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 | NSF SECURE Center