NSF SECURE Center Research Security Briefing

Vol. 1 No. 12: September 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.

Contents

Federal Agency News & Updates

New Application Structure for NIH-Funded International Collaborations

On September 12, 2025, the National Institutes of Health (NIH) issued NOT-OD-25-155, "New Application Structure for NIH-Funded International Collaborations," providing additional information on the agency's new process for handling foreign components, as NIH announced in NOT-OD-25-104 that the agency would not issue awards for proposals that include subawards to foreign entities.

Under the process described in NOT-OD-25-155, competing applications that include one or more foreign components must submit to a Notice of Funding Opportunity (NOFO) that supports a complex mechanism activity code, including two new international project "parent" activity codes that NIH is creating: PF5 for grants and UF5 for cooperative agreements.

- NIH anticipates the new application structure being available for the January 2026 application submission cycle.
- Applications will be submitted and reviewed as a whole.
- For those applications being considered for funding, the international components will be disaggregated, and each will be assigned its own grant number with an activity code of RF2 (for grants) or UL2 (for cooperative agreements). Each RF2/UL2 will be considered its own applicant/recipient for the associated grant or cooperative agreement.
- NIH will request Just-In-Time (JIT) information from the domestic "parent" entity and any foreign components independently. If not already completed, the international project components must verify registration in SAM.gov, grants.gov, and eRA Commons.
- Each recipient organization will be responsible for its own financial reporting.
- Additional details regarding progress reporting (e.g., RPPRs) and terms and conditions of the Notice of Award will be forthcoming.
- For existing submissions, NIH is looking into a system-based mechanism of converting applications to fit the new structure, but resubmission by applicant organizations is a possibility.
- NIH will be providing additional resources, FAQs, and training for the new activity codes and application structure.

Department of Education OIRA Posting Signals HEA 117 Rule Change

The Department of Education recently posted a notice on the Office of Information and Regulatory Affairs reginfo.gov website indicating that the "Department intends to propose regulations covering institutions' reporting of statutorily defined gifts, contracts, and/or restricted and conditional gifts or contracts from or with defined foreign sources, pursuant to the requirements of section 117 of the Higher Education Act of 1965, as amended (HEA)."

Professional Association Resources & Meeting Reports

The SECURE Center and AIRI: Partnering with Nonprofit Research Institutions

In a session at the Association of Independent Research Institutes, SECURE Center Senior Advisors Jim Luther and Lisa Nichols shared community feedback gathered from AIRI's June Discovery Co-creation Stakeholder Activities (CSAs), which engaged fifteen member institutes. The session was moderated by Rosemary Madnick, Vice President for Research Administration, Lundquist Institute for Biomedical Innovation. Additional insights were gathered in a follow-up discussion with participants to further inform the next phase of resource development.

Several AIRI session participants agreed with the need for guidance expressed in the earlier CSAs on how to approach research security for faculty who are affiliated with multiple U.S. based research entities. Researchers have academic appointments through universities and research institutes and may have multiple appointments, making it challenging to track completion of requirements such as training. Tracking training through the SECURE Center's Shared Virtual Environment would help to reduce the burden associated with these arrangements. There was discussion on how to consolidate training to reduce burden, and participants echoed interest in free tools similar to Visual Compliance. There was discussion on the federal Consolidated Screening List Search Engine which participants were not aware of, but also that this free tool wouldn't provide dynamic (continuous) screening. Participants expressed that step by step guidance on how to be at least minimally compliant would be helpful as well as other free resources including in relation to foreign travel.

These discussions will help inform the SECURE Center's year 2 planning for the design and development of new resources and tools. Opportunities for continued engagement were discussed.

FDP Virtual Meeting, September 15-17

Reports from the Research Security-related sessions at the September 2025 Federal Demonstration Partnership (FDP) virtual meeting will be provided in next week's Briefing, Vol 1, No 13.

U.S. Congressional Activity

U.S. House Committees Report: Joint Institutes, Divided Loyalties

On September 11, 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, "Joint Institutes, Divided Loyalties." The report, written largely in follow-up to the Committees' September 2024 report, "CCP on the Quad," suggests that:

> *U.S.-PRC joint institutes are entities based in China that pair American universities with PRC institutions and serve as key technology transfer points. These joint institutes operate under PRC law, are run by Chinese majority boards, and are aligned with the CCP's national strategy, including its military buildup.*

Similar to the Committees' other recent report, "Fox in the Henhouse: the U.S. Department of

Defense Research and Engineering's Failures to Protect Taxpayer-Funded Defense Research," this 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 (also see Research Security Briefing No. 11).

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.

Former Defense Contractor Sentenced to Over 10 Years in Prison for Attempted Espionage (U.S. Department of Justice, 9/15/2025)

John Rowe Jr., a former defense contractor who acted as an insider threat, used his nearly 40 years of experience and access to highly classified U.S. military information to attempt to share sensitive national defense secrets with someone he believed to be a Russian agent. Rowe pleaded guilty to multiple charges of attempted espionage, including delivering and willfully communicating classified information. Despite his trusted position and security clearances, he repeatedly betrayed U.S. national security, exchanging over 300 emails and disclosing classified details in meetings with an undercover FBI agent. Rowe was sentenced to 10 years in prison. (more)

Trump administration escalates space race with China, banning visa-holding scientists from working at NASA (CNN, 9/11/2025)

CNN reports that, effective September 5, 2025, "NASA has banned Chinese citizens with US visas from participating in agency programs… [and] are no longer allowed to have physical access to NASA facilities, to join Zoom calls with their NASA colleagues or access the agency's supercomputing resources." (more)

Alien from Wuhan, China Sentenced for Smuggling Biological Materials into the U.S. for Her Work at a University of Michigan Laboratory and For Lying About the Shipments (U.S. Attorney's Office, 9/10/2025)

On September 10, 2025, Chengxuan Han was sentenced to time served (3 months) after pleading guilty to smuggling charges and making false statements to U.S. Customs and Border Protection Officers. Ms. Han will also be removed from the United States and barred from re-entry. Han, a citizen of the People's Republic of China (PRC) and a PhD student at the Huazhong University of Science and Technology, Wuhan, sent packages from the PRC containing concealed biologic material related to roundworms, addressed to individuals associated with a lab at the University of Michigan. Han was arrested on June 8, 2025, after arriving at Detroit Metropolitan Airport on a J1 visa. (more)

Russian scientists' international collaborations to be vetted by security services under new law (*Science*, 7/17/2025)

"Russian universities and research institutions will soon be obliged to report all scientific collaborations with foreign citizens to the country's security services, who will have the ultimate say over whether those projects can go ahead.

The government says the new law, signed by President Vladimir Putin on 24 June, will allow the Russian Federal Security Service (FSB) to prevent the unauthorized transfer of scientific results outside of the country, 'without violating the freedom of scientific creativity and without creating obstacles for organizations to engage in scientific activities.'" (more)

International Research Security Policy & Resources

Recent Updates to Japanese and South Korean Research Security Policy

Japan and Korea are making great strides in research security. Stung by recent, well-publicized cases of foreign misappropriation of research in academia and industry, both countries have initiated multi-stakeholder processes to raise domestic awareness of research security risk, strengthen regulations, formulate best practices, and build analytical and administrative capacity. They are sending representatives to global research security conferences, inviting international experts to local workshops to exchange perspectives, and studying developments in Australia, North America, and Europe with care. In addition, research security features in the bilateral and multilateral (e.g. G7 and OECD) consultations between the Japanese and Korean governments and their key partners on critical and emerging technologies, scientific collaboration, export controls, and international security.

Korea is explicitly adopting a whole-of-government approach to research security. Its 2023 Industrial Technology Protection Act empowers the Ministry of Trade, Industry, and Energy to protect competitiveness and national security in core technologies and other products and services. Supporting legislation prioritizes twelve national strategic technologies. In 2024, the Ministry of Science and ICT released a Blueprint for National S&T Sovereignty that defines proactive measures for technological security as a key objective. The Blueprint calls for the establishment of research security guidelines for researchers, strengthened research security systems conducive to global joint research, and robust strategic partnerships with like-minded countries. Academic research security programs are now beginning to pilot the implementation of these initiatives in coordination with government. Japan has been a member of the G7 SIGRE (Security and Integrity of the Global Research Ecosystem) Working Group since 2021. It's Ministry of Education, Culture, Sports, and Technology (MEXT) will soon pilot an analogue to the NSF TRUST program in the areas of quantum and semiconductor technology to screen proposals for risks and promote tailored mitigation measures. MEXT is also establishing regional research security contact points for universities in coordination with other government departments, as well as training programs to raise awareness across universities and researchers. Meanwhile, Japan's Cabinet Office is preparing draft guidelines on research security that

will focus on sensitive research and a national contact point to support implementation. Finally, the Ministry of Economy, Trade, and Industry (METI) is enhancing Japan's export control regime.

These are just a few of the research security initiatives being pursued in both nations. Each regards balancing openness and security in alignment with its key international partners as paramount. Together, they promise to set new standards for the region.

Safeguarding Western Tech Startups: Exploitation of International Pitch Competitions (Government of Canada, 09/08/2025)

On September 8, 2025, the Canadian Security Intelligence Service in the Canadian Government posted information on potential concerns related to international pitch competitions, with a focus on those affiliated with the Chinese government or the Chinese Communist Party (CCP), and the associated risks to startup companies. They identify primary risks such as losing intellectual property, misuse of data, or having talented individuals recruited away along with other potential risks. Specific case examples are provided along with mitigation efforts that companies can take. (more)

Research Security-Related Events & Conferences

COGR October Meeting:

Registration is open for the COGR October 23-24, 2025, meeting in Washington D.C. at the Washington Marriott in Georgetown. Preliminary agenda topics include:

- Simplifying Research Regulations and Policies: Optimizing American Science: A NASEM Report
- 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.(more)

Looking to participate in NSF SECURE Center co-creation activities or contribute to weekly briefings?
Sign up Here!