittee Chair Rich McCormick (R-GA) sent a letter to MD Anderson Cancer Center expressing concern regarding a July 9, 2025 security incident involving an MD Anderson post-doctoral researcher, charged with theft and tampering with proprietary research. (more)

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.

Cyber threat information law hurtles toward expiration, with poor prospects for renewal (Cyberscoop, 9/22/2025)

The Cybersecurity Information Sharing Act of 2015, which allows private companies to share cyber threat data with the U.S. government, is set to expire September 30, 2025. Efforts in Congress to renew or extend the law are failing, due to political disagreements. A Senate proposal for a clean 10-year extension was blocked by Sen. Rand Paul (R-KY). Attempts to attach extensions to larger bills like the National Defense Authorization Act have also stalled. Without renewal, experts warn it could weaken cybersecurity cooperation between the private sector and government, especially during a major cyberattack. (more)

Texas HB 127 brings new research security rules to Texas (*Daily Toreador*, 9/17/2025)

Texas has passed a new state law that impacts how institutions of higher education (IHEs) manage foreign gifts and research partnerships. Among its requirements, House Bill 127 mandates the establishment of a Higher Education Security Council (comprised of research security officers from Texas universities); restricts gifts from "foreign adversaries" that can be accepted by IHEs, their employees, and student organizations; requires IHEs to conduct background screenings of non-citizen/resident applicants before offering employment in research-related positions; and requires IHEs to establish international travel approval and monitoring programs. (more)

Cybersecurity Training Programs Don't Prevent Employees from Falling for Phishing Scams (UC San Diego Today, 9/17/2025)

A major UC San Diego study involving 19,500 health employees found that common cybersecurity training methods—annual courses and embedded phishing simulations—do not significantly reduce the risk of falling for phishing scams. Employees who completed training were just as likely to click on phishing links as those who hadn't. Engagement with training was low, with most users spending less than a minute on the material or closing it immediately. Over the eight-month study, phishing susceptibility actually increased, with more than half of employees clicking on at least one phishing

link by the end. The study also revealed that some phishing emails were far more convincing than others. For example, an email claiming to update the company vacation policy had a much higher click rate than one requesting an Outlook password update. Researchers recommend shifting focus from traditional training to technical solutions like two-factor authentication and password managers that detect phishing sites. Their conclusion: current anti-phishing training programs are largely ineffective. (more)

'I have to do it': Why one of the world's most brilliant AI scientists left the US for China (*The Guardian*, 9/16/2025)

An in-depth look into the factors that contributed to Song-Chun Zhu, one of the world's foremost authorities in artificial intelligence, leaving the US after 28 years here. In August 2020, Zhu returned to China, where he now leads the Beijing Institute for General Artificial Intelligence (BigAI). (more)

Research Security-Related Events & Conferences

COGR October Meeting:

Registration is now open for COGR's 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!

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!

NSF SECURE Center Research Security Briefing

Vol. 1 No. 15: October 9, 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

SECURE Center News & Updates

SECURE Center Completing First Wave of Use-Feedback-Refine Sessions

The SECURE Center's first Use, Feedback, Refine (UFR) wave is wrapping up its fourth and final week, with 27 participants actively using and evaluating features in the Shared Virtual Environment (SVE). This phase emphasizes real-world engagement with the SVE's Resource Center and Community Forums to assess usability, value, and impact in authentic research security workflows. Early feedback is already guiding refinements that will enhance several features, ahead of broader release.

Preparations are now underway for Wave 2, which will begin the week of October 13 and engage 30 additional participants. These users will be among the first to explore and test resources designed specifically *by and for* research security professionals.

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.

Georgia Tech Research Corporation to Pay $875,000 to Resolve Civil Cyber-Fraud Litigation (U.S. Department of Justice, Office of Public Affairs, 9/30/2025)

Georgia Tech Research Corporation (GTRC) has agreed to pay $875,000 to settle allegations that it violated the False Claims Act by failing to meet required cybersecurity standards in certain Department of Defense (DoD) contracts. The U.S. government alleged that GTRC and its affiliate, Georgia Tech, did not properly secure sensitive systems, submitted a false cybersecurity assessment score, and lacked a required security plan for a lab conducting cyber-defense research. The case was brought by whistleblowers under the False Claims Act, who will receive $201,250 from the settlement. The government emphasized the importance of cybersecurity compliance in protecting national security. There has been no determination of liability. (more)

Fears grow over US scrutiny of Chinese university outposts (University World News, 09/29/2025)

An overview of the status of academic outposts in China, including some recent closures, and comments from currently involved institutions. The article also highlights the efforts by some US universities to maintain these intellectual collaborations, particularly for those with stand-alone branch campuses located in China. (more)

International Research Security Policy & Resources

Research Security in the Indo-Pacific: Why it matters to Australia

Using internationally available data, Dr Brendan Walker-Munro of the Perth USAsia Center posits the need for Australia to develop a national strategy, build capacity among partners to manage potential threats, and position itself as a hub for regional research collaboration. The Perth USAsia Centre, an independent think-tank, is a non-partisan, not-for-profit institution, based at The University of Western Australia since 2013. Its publications include other research security analyses related to the Indo-Pacific region. (more)

Research Security-Related Events & Conferences

COGR October 2025 Meeting:

Registration is now open for COGR's October 23-24, 2025 meeting in Washington D.C., at the Washington Marriott in Georgetown. Research security-related agenda topics include:

Thursday, October 23

3:45 – 4:45 pm: *Simplifying Research Regulations and Policies: Optimizing American Science – A NASEM Report*

Dr. Alex Helman, Senior Program Officer at the National Academy of Sciences, Engineering, and Medicine (NASEM), National Academies, Dr. Stacy Pritt, Associate Vice Chancellor for Research, Texas University A&M, and Dr. Lisa Nichols, Executive Director, Research Security, Notre Dame University will discuss the new report.

4:45 – 5:45 pm: *Cybersecurity Implementation and Cybersecurity Updates from the University Perspective*

A panel of university representatives will provide updates on their institutions' efforts to implement level 2 Cybersecurity Maturity Model Certification (CMMC) requirements, including practical challenges, lessons learned, and strategies for compliance. The discussion will also cover related cybersecurity issues and how institutions are adapting to the evolving federal requirements. Panelists include Allen DiPalma, Executive Director, Office of Research Security & Trade Compliance, University of Pittsburgh, Kelly Hochstetler, Associate Vice President for Research, University of Virginia, and Thomas Burns, Associate Vice Provost, Research Compliance, Johns Hopkins University. Kevin Wozniak, COGR's Research Security & Intellectual Property Director, will moderate.

Friday, October 24,

9:45 – 10:45 am: *Legislative Update & Outlook*

Joanne Carney, Chief Government Relations Officer at the American Association for the Advancement of Science and Tobin Smith, Senior Vice President for Government Relations & Public Policy at the Association of American Universities will discuss with COGR President Matt Owens the latest legislative developments and outlook for the rest of this year for federal research policy and funding.

Among the issues to be discussed: FY26 appropriations for research, facilities and administrative costs reimbursement, research security, immigration issues, and more.

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. through noon (CST) on August 31, 2025. Proposals are being accepted through noon (CST) on August 31, 2025 (more)

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

Sign up Here!

NSF SECURE Center Research Security Briefing

Vol. 1 No. 16: October 16, 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

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.

SBIR Programs Lapse (Breaking Defense, 10/8/2025; AIP 10/9/2025)
As reported by *Breaking Defense*, Senate lawmakers are at an impasse over the Small Business Innovation Research (SBIR) program, used by the Department of Defense (DOD) to provide seed funding for small companies, that expired on September 30, 2025. Critics of the program in its current form assert that a small number of SBIR recipients are receiving a disproportionately large percentage of funding. Led by Senator Joni Ernst (R-IA), they are calling for a number of revisions to the program, including a cap on the amount of SBIR funding any single company could be awarded throughout its lifetime.

In its reporting on the topic, the American Institute of Physics (AIP) noted that Ernst's proposed bill would also limit the number of proposals a company is permitted to submit per year, the number of proposals a company may submit per solicitation, and the number of concurrent projects on which an individual can serve as principal investigator.

Ernst's bill also includes research security-related provisions, including the implementation of a common definition of "Foreign Risk" for use across all participating federal research funding agencies, and the ability for agencies to revoke funding if a recipient small business provides intellectual property to a foreign country.

Sen. Peters tries another approach to extend expired cyber threat information-sharing law (CyberScoop, 10/09/2025)
Senator Gary Peters (D-MI) has introduced the Protecting America from Cyber Threats (PACT) Act, after the Cybersecurity Information Sharing Act of 2015 (CISA 2015) lapsed on September 30, 2025. The PACT Act would reauthorize the cyber threat-sharing law for another 10 years, through September 30, 2035. Peters' bill would continue the framework created under CISA 2015, which allows companies to voluntarily share cyber threat indicators with one another and with the government and continue to provide legal protections to companies that share cyber threat information in accordance with the law. The new name also potentially prevents confusion by distinguishing the Act from the agency that bears the same acronym: the Cybersecurity and Infrastructure Security Agency (CISA). (more)

International Research Security Policy & Resources

Cautionary Notes from the UK
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

A firestorm implicating senior members of government has erupted over the collapsed prosecutions of two researchers in the United Kingdom. The Crown Prosecution Service (CPS) alleged that between December 2021 and February 2023 a Chinese intelligence officer commissioned from the first researcher at least 34 reports on topics of political interest, ten of which were deemed prejudicial to national security. According to the CPS, the reports reached top officials in China and included "sensitive" information supplied by the second researcher, who worked in the office of the chair of the House of Commons' Foreign Affairs Select Committee but did not have access to classified information. Both researchers were charged under the Official Secrets Act with providing information directly or indirectly useful to an enemy for a purpose prejudicial to the safety or interests of the State. The researchers maintained their innocence. Shortly before their trials were to start, in September 2025, the CPS dropped the prosecutions citing the withdrawal of a key government witness and the failure of the government to provide essential evidence. The US government has expressed concern about this outcome.

While much of the commentary about this episode has focused on its political dimensions, at least three critical lessons from it bear on research security. First, risk extends beyond the STEM disciplines that dominate the research security discourse; for example, social scientists and humanists, especially those who engage in policy work, may possess unclassified but nevertheless sensitive or non-public information about the proceedings of a meeting; the opinions and activities of an individual or office; the deliberations attending an important decision; critical social, political, and economic trends; and legislative and regulatory developments. Proper discretion may be tested when disclosure of such information is remunerated and out of the public eye.

Second, not all patrons are the same. Know your partner or beneficial client, particularly if the relationship involves professional services outside of your principal employment. Though such opportunities can be flattering and lucrative, they may be too good to be true, even when they arrive from established knowledge services firms, which may insist on preserving the anonymity of their clients when they hire outside academic consultants. Do not presume that a recruiter has performed adequate due diligence on their client or shares your risk preferences or interests. Inattention to such matters entails an assumption of risk that may yield adverse legal or reputational consequences.

Third, law enforcement is an essential but frequently unsatisfactory instrument for addressing research security incidents. Prosecutions generally occur only after alleged activities have transpired and are extraordinarily resource-intensive undertakings that cannot scale very far. Moreover, many incidents will involve behavior that falls short of illegality but nevertheless incurs harms, and the best response may not be to lower the bar by defining new crimes or expanding the scope of existing ones. Cases can turn on myriad factors. The present UK scandal and the mixed record of US research security prosecutions counsel humility about what law enforcement can achieve, and underscore the importance of adopting a layered, comprehensive, and proactive research security culture that begins at the grass roots and prevents, detects, and intervenes early in incidents well before they reach the level of potential crimes.

Research Security-Related Events & Conferences

COGR October 2025 Meeting:

Registration is now open for COGR's October 23-24, 2025, meeting in Washington D.C., at the Washington Marriott in Georgetown. Research security-related agenda topics include:

Thursday, October 23

3:45 – 4:45 pm: *Simplifying Research Regulations and Policies: Optimizing American Science – A NASEM Report*

Dr. Alex Helman, Senior Program Officer at the National Academy of Sciences, Engineering, and Medicine (NASEM), National Academies, Dr. Stacy Pritt, Associate Vice Chancellor for Research, Texas University A&M, and Dr. Lisa Nichols, Executive Director, Research Security, University of Notre Dame will discuss the new report.

4:45 – 5:45 pm: *Cybersecurity Implementation and Cybersecurity Updates from the University Perspective*

A panel of university representatives will provide updates on their institutions' efforts to implement level 2 Cybersecurity Maturity Model Certification (CMMC) requirements, including practical challenges, lessons learned, and strategies for compliance. The discussion will also cover related cybersecurity issues and how institutions are adapting to the evolving federal requirements. Panelists include Allen DiPalma, Executive Director, Office of Research Security & Trade Compliance, University of Pittsburgh, Kelly Hochstetler, Associate Vice President for Research, University of Virginia, and Thomas Burns, Associate Vice Provost, Research Compliance, Johns Hopkins University. Kevin Wozniak, COGR's Research Security & Intellectual Property Director, will moderate.

Friday, October 24

9:45 – 10:45 am: *Legislative Update & Outlook*

Joanne Carney, Chief Government Relations Officer at the American Association for the Advancement of Science and Tobin Smith, Senior Vice President for Government Relations & Public Policy at the Association of American Universities will discuss with COGR President Matt Owens the latest legislative developments and outlook for the rest of this year for federal research policy and funding. Among the issues to be discussed: FY26 appropriations for research, facilities and administrative costs reimbursement, research security, immigration issues, and more

Save the Date for ASCE 2026:

Mark your calendar 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. Registration opens November 1, 2025. (more)

NCURA 2026 Annual Meeting Call for Proposals, Due Nov. 21:
The National Council of University Research Administrators (NCURA) will hold its 68th annual meeting from August 1-4, 2026 in New York City, NY. The deadline for session proposals is November 21, 2025. (more)

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

NSF SECURE Center Research Security Briefing

Vol. 1 No. 17: October 23, 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

SECURE Analytics News & Updates

NSF SECURE Analytics Launches Survey

NSF SECURE Analytics is seeking input from research security practitioners to help guide the product roadmap for the NSF SECURE Analytics Due Diligence Platform. The goal is to understand user workflows, minimum requirements, platform expectations, and solution preferences. All survey responses are anonymous and intended for internal market research only. (take the survey)

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.

China and the US have long collaborated in 'open research.' Some in Congress say that must change (Associated Press, 10/13/2025):
An overview of concerns raised by U.S. lawmakers regarding American colleges' and universities' research-related ties to Chinese scholars and institutions, including those expressed in three recently released reports from the House Select Committee on the Chinese Communist Party. (more)

China hits out at 'malicious' report that says it used US universities to boost military (South China Morning Post, 10/9/2025):
The Chinese foreign ministry has responded to the "malicious actions" of the U.S. House of Representatives Select Committee on the Chinese Communist Party (CCP), following the release of the Committee's report, "From PhD to PLA." The report posits that six universities investigated by the Committee admitted large numbers of Chinese students with significant ties to the Chinese military and defense industrial base. In a press briefing, a spokesperson for the ministry stated that the Committee has "no credibility whatsoever" and that "Certain US politicians, by overstretching the concept of national security and disrupting normal US-China exchanges in education and cultural fields, are acting against the will of the people and are doomed to fail." (more)

Research Security-Related Events & Conferences

NCURA 2026 Annual Meeting Call for Proposals, Due Nov. 21:
The National Council of University Research Administrators (NCURA) will hold its 68th annual meeting from August 1-4, 2026, in New York City, NY. The deadline for session proposals is November 21, 2025. (more)

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. Registration opens November 1st (more)

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

NSF SECURE Center Research Security Briefing

Vol. 1 No. 18: October 30, 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

Professional Association Resources & Meeting Reports

COGR October 2025 Meeting: Research Security Highlights

The Council on Governmental Relations (COGR) held its October 23-24, 2025, meeting in Washington D.C. Meeting materials from the event are now available.

COGR Session: Simplifying Research Regulations and Policies – Optimizing American Science: A NASEM Report

The COGR meeting included a briefing of the recently released National Academies report, *Simplifying Research Regulations and Policies: Optimizing American Science* which presents options for federal actions to improve regulatory efficiency affecting researchers and their institutions. Dr. Alex Helman, Study Director, National Academies of Sciences, Engineering, and Medicine, served as the moderator. Speakers included committee members Dr. Lisa Nichols, University of Notre Dame, and Dr. Stacy Pritt, Texas A&M University System.

Additional details regarding the information presented in this session, including options for reducing administrative burden in the area of research security, can be found in SECURE Center Research Security Briefing Number 13. In her remarks, Dr. Helman indicated that the report has been favorably received by Congress and federal agencies and offices.

COGR Session: Cybersecurity Implementation and Cybersecurity Updates

The Council on Governmental Relations (COGR), a higher education association, held the session "Cybersecurity Implementation and Cybersecurity Updates from the University Perspective" at their October 23-24 meeting. The presentation can be found here.

Allen DiPalma, Executive Director, Office of Research Security & Trade Compliance, University of Pittsburgh (Pitt); Kelly Hochstetler, Associate Vice President for Research, University of Virginia (UVA), and Thomas Burns, Associate Vice Provost, Research Compliance, Johns Hopkins University (JHU) joined Kevin Wozniak, COGR's Research Security and Intellectual Property Director for this panel presentation. Panelists provided "updates on their institutions' efforts to implement level 2 Cybersecurity Maturity Model Certification (CMMC) requirements, including practical challenges, lessons learned, and strategies for compliance" as well as related cybersecurity issues and how institutions are adapting to evolving federal requirements.

The session began with an audience poll, which indicated the following:

- 28% of institutions plan to meet CMMC compliance for Level 1 only, 31% Level 2 self-certification, 34% Level 2 third-party assessment, and 7% eventually Level 3.
- Current readiness for CMMC compliance: fully ready 10%; active planning or assessment 70%; haven't started implementation 15%.
- Regarding implementation of CMMC Level 1: contract- or project-specific 19%; dedicated

enclaves 24%; dedicated cloud environments 20%; institution-wide 15%; more than one of these options 21%

- Number of Level 1 environments that will be registered with SPRS (Supplier Performance Risk System): Only 1 31%; 2-5 15%; 5-10 3%; unsure 51%
- Institutions biggest challenge in preparing for CMMC: Funding and resource allocation, 38%; understanding applicability and scope, 9%; coordinating across multiple departments, 44%; limited staff expertise, 5%; communicating requirements to researchers, 5%
- Who currently owns responsibility for CMMC: Central IT/information security 54%; research compliance 16%; no designated owner (yet) 22%; unsure 7%

Panelists noted that the timeline for implementing DFARS 252.204-7021 is 3 years, beginning November 10, 2025. The detailed CMMC implementation timeline is included in the slides. Initial impacts will include solicitations and vendor profiles requiring CMMC.

The UVA panelist indicated that their CMMC Level 2 preparedness was approximately 95%, while their CMMC Level 1 preparedness was to be determined. UVA has not scheduled their audit but suggested they are close regarding Level 2. Options under consideration for moving forward included the possibility of skipping Level 1 and not pursuing FCI and engaging on a project-by-project basis, using the Level 2 environment for all. They suggested that defining an environment that included physical security didn't seem possible at the institutional level. SPRS certifications will be project-by-project (with approximately 35 contracts). It was noted that prime recipients sometimes flow down CMMC terms even when the subrecipient is only conducting fundamental research (FR). Institutions need to determine their comfort level when FR is involved, but the CMMC clause is still included in the contract.

There was discussion on defining the group of central assets to include in scope and who takes ownership. It was suggested that administrative systems would be in scope if deliverables were placed there. It was noted that no single office is responsible for CMMC. The VPR's office (contracts, compliance, research security), deans and provosts, and IT are generally involved.

The JHU panelist indicated that they have a secure, compliant environment via CMMC Level 1 and 2 self-assessments but have not yet done the independent audit. They are handling classified and restricted work, but there are separate CAGE codes and management teams. At the school and department level they are not NIST compliant; however, they don't store controlled unclassified information (CUI) here (not in scope), including NIH data subject to 800-171. The need for clear governance and reporting lines was noted.

The Pitt panelist suggested that many FR institutions now have exception processes that allow for restricted research/CUI. They thought they would do something on premises. They had an experience where DoD wanted to review and approve the technology control plans that included system security plans with the 110 controls. This represented a large amount of work. Pitt also suggested that on premises gets very expensive because of manpower. They decided to step back and consider

alternative solutions, landing on use of Microsoft Azure GCC High, which is in place now.

Pitt is currently preparing for CMMC Level 2 certification with plans to initiate the process in December 2025. Their estimated five-year cost for certification and maintenance of a CUI environment is $3,287,000 (see details in the slides). They have outsourced a lot of this work. This is for one specific enclave. It represents base costs, not variable costs like computing time. They want to develop a cost model to charge back as much as possible and are working with COGR on a FAIR model along these lines. It was suggested that clear messaging is needed from leadership that researchers must use this one enclave and need to understand the limits and parameters.

Regarding offboarding the data, Pitt noted that GCC High is cloud-based and very expensive. There will be costs for the faculty member. They may look for funding at the department level. UVA set up GCC High and found it was too expensive. They ended up just using it for calls. They decommissioned that environment due to the costs for the one program which were not being recovered from the associated DoD contract. The institution still has a number of responsibilities if GCC High is used, such as training, policy, and checking logs, across different offices and functions.

An audience member noted that every system that touches CUI is in scope. This includes authentication systems if used enterprise-wide (or, alternatively, to stand up a separate system). There are pros and cons that need to be thought through. It was noted that when a project ends, CUI is still CUI. For CMMC, it was suggested that an archival solution may not be required, but the CUI implications remain.

There was a question about who serves as the institution's affirming official. Panelists suggested it must be someone at a senior level, potentially the CISO and/or CIO. They are seeing Presidents and Provosts signing. As noted previously, it impacts many areas of the institution. UVA will roll-up certifications, so the ultimate signer feels comfortable, which is likely the VPR. At Pitt, IT will do this, as they're responsible for the scoring (i.e., the CISO or Vice Chancellor who is also the CIO). At JHU, it's likely the CISO, and the panelist thought this would be the right approach, but it is not yet resolved. Background materials linked to the session description included the following:

COGR's September 2025 Update

Department of Defense Cybersecurity Maturity Model Certification 2.0

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.

Uncertainty Swirls as CMMS Rollout Nears (Defense News, 10/20/2025)

A report on how the Department of Defense's Cybersecurity Maturity Model Certification (CMMC) program is set to begin its first phase on November 10, 2025, with full implementation by 2028. The initiative aims to ensure defense contractors meet standardized cybersecurity requirements to

protect sensitive information across the defense industrial base. However, uncertainty remains, as many contractors and acquisition offices may not be fully prepared, and a shortage of certified assessors could slow compliance efforts. While some expect initial disruption, officials emphasize that the rollout will proceed as planned following years of preparation. (more)

Trump's Crackdown on Chinese Students Ignores a Startling New Reality (*The New York Times*, 10/19/2025)

Guest authors from the Australian Strategic Policy Institute argue that U.S. efforts to restrict Chinese students from studying strategic technologies at top American universities are counterproductive.

The lawmakers' rationale is that allowing Chinese nationals to study advanced science and technology in the U.S. could help China surpass America. However, the authors state that this fear ignores the reality that China has already overtaken the United States in many areas of cutting-edge scientific research.

Based on their analysis of millions of peer-reviewed papers, China ranks first globally in 57 of 64 critical technologies, dominating the top 10 institutions in most of them. Tsinghua University leads worldwide in multiple areas, including artificial intelligence and autonomous systems, while MIT, the best U.S. performer, ranks first in only two fields. If China's Academy of Sciences were included, it would be the top global institution in 28 technologies. (more)

Similar data has been reported in the 2025 Research Leaders: Leading Institutions, released in June 2025. Based on Nature Index data of "high-quality research outputs" produced from 1/1/2024 through 12/31/2024, the data show that:

- Eight out of the top ten leading institutions, globally, are Chinese.
- Harvard University, ranked at number two, is the only U.S. institution included in the top ten leading institutions.
- 25 U.S. universities were included in the top 100 leading institutions. Except for the University of Chicago (+1.9%), all of these U.S. universities experienced a decrease in output from the previous year's data, ranging from -3% to -18%.

U.S. anti-science 'Cultural Revolution' fuels unease (South China Morning Post, 10/23/2025)

A number of Chinese American researchers have noted, either independently or in interviews with the South China Morning Post, what they perceive as similarities between the Chinese Cultural Revolution and the current state of scientific research in the United States. Instigated by Mao Zedong in 1966, the Cultural Revolution sought to consolidate power and purge the nation of "bourgeois" influences. The researchers note that, while the U.S. has not seen the widespread violence associated with the China's Cultural Revolution, the potential long-term impacts to higher education and the scientific enterprise are similar. (more)

RISC Bulletin

Texas A&M University's Research and Innovation Security and Competitiveness (RISC) Institute disseminates weekly RISC Media Bulletins, covering topics related to research security, foreign influence, and the intersection of science, technology, and national security. To join the distribution list for the RISC Bulletin or view previous editions, click here.

Research Security-Related Events & Conferences

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. through noon (CST) on August 31, 2025. Proposals are being accepted through noon (CST) on August 31, 2025 (more)

Previous NSF SECURE Center Research Security Briefings

Previous issues of the SECURE Center Research Security Briefings, in addition to the current issue, can be found on the NSF SECURE Center website.

Looking to participate in NSF SECURE Center co-creation activities or sign up for weekly briefings?

Sign up Here!

NSF SECURE Center

NSF SECURE Center
Research Security Briefing

Vol. 1, No. 19
November 6, 2025

The SECURE Center distributes Center information, 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 briefing also includes SECURE Center updates and opportunities. 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.

Briefing Contents

Federal Agency News & Updates

BIS 50% Rule Put on Hold

President Trump and Chinese President Xi reached a deal last week marking a thaw in U.S.–China trade relations. The agreement pauses key trade restrictions for one year: Washington will suspend enforcement of the Department of Commerce, Bureau of Industry and Security (BIS) "50% rule," which extends export controls to affiliates of listed entities, in exchange for Beijing suspending its rare earth export licensing regime.

U.S. Treasury Secretary Scott Bessent called the move "an opportunity to reset the relationship between the U.S. and China," explaining, "We are going to be suspending that [BIS 50% rule] for a year in return for the suspension on the rare earth licensing regime."

During this "cooling-off period," China will also lift tariffs on U.S. farm goods and commit to large soybean purchases, while the U.S. reduces certain tariffs on Chinese imports. For exporters and compliance teams, however, the rule's pause offers only temporary relief—the underlying restrictions could return once the year ends.

The deal was struck shortly after COGR, the Association of American Universities (AAU), and the Association of Public and Land grant Universities (APLU) submitted joint comments to the Department of Commerce, voicing concerns that the rule "creates new, substantial, and uncertain compliance burdens on the higher education research community and does not provide sufficient clarity or support for implementation."

International Research Security Policy & Resources

Europe to Ramp Up Research Security Measures

(Research Professional News, 10/29/2025)

Europe is increasing efforts to safeguard its research ecosystem by introducing a set of new measures under the forthcoming European Research Area Act, which will embed "research security" into law for the first time. These measures—announced by the EU's research commissioner at a 10/28/2025 conference in Brussels—include establishing a dedicated Centre of Expertise on Research Security, creating a due-diligence platform to assess risks in international collaborations, and developing a common methodology for research organization resilience. These measures reflect the EU's goals to balance openness in collaboration with stronger safeguards across member states. (more)

Balancing Opportunity and Risk: Rethinking China Scholarship Council Programs Amid Geopolitical Tensions

On October 23, 2025, the Centre for Science and Technology Studies (CWTS) at Leiden University, in the Netherlands, posted an article examining the programs run by the China Scholarship Council (CSC) in the context of rising geopolitical tensions, by means of a large-scale study of over 100,000 publications from CSC-funded researchers between 2009 and 2021. It finds that CSC scholars

overseas tend to produce high-impact work and engage in broad international collaborations, while only a small share (~ 5%) of the research was tied to China's military-linked institutions (e.g., "Seven Sons" universities), and only about 0.5% was related to dual-use technologies. The authors argue that, rather than sweeping bans, what is needed is a balanced, evidence-based approach that safeguards academic freedom and openness while incorporating due diligence and transparency to address legitimate security and research-integrity concerns.

Balancing Research Security and Open Science

On October 21, 2025, the Council of Canadian Academies released the report "Balancing Research Security and Open Science." The report's authors were charged with responding to the question "What does current evidence suggest for identifying and protecting dual-use research of concern (DURC) while balancing open science and innovation?" The report emphasizes that many of Canada's most vital research areas are simultaneously vulnerable to foreign interference, theft of intellectual property, or unintended harmful applications, such that a purely open-science stance is insufficient.

The authors note that risk is not static: what is non-sensitive at one stage can become sensitive later, so research security must be integrated across all the phases of the research lifecycle.

The report calls for a "modern research mindset" where institutions, funders, and governments share responsibilities and maintain adaptive systems rather than one-off checks. The report also highlights potential gaps, such as weaker oversight of industry research, inconsistent frameworks across jurisdictions, and low awareness of risk in certain fields that have traditionally not been seen as sensitive

NSF SECURE Center Opportunities & Updates

Research Security Mentorship Workshop Series

SECURE Center Midwest invites research security administrators from institutions of higher education to participate in the Research Security Mentorship Workshop Series. During this series participants will work to co-design a Mentorship Program utilizing needs-based pairing profiles that connect research security professionals with those better able to address the specific gaps within their program or practice. Register now for this opportunity to provide insights that will shape the program and equip participants for future program testing.

Any questions regarding SECURE Center Midwest initiatives can be directed to project manager Amy Brenneke at asbrenneke@umkc.edu or midwestsecurecenter@umkc.edu.

Research Security Events & Conferences

ASCE 2026 Registration Opens This Week

Registration opens the week of November 3, 2025, 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)

Previous NSF SECURE Center Research Security Briefings

Previous issues of the SECURE Center Research Security Briefings, in addition to the current issue, can be found on the NSF SECURE Center website.

RISC Bulletin

Texas A&M University's Research and Innovation Security and Competitiveness (RISC) Institute disseminates weekly RISC Media Bulletins, covering topics related to research security, foreign influence, and the intersection of science, technology, and national security. To join the distribution list for the RISC Bulletin or view previous editions, click here.

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

Contact info@secure-center.org or sign up here.

NSF SECURE Center

NSF SECURE Center
Research Security Briefing

Vol. 1, No. 20
November 13, 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.

Briefing Contents

Federal Agency News & Updates

Three Chinese National Scholars from University of Michigan Laboratory Charged for Conspiring to Smuggle Biological Materials into the U.S.

On November 5, 2025, the U.S. Department of Justice Office of Public Affairs issued a press release stating that three Chinese nationals conducting research at the University of Michigan have been charged with conspiring to smuggle biological materials into the country and making false statements. According to the complaint, they received shipments of concealed biological specimens from China, refused to cooperate with the university's internal investigation, and attempted to leave the country before being located by federal agents. (more)

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.

Let's Talk About Hard Power: America's Universities Are National Security Assets

(Inside Higher Ed, 11/10/2025)
In this opinion piece, the author (Brian L. Heuser, Associate Professor, Vanderbilt University) argues that U.S. universities are not just centers of culture or soft power, but key national security assets. It highlights how many campuses host large-scale research in defense, cybersecurity, biosecurity and technology, and also train officers, linguists, and analysts for the military and intelligence community. The author warns that under-funding and politicizing this higher-education ecosystem threatens America's ability to compete globally in innovation and strategic security. (more)

U.S.–China Scientific Collaboration at a Crossroads: Navigating Strategic Engagement in the Era of Scientific Nationalism

(Quincy Institute, 11/4/2025)
The authors propose that the era of open global scientific cooperation between the U.S. and the People's Republic of China is being replaced by selective decoupling and strategic competition. They document how China now matches (and, in some metrics, exceeds) the U.S. in research output. Yet collaboration between the two countries has fallen, especially in sensitive fields such as AI, advanced materials, and wireless communications. The authors argue that a binary choice between full openness and full separation is a false one. Instead, they suggest a "smart openness" model, based on a revised version of the U.S.–China Science and Technology Agreement to create a new framework for research collaboration that permits cooperation under safeguards, in areas where mutual benefits remain and national security risks can be managed. (more)

China academic intimidation claim referred to counter-terrorism police

(BBC, 11/3/2025)
Documents obtained by the BBC suggest that China conducted a two-year campaign of harassment and intimidation against Sheffield Hallam University to halt research led by Professor Laura Murphy into forced labor and human rights abuses against Uyghur Muslims in Xinjiang. “Chinese National Security Service” agents reportedly threatened the university’s China-based staff, blocked its websites, and curtailed communication channels, severely affecting the university’s ability to recruit Chinese students. Facing mounting pressure, a defamation lawsuit, and loss of insurance coverage, Sheffield Hallam decided not to publish Murphy’s final report and ultimately shut down her research unit in early 2025. Murphy accused the university of trading academic freedom for access to the Chinese student market and initiated legal action. (more)

The BBC has also reported that the university’s allegations of intimidation and harassment have now been referred to counter-terrorism police in the United Kingdom.

How China’s 15th five-year plan signals a new phase of strategic adaptation

(World Economic Forum, 10/30/2025)
The article suggests that China’s newest five-year plan, covering the years 2026 through 2030, signals a strategic pivot rather than continuation of past patterns. The new plan will prioritize industrial modernization first, with technological innovation placed immediately after. It also underscores how China is linking economic security, opening-up, and domestic demand with growth, indicating that external risks and supply-chain resilience are now high priorities. (more)

International Research Security Policy & Resources

Arctic Circle Issues and Concerns

Glenn Tiffert, PhD, Hoover Institution/Stanford

On October 16, the Arctic Circle Assembly in Reykjavik hosted a panel on research security with representatives from Canada, Denmark, Norway, and the United States. The panel included a scientist, a university research security officer, and analysts of great power competition in the region. The Arctic Circle Assembly is attended by more than 2,000 participants from civil society organizations, governments, think tanks, universities, and indigenous communities in more than 60 countries. It is the largest annual event dedicated to Arctic issues.

The panel focused on how the intensifying securitization of the Arctic is affecting the practice of science. For example, cooperation with Russian institutions and researchers in the Arctic has plummeted since the invasion of Ukraine and joint projects have experienced disruptions. Intensifying Russian military activity, poorly maintained shadow fleet tankers that risk environmental accidents, drone incursions into restricted airspace over ports and other critical infrastructure, and incidents damaging undersea pipelines and cables have the region on edge. Research vessels report intimidating, close range encounters with other ships at sea.

Retreating sea ice is opening new maritime routes for navigation and research that raise questions about national territory and sovereignty. Gaps in coastal domain awareness mean that unidentified

ships are appearing at the edge of indigenous communities and disrupting the hunts that sustain their ways of life. Securitization could impact the ability of these communities to benefit from research conducted on their lands and their rights to data they collect and store.

Panelists noted that in the Arctic civilian and military research frequently intersect. Civilian scientists may rely in part on military infrastructure or transport, which is increasing requirements for due diligence particularly around access to shared facilities. As new nations conduct research in the region, trust deficits loom large. Climate observatories can gather data vital to compensating for the magnetic conditions that interfere with military communications at the poles. Survey ships that map the sea floor or measure ocean currents, salinity, and temperature may advance submarine warfare or identify vulnerable undersea infrastructure. The panel underscored that, far from being a refuge from the security considerations that increasingly weigh on research elsewhere in the world, the Arctic may instead be a focal point for them. Consultative mechanisms that include the inhabitants of the region, visiting scientists, governments, and research institutions must rise to that challenge.

NSF SECURE Center Opportunities & Updates

Research Security Mentorship Workshop Series

Registration for the Research Security Mentorship Workshop Series closes Friday, 11/14/2025. Any questions regarding registration can be directed to the SECURE Center Midwest Project Manager, Amy Brenneke, at asbrenneke@umkc.edu.

Conferences

ASCE 2026 Registration Now Open

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

RISC Bulletin

Texas A&M University's Research and Innovation Security and Competitiveness (RISC) Institute disseminates weekly RISC Media Bulletins, covering topics related to research security, foreign influence, and the intersection of science, technology, and national security. To join the distribution list for the RISC Bulletin or view previous editions, click here.

Previous NSF SECURE Center Research Security Briefings

Previous issues of the SECURE Center Research Security Briefings, in addition to the current issue, can be found on the NSF SECURE Center website.

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

Contact info@secure-center.org or sign up here.

NSF SECURE Center

NSF SECURE Center
Research Security Briefing

Vol. 1, No. 21
November 20, 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.

Briefing Contents

NSF SECURE Center Opportunities & Updates

New SECURE Center Resources Now Available

The SECURE Center is dedicated to enhancing research security by providing unique solutions identified, prioritized, designed, and developed by and with the research community, for the research community. As part of this effort, several new resources are now available on the Products page of the Center's website, including:

- Travel resources to help Research Security/Compliance Officers guide and advise their faculty on international travel and how to best protect themselves and their research intellectual property:
    - A Basic Travel Checklist designed for all international travelers, focused on cybersecurity and other considerations for protecting research data, intellectual property, and personal information
    - A Travel Resource Guide that provides additional context to the checklist, including travel case studies and additional resources and implementation considerations for rolling out a travel awareness campaign
    - A Sample Travel Briefing providing a structured curriculum research security professionals can use for discussion with travelers prior to departure, with a focus on cybersecurity best practices, export controls, and personal safety
- A Risk Assessment Framework, adaptable for use by any institution, regardless of size, structure, or available resources. Institutions can use the framework to conduct risk assessments, develop new institutional risk assessment processes, benchmark and improve existing workflows, and train and educate staff.
- A Risk Matrix Reference Guide designed to save the research community time in understanding agency risk factors, including differences, and commonalities. The guide integrates NIH, NSF, DOE, and DoD risk assessment information for fundamental research proposal review.
- Process Pathfinder resources to help create, execute, and facilitate tabletop exercises to understand and refine organizational operations:
    - A Facilitation Guide
    - A Process Gates diagramming method to understand the existence and flow of organizational processes and the barriers they encounter
- Reference Resources that provide foundational information about research security:
    - A cross-agency Glossary designed to clarify key terms and expectations in research security for diverse stakeholders
    - A Research Security Reference Library that provides a comprehensive compilation of current and historical research security documents, including concise summaries and impact descriptions of federal-wide efforts, legislative requirements and congressional activities, and agency-specific policies and requirements

Professional Association Resources & Meeting Reports

AAU/APLU Send Joint Letter in Response to SAFE Act in NDAA

On October 15, 2025, the presidents of the Association of American Universities (AAU) and Association of Public Land-Grant Universities (APLU) sent a joint letter to the chairs and ranking members of the U.S. House and Senate Committees on Armed Services, requesting that the Securing American Funding and Expertise from Adversarial Research Exploitation Act (or SAFE Research Act) be removed from the final version of the National Defense Authorization Act (NDAA). The US House version of the NDAA, which included the SAFE Research Act, was passed on September 10, 2025 and advanced to the Senate for reconciliation with its version. In their letter, the presidents note that, if passed, the SAFE Act would impact all federal research funding agencies and create "enormously broad definitions of 'hostile foreign entity' and 'affiliation' that would apply to *any* agreement that a U.S. university has with *any* university in China…" and would "functionally require any U.S. institution of higher education and their faculty to terminate all engagements with numerous international universities and researchers as a condition of federal funding, regardless of whether these programs and collaborations are currently even active or inactive."

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.

EU moves to bar China from parts of Horizon Europe

(Research Professional News, 11/11/2025)

A draft program from Horizon Europe, the European Union's key research and innovation program for 2021-2027, proposes new restrictions on Chinese participation. In the proposed program, Chinese "entities" would be barred from three of the six major research areas (or "clusters"). Specifically, Chinese entities would be prohibited from participating in any "Research and Innovation Actions" (projects that aim to produce innovative products, services, or processes that are nearing market readiness) in the clusters for: health; civil security and society; or digital, industry and space. Chinese entities would still be allowed to participate in the clusters related to culture, climate/energy/mobility, and natural resources. Chinese universities supervised by China's Ministry of Industry and Information Technology would be prohibited from participating in any parts of the program. (more)

International Research Security Policy & Resources

Research security as a collective responsibility: empowering universities, enabling Europe

On October 27, 2025, prior to the European Flagship Conference on Research Security, the Conference of European Schools for Advanced Engineering Education and Research (CESAER) published the input note, "Research security as a collective responsibility: empowering universities,

enabling Europe." The publication emphasizes the importance of research security as a shared responsibility to sustain Europe's research excellence while protecting academic freedom and fostering global competitiveness. It stresses the need for proportionate, risk-based safeguards to prevent misuse of research, particularly in sensitive areas like dual-use technologies, and to maintain open science principles. The publication also outlines key recommendations for universities, EU institutions, and national governments, including building strong institutional foundations, incentivizing and empowering researchers, integrating openness and security, ensuring responsible collaboration, and creating a cohesive, level playing field across Europe. (more)

Research Security Events & Conferences

ASCE 2026 Registration Now Open

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

RISC Bulletin

Texas A&M University's Research and Innovation Security and Competitiveness (RISC) Institute disseminates weekly RISC Media Bulletins, covering topics related to research security, foreign influence, and the intersection of science, technology, and national security. To join the distribution list for the RISC Bulletin or view previous editions, click here.

Previous NSF SECURE Center Research Security Briefings

Previous issues of the SECURE Center Research Security Briefings, in addition to the current issue, can be found on the NSF SECURE Center website.

No SECURE Center Research Security Briefing 11/27/2025

In observance of the Thanksgiving holiday, there will be no NSF SECURE Center Briefing distributed on Thursday, November 27, 2025.

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

Contact info@secure-center.org or sign up here.