NSF SECURE Center

NSF SECURE Center
Research Security Briefing

Vol. 1, No. 24
December 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.

Briefing Contents

Federal Agency News & Updates

NIH Posts Scenarios of Monetary Donations as Other Support vs. Gifts

The National Institutes of Health (NIH) Office of Policy for Extramural Research Administration (OPERA) has posted a document providing illustrative scenarios to help investigators and institutions determine when monetary donations must be disclosed as "Other Support" versus when they qualify as unrestricted gifts. The document explains that donations must be reported as Other Support when they are intended to directly support an investigator's research activities and carry explicit *or implicit* expectations, such as use for specific projects, placement into an investigator's research account, or requirements to provide updates to donors.

The scenarios included in the OPERA document correspond with those included in the Office of the Inspector General's March 2025 review, "Most Institutions That Received NIH Funding Did Not Fully Understand When They Must Report Monetary Donations."

Professional Association Resources & Meeting Reports

FDP Update on Status of Federal Research Security Requirements

The Federal Demonstration Partnership's Research Security Subcommittee posted an Update on the Status of Federal Research Security Requirements on December 17, 2025. The update provides an overview of the current status of federal research funding agency implementation of research security requirements for researchers and institutions in accordance with the conditions of the CHIPS and Science Act of 2022 (CHIPS Act) and National Security Presidential Memorandum-33 (NSPM-33).

The update includes agency notices, implementation, and resources related to Research Security Training Requirements, Disclosure through Common Form Implementation, Research Security Program Requirements, Foreign Gift and Contract Reporting, and Risk Reviews of Fundamental Research Proposals.

AAU: House Passes FY26 NDAA

On December 12, 2025, the American Association of Universities (AAU) posted a follow-up on the status of the FY26 National Defense Authorization Act (NDAA), that provides a status update on the research security-related provisions that have been included in previous iterations of the bill, which is now pending review by the Senate. Notably, provisions of concern that AAU and the Association of Public and Land-grant Universities objected to, including the SAFE Research Act), are not included in the final version of the legislation.

U.S. Congressional Activity

House Subcommittee Hearing on Implementation of Research Security Measures

On Thursday, December 18, 2025, the U.S. House of Representatives Committee on Science, Space, and Technology held a subcommittee hearing, “Research Security: Examining the Implementation of the CHIPS and Science Act and NSPM-33.” Witnesses at the hearing, held by the Subcommittee on Investigations and Oversight, included:

- Dr. Rebecca Keiser, Acting Chief of Staff, National Science Foundation (NSF)
- Dr. Daniel Evans, Assistant Deputy Associate Administrator for Research, National Aeronautics and Space Administration (NASA)
- Dr. Patricia Valdez, Chief Extramural Research Integrity Officer, National Institutes of Health (NIH)
- Mr. Jay Tilden, Director of Office of Intelligence and Counterintelligence, U.S. Department of Energy (DOE)

The hearing examined how federal research agencies are implementing research security requirements amid growing concern that inconsistent guidance, limited resources, and administrative burden are undermining both security and U.S. competitiveness. Members from both parties agreed that research security is a national security imperative, given persistent efforts by foreign adversaries—particularly China—to exploit the openness of the U.S. research enterprise. At the same time, many lawmakers emphasized that excessive bureaucracy, agency and research funding instability, capped indirect costs, and the loss of federal staff risk driving away top talent and weakening the very scientific ecosystem these policies are meant to protect. A central theme was the need for clear, harmonized, and actionable guidance across agencies so compliance does not depend on which funder or program a researcher engages with.

Agency witnesses described steps taken to strengthen safeguards while trying to preserve openness. NSF highlighted its TRUST framework, prohibition on malign foreign talent recruitment program participation, certifications, training requirements, and the foundation of the SECURE Center and SECURE Analytics. NASA emphasized a shift away from the “honor system” to verified certifications, clarity through standardized disclosures, and agency alignment to minimize administrative burden on scientists. NIH outlined their comprehensive program focused on disclosure, training, use of common forms, and investigative measures. DOE underscored the role of national laboratories, enhanced due diligence and post-award monitoring, and the need for tailored, risk-based mitigation. Across agencies, witnesses acknowledged staffing shortages, uneven institutional capacity—especially for smaller institutions—and the absence of strong interagency coordination, while members repeatedly stressed that Congress must ensure stable funding, harmonization, and oversight to secure U.S. research without sacrificing global collaboration or long-term U.S. leadership.

House Committee Report Claims China Exploits DOE-Funded Research

The U.S. House of Representatives Select Committee on the Chinese Communist Party (CCP) released a report on December 17, 2026, alleging that the U.S. Department of Energy (DOE) has systematically failed to protect DOE-funded research from exploitation by the CCP, particularly by entities tied to China’s defense research and industrial base. Based on a review of publications, grants, and Chinese-language sources, the authors claim that thousands of DOE-funded research papers between 2023 and 2025 involved collaborations with Chinese institutions, with roughly half linked to military- or defense-designated entities. The report states that these collaborations, which span highly sensitive and dual-use fields, such as quantum science, advanced materials, artificial intelligence, semiconductors, nuclear science, and high-performance computing, raise national security, ethical, and reputational concerns.

The authors posit that these risks persist because DOE's research security framework is fragmented, under-resourced, and slow to adapt, with gaps in vetting, disclosure, post-award monitoring, and interagency coordination. It cites weaknesses such as limited access to grant data, inconsistent risk assessments, inadequate oversight of national laboratories, insufficient scrutiny of foreign affiliations (including China Scholarship Council involvement), and a failure to draw clear boundaries regarding partners implicated in human rights abuses. The report recommends stronger safeguards and legislative action (particularly the SAFE Research Act) to prohibit high-risk collaborations, enhance disclosure requirements, and protect U.S.-funded research.

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.

Purdue Allegedly Rejecting Grad Students from China and Other 'Adversary Nations'
(Inside Higher Ed, 12/12/2025)

Purdue University is facing accusations from current and prospective graduate students that it has rejected large numbers of applicants from China and other countries labeled as "adversary nations," for its graduate programs this year. Students and some faculty say admissions committees were informally instructed that offers to applicants from these countries are "highly unlikely," though no formal policy exists. Critics argue the practice may be discriminatory and could harm both the students affected and the university's reputation, while Purdue remains silent on the specifics of its admissions decisions. (more)

NSF SECURE Center Opportunities & Updates

Updated Version of Consolidated Training Module (CTM) Now Available

In response to user feedback, the SECURE Center has updated the condensed research security training module to further enhance accessibility. The transcript now includes content that is not narrated in the module. This includes all "knowledge check" on-screen text and text from pop-up windows that contain additional information and links. In addition, links now use content-specific text rather than "click here." These changes allow users accessing the content through the transcript to have a similar experience as those using the web-based module. Links to additional materials are now also included in the transcript. The training module and audio files have been updated to reflect the content-specific text. The updated transcript and module files (CTM 1.2) can be found on the training page of the SECURE Center's website.

Researchers in Quantum and Computer Science Sought for Input on RS Resources

Researchers working in quantum computing, computer science, and related fields are being invited to volunteer for a short virtual information-gathering session to help shape new tools that support emerging federal research security requirements. The sessions, organized by the NSF-funded SECURE Center, aim to gather researcher perspectives on challenges related to research security and international collaboration, with a focus on developing practical, low-burden resources to address these challenges. Participation will directly inform future guidance, training, and tools intended to reduce administrative workload and impediments to international collaborations while safeguarding research. Faculty are encouraged to share this opportunity with colleagues who may be interested; questions or offers to participate should be directed to SECURE Center staff at researchsecurity@nd.edu. Sessions are currently scheduled for:

- Thursday, January 15, 2026, 12-1:00 pm ET
- Thursday, January 15, 2026, 4-5:00 pm ET
- Friday, January 23, 2026, 12-1:00 pm ET
- Tuesday, January 27, 2026, 2-3:00pm ET
- Friday, January 30, 2026, 12-1:00 pm ET

Research Security Events & Conferences

FDP January 2026 Virtual Meeting Registration Now Open

Registration is now open for the Federal Demonstration Partnership (FDP) virtual meeting, January 26-28, 2026. Information regarding dates and times of research security-related sessions will be included in future SECURE Research Security Briefings as details become available.

COGR February 2026 Virtual Membership Meeting Registration Now Open

Registration is now open for COGR's virtual membership meeting, taking place February 24-27, 2026. Information regarding dates and times of research security-related sessions will be included in future SECURE Research Security Briefings as details become available.

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.

NSF SECURE Center Briefings Resume January 8, 2026

In observance of the holiday season, distribution of the NSF SECURE Center Briefing will be paused until January 8, 2026.

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.

The information provided by the NSF SECURE Center is intended for general research and educational purposes only. While we strive to ensure the accuracy and reliability of our content, we do not guarantee its completeness, timeliness, or applicability to specific circumstances. Each user is responsible for conducting their own risk assessments and making decisions based on independent judgment.

Further, the NSF SECURE Center does not provide professional or legal advice, and users are encouraged to consult qualified professionals before making decisions based on the information found here. The NSF SECURE Center shall not be liable for any damages or costs of any type arising out of or in any way connected with your use of this information. External links are provided for convenience and do not constitute an endorsement of the content or services offered by any third-party resources.