NSF SECURE Center

NSF SECURE Center
Research Security Briefing

Vol. 1, No. 22
December 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.

Briefing Contents

Federal Agency News & Updates

NIH Issues Two Research Security-Related Notices

On December 2, 2025, the National Institutes of Health (NIH) released two research security-related notices.

Research Security Training Requirements for NIH

In Notice NOT-OD-26-017, NIH notifies the extramural community that effective with applications submitted for due dates on or after **May 25, 2026**, each individual listed as senior/key personnel on the application must certify they have completed research security training (RST) within 12 months of the date of application submission. NIH will collect this certification via the Biographical Sketches completed by senior/key personnel in SciENcv.

While the Notice states that applicants/recipients may use any RST that addresses the topics mandated under the CHIPS and Science Act, it notes that the SECURE Center condensed training module (CTM) meets these requirements and, therefore, NIH recognizes completion of the CTM as compliant with this Notice.

NIH's Implementation of Common Forms for Biosketch and Current and Pending (Other) Support

Notice NOT-OD-26-018 announces NIH adoption of the Common Forms for Biographical Sketches and Current and Pending (Other) Support. Use of the Common Forms and the NIH Biosketch Supplement will be required for applications with due dates on or after **January 25, 2026**, and for Research Performance Progress Reports (RPPRs) and Just-In-Time (JIT) responses submitted on or after that date. All forms will be completed via SciENcv.

While eRA system validations will initially generate a warning message if the incorrect forms are used, by February 6, 2026, failure to use the Common Forms will generate an error, preventing submission.

NIH's transition to the Common Forms will include malign foreign talent recruitment program (MFTRP) certifications from applicant institutions and individuals identified as senior/key personnel.

- By signing the face page of an application, Authorized Organization Representatives (AORs) will certify that "all individuals identified by the applicant as senior/key personnel have been made aware of and have complied with their responsibility under that section to certify that the individual is not a party to a malign foreign talent recruitment program."
- At the time of application, each individual identified as senior/key personnel will certify they are not a party to an MFTRP via completion of the Biosketch Common Form.
- At the time of annual RPPR, each individual identified as senior/key personnel will certify they are not a party to an MFTRP by uploading a certification statement, as a flattened PDF, in section G.1 of the eRA RPPR submission.

All individuals required to submit a Biosketch, Biosketch Supplement, or Current and Pending (Other) Support to NIH must:

- Obtain an Open Researcher and Contributor Identifier (ORCID iD)

- Link their ORCID iD to their eRA Commons account.
- Confirm their ORCID iD is displayed in the Persistent Identifier (PID) section of the Common Forms.

A preview of the Common Forms and NIH Biosketch Supplement are currently available via SciENcv. NIH anticipates finalizing the SciENcv templates for these forms, and instructions for using them, by the week of December 15, 2025.

Department of Education Announces New HEA 117 Reporting Portal

On December 1, 2025, the U.S. Department of Education (DoED) announced the **January 2, 2026** launch of a new reporting portal for institutions of higher education (IHEs) to submit their disclosures of foreign gifts and contracts, in compliance with Higher Education Act (HEA) Section 117. The redesigned portal incorporates feedback DoED has received from IHEs since the implementation of the existing portal in June 2020, including functionality to:

- "Bulk upload" reportable gifts and contracts
- Save draft submissions
- Self-correct prior submissions (for reports submitted through the new portal)
- Download the full set of submitted records
- Assign more granular roles to IHE personnel involved in the HEA 117 reporting process

DoED will provide a training webinar on the new portal on December 15, 2025 at 2:30pm ET and will release a recording of the webinar on December 18, 2025.

Access to the existing portal will be disabled on December 16, 2025.

After its launch, both the new portal and existing and future guidance/information will be accessed at www.ForeignFundingHigherEd.gov.

NSF Important Notice No. 149 Requirements Take Effect Dec. 2, 2025

On November 25, 2025, the National Science Foundation (NSF) released an update to the agency's Important Notice No. 149. The update states that the requirements originally slated to take effect in October 2025, instead take effect on December 2, 2025 as a result of the recent government shutdown. The impacted requirements include:

- Certifications of research security training for senior/key personnel,
- Institutional certifications regarding contracts or agreements with Confucius Institutes,
- Recipient institutions providing supporting documentation for senior/key personnel activities reported as current and pending (other) support (e.g., contracts, grants, appointment letters) to NSF, upon request.

For additional details about the requirements set forth in NSF Important Notice No. 149, see SECURE Center Research Security Briefing No. 2.

Chinese National Pleads Guilty, Sentenced for Smuggling Pathogen into U.S.

On November 12, 2025, the Department of Justice U.S. Attorney's Office for the Eastern District of Michigan issued a press release stating that Yunqing Jian, a 33-year-old Chinese national who had worked at a University of Michigan laboratory, pleaded guilty to smuggling a dangerous biological pathogen into the United States and lying to Federal Bureau of Investigation agents. According to prosecutors, Jian had previously received funding from the Chinese government for her work with the pathogen (Fusarium graminearum, a fungus that causes "head blight" in crops such as wheat, barley, and rice), and her electronic devices included details of Jian's affiliation with the Chinese Communist Party. Jian was sentenced to time served—a five-month jail term. (more)

Professional Association Resources & Meeting Reports

COGR Releases Research Security Document for Technology Transfer Professionals

On November 20, 2025, COGR released a new document, "Research Security Regulations: Practical Considerations for Technology Transfer Professionals" that provides an overview of the research security-related regulations and frameworks most salient to Technology Transfer Offices. Topics include:

- Disclosure and transparency requirements
- Fundamental research and export control
- Restricted information
- Sensitive information transfers
- Patents and foreign filings
- Foreign investments and CFIUS

The document was developed by COGR's Research Security and Intellectual Property committee led by Kevin Wozniak. Allen DiPalma, Executive Director, Office of Research Security & Trade Compliance at the University of Pittsburgh, a member of the committee and contributor to the document, noted that the document "provides a much-needed bridge between the research security and technology transfer fields that is easy to understand and relevant to both research security officials and technology transfer 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.

Researcher's Smuggling Arrest Casts Light on Dispute Over Chinese Students

(*New York Times*, 11/21/2025)

The case of a Chinese postdoctoral fellow at the University of Michigan who smuggled seeds and a crop-infecting fungus into the United States has sparked a broader political debate over Chinese researchers, even though prosecutors ultimately conceded they could not prove harmful intent and the postdoctoral fellow, Yunqing Jian, received only a time-served sentence. While prosecutors argued the materials posed potential national security and agricultural risks, Ms. Jian's defense described the case as overblown and driven by politicized scrutiny of Chinese students. The case unfolded as Congress and federal agencies have pushed universities to sever research ties with Chinese institutions and pursued similar prosecutions involving undeclared biological materials. Critics warn such measures harm scientific collaboration and are increasingly contradicted by the Trump administration's recent stance acknowledging U.S. universities' dependence on Chinese students. (more)

'Red flags' over teaching partnership with Chinese university
(Times Higher Education, 11/6/2025)
Sydney's Macquarie University has denied the *Daily Telegraph* newspaper's claims that the university's joint institute with Nanjing Normal University (NNU) will train Chinese "cyber warriors" and that the NNU partner program provided "'talent recruitment' sessions for the People's Liberation Army (PLA)," and supplied recruits for Chinese defense companies that have been restricted by the U.S. Macquarie stated that the bachelor's degrees offered through the joint institute do not involve research and that Macquarie completed a thorough due-diligence review before entering into the joint institute arrangement. Critics, however, have raised concerns about the nature of work Chinese graduates from the joint institute may ultimately undertake, and the institute's future impacts to Macquarie's ability to obtain overseas research funding (e.g., from the U.S. or Canada), given the university's collaboration with a PLA-linked entity. (more)

International Research Security Policy & Resources

Research Security in Europe: An Emerging Community

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

From October 28 to 30, 2025, more than 500 policymakers, practitioners, and experts gathered in Brussels for the first European Flagship Conference on Research Security. The conference was sponsored by the European Commission in partnership with a dozen European stakeholder associations: ALLEA, CESAER, Coimbra Group, EARTO, EECARO, EUA, EU-LIFE, G6, LERU, Science Europe, The Guild and YERUN. Event organizers cite the Academic Security and Counter-Exploitation (ASCE) Program seminar, held every February at Texas A&M University, as a source of inspiration.

The conference was an important milestone following the adoption of the 2024 Council Recommendation on Enhancing Research Security. More than one hundred speakers surveyed the research security strategies and practices adopted by governments and institutions, the roles played by funding organizations, how public authorities can support the research sector, and the possibilities for multilateral coordination. Speakers from the U.S. included Sarah Stalker-Lehoux, acting chief of

research security and policy at the National Science Foundation, and Drs. Kevin Gamache and Glenn Tiffert of Texas A&M University and the Hoover Institution, respectively.

In her keynote address, the European Commissioner for Startups, Research, and Innovation, Ekaterina Zaharieva, announced several forthcoming initiatives: 1) the establishment of a new European Centre of Expertise on Research Security inside the European Commission; 2) the creation of a due diligence platform to help researchers assess risks of international cooperation; and 3) a new common methodology for member states to test the resilience of their research-performing organizations. The Centre of Expertise is expected to launch in mid-2026; and contracts for building the due diligence platform have been issued to a handful of European stakeholder organizations with the aim of a late-2026 pilot release date. The Commission is also preparing a periodic Research Security Monitor report.

These initiatives are part of an integrated policy of strategic autonomy and economic and research security. Since 2000, the European Commission has been working towards a single European market for research, technology, and innovation, the European Research Area (ERA), and in May 2025, it added research security to the 2025-27 ERA Policy Agenda as a priority action item.

Substantial challenges lie ahead in translating emerging European-level research security frameworks and policies into consistent implementation. Institutional capacity, legal authorities, resources, risk exposure, and awareness vary significantly among member states. Much will depend on the levels of commitment and political capital that governments bring to bear amid the other fiscal, military, and economic competitiveness concerns competing for their attention.

Americans should nevertheless take notice. Research security is gaining momentum in Europe, and collaborators from the European Union are collectively our most frequent international research partners by a wide margin. Ongoing efforts by stakeholders at every level to mutually align requirements, accommodate difference, and foster interoperability will be vital to sustaining the communities of trust undergirding our strong traditions of transatlantic research collaboration, discovery, and innovation.

What is research security and why does it matter for global science?

A November 21, 2025, blog post from analysts at Europe's Organisation for Economic Co-operation and Development (OECD) note that, since 2018, the number of national research security initiatives has surged nearly tenfold and argue that the challenge for policymakers is to find a balance between protecting national and economic security while maintaining an open, cooperative global science system.

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.

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.