NSF SECURE Center

NSF SECURE Center
Research Security Briefing

Vol. 1, No. 23
December 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.

Briefing Contents

Federal Agency News & Updates

DOE Implements Common Forms for Biosketches and Current & Pending Support

On December 3, 2025, the U.S. Department of Energy (DOE) issued Financial Assistance Letter FAL 2026-02, mandating that any notices of funding opportunities (NOFOs) issued by DOE (including the National Nuclear Security Administration) on or after December 3, 2025, require use of the Common Forms via the SciENcv system for Biographical Sketches (Biosketches) and Current and Pending (Other) Support (CPS).

DOE's implementation of the Common Form for Biosketches replaces the agency's use of the Resume form. DOE is not changing any of the data collection fields used in the Biosketch Common Form, however, the FAL provides DOE program offices with latitude to specify within a given NOFO certain aspects of the data collected, for example: whether a digital persistent identifier (e.g., ORCID ID) is required, or the reporting timeframe of appointment information that must be included.

Similarly, DOE is implementing the CPS Common Form without changes to the data collection fields, however, the FAL allows DOE program offices to determine whether, for a specific NOFO, additional data must be provided within the CPS, for example: whether disclosure of *past* support is required, or whether disclosure of "'Travel supported/paid by an external entity to attend a conference or workshop' located in a foreign country of concern" (i.e., non-research-related) as in-kind support is required.

During the life of an award, recipient/subrecipient institutions adding new covered individuals to a project must submit the Biosketch and CPS Common Forms for the individual and receive DOE's approval prior to the new covered individual joining the project team. For covered individuals that were previously approved, if there are any changes to the Biosketches or CPS forms that were previously submitted to DOE, "the individuals must update their disclosures within 30 days of the change, or on a timeline consistent with the program office instructions."

Registration Open for Dept. of Education HEA 117 Reporting Portal Training Webinar

The U.S. Department of Education (ED) has released registration information for its upcoming training webinar, "Using the New Section 117 Reporting Portal." The webinar will be held on December 15, 2025, from 2:30-4:30pm (ET). A recording of the webinar will be made available on December 18, 2025, via ED's Knowledge Center. Additional information about ED's new portal for institutions of higher education (IHEs) to report foreign gifts and contracts, as required under Higher Education Act (HEA) Section 117, can be found here, and also in Research Security Briefing No. 22.

The new portal will be accessed at www.ForeignFundingHigherEd.gov, after its launch on January 2, 2026. This page also includes a dashboard with data visualizations of IHEs' foreign gift/contract data submitted to ED as of January 31, 2025.

NSF Issues Grace Period for Important Notice No. 149

On December 5, 2025, the National Science Foundation (NSF) notified the research community that the agency is "offering a grace period [for enforcement of NSF Important Notice No. 149] for

proposals submitted between Dec. 2, 2025, and Dec. 31, 2025, to accommodate challenges for NSF programs with deadlines that fall close to the Dec. 2, 2025, effective date."

In an email distributed by the Office of the Chief of Research Security Strategy and Policy, NSF noted that the December 2, 2025, effective date posed difficulties for some recipient institutions to collect and submit updated Biographical Sketches (Biosketches) and Current and Pending (Other) Support (CPS) forms incorporating the new certifications from senior/key personnel required under Important Notice No. 149. The Notice requires that senior/key personnel certify in their Biosketches and CPS documents that they have completed research security training within the past 12 months and that they are not a party to a malign foreign talent recruitment program.

As a result, NSF will continue to accept proposals using the previous version of the Biosketch and CPS forms until December 31, 2025. After December 31, 2025, all proposals submitted must be compliant with Special Notice No. 149. For additional details on the requirements included in Special Notice No. 149, see SECURE Center Research Security Briefings No. 2 and No. 3.

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.

Report: Impact of Chinese Research 'On Par' With U.S.
(Inside Higher Ed, 12/8/2025)

A new report from the Institute for Scientific Information (ISI), covering research output, citations, and collaborations from 1999 to 2024, finds that the research enterprise of Mainland China has, for the first time, reached approximate parity with that of the United States, and that the shift coincides with the U.S. government's heightened focus on research security. In 2024, China authored 878,307 journal articles and reviews, compared with 509,485 from the U.S. In addition, China's citation "impact," a common measure of research influence, has risen to nearly match that of the U.S. The report also highlights a shift in global collaboration dynamics: historically, U.S.–European partnerships yielded the most highly cited work; but citations for papers co-authored by Chinese and U.S. or Chinese and European researchers have surged, narrowing the lead once held by traditional Western collaborations. Meanwhile, U.S.– China collaborations have declined since their 2019 peak, a drop attributed largely to increased research security scrutiny and stagnant research funding in the U.S., compared with China's rising investment.

Taken together, the data suggest that China is no longer just catching up but also positioning itself as a peer competitor to the U.S. in research volume and influence. The report warns that continued reductions in international collaboration, especially between the U.S. and China, could erode the U.S.'s traditional competitive advantage in global science. (more)

Moving beyond "dual use": quantum technologies and the need for new research security paradigm
(*EPJ Quantum Technology*, 11/26/2025)

The paper asserts that quantum technologies (QT) are transforming the national security landscape in ways that make the traditional concept of "dual-use" technology increasingly inadequate. Because QT underpins disruptive capabilities with both civilian and military applications (including communications, cryptography, computing, sensing, and advanced materials) the current binary dual-use classification fails to guide effective research security policy. The author argues that this is especially true in universities, where most quantum research occurs and where strong security cultures are often lacking. The author shows how QT's low barriers to entry, rapid global diffusion, and unpredictable future applications challenge export controls, economic competitiveness strategies, and foreign-policy tools such as sanctions or talent program restrictions. To address these gaps, the paper proposes moving beyond dual-use toward more nuanced frameworks: multivariate risk measures that better capture national security implications; risk-response classifications that allow universities and governments to tailor oversight rather than simply "permit or ban;" and the development of international standards bodies to coordinate norms for emerging technologies. The article concludes that as QT accelerates, research security must evolve toward collaborative, flexible, and risk-focused models capable of protecting innovation without hindering academic freedom. (more)

NSF SECURE Opportunities & Updates

NSF SECURE Analytics Expands to Include AI Partner, Finch AI

On December 9, 2025, NSF SECURE Analytics announced a new partnership with artificial intelligence (AI) company Finch AI, based in Herndon, VA. Dr. Kevin Gamache, Principal Investigator and Director of NSF SECURE Analytics, noted that he looks forward to "the ways in which the Finch AI team will amplify the potency of the Argus platform and expand our reach, enabling us to provide those throughout the research security community and beyond, with a platform to enhance their ability to make risk-informed decisions."

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.