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!