NSF SECURE Center Research Security Briefing

Vol. 1 No. 16: October 16, 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

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.

SBIR Programs Lapse (Breaking Defense, 10/8/2025; AIP 10/9/2025)
As reported by *Breaking Defense*, Senate lawmakers are at an impasse over the Small Business Innovation Research (SBIR) program, used by the Department of Defense (DOD) to provide seed funding for small companies, that expired on September 30, 2025. Critics of the program in its current form assert that a small number of SBIR recipients are receiving a disproportionately large percentage of funding. Led by Senator Joni Ernst (R-IA), they are calling for a number of revisions to the program, including a cap on the amount of SBIR funding any single company could be awarded throughout its lifetime.

In its reporting on the topic, the American Institute of Physics (AIP) noted that Ernst's proposed bill would also limit the number of proposals a company is permitted to submit per year, the number of proposals a company may submit per solicitation, and the number of concurrent projects on which an individual can serve as principal investigator.

Ernst's bill also includes research security-related provisions, including the implementation of a common definition of "Foreign Risk" for use across all participating federal research funding agencies, and the ability for agencies to revoke funding if a recipient small business provides intellectual property to a foreign country.

Sen. Peters tries another approach to extend expired cyber threat information-sharing law (CyberScoop, 10/09/2025)
Senator Gary Peters (D-MI) has introduced the Protecting America from Cyber Threats (PACT) Act, after the Cybersecurity Information Sharing Act of 2015 (CISA 2015) lapsed on September 30, 2025. The PACT Act would reauthorize the cyber threat-sharing law for another 10 years, through September 30, 2035. Peters' bill would continue the framework created under CISA 2015, which allows companies to voluntarily share cyber threat indicators with one another and with the government and continue to provide legal protections to companies that share cyber threat information in accordance with the law. The new name also potentially prevents confusion by distinguishing the Act from the agency that bears the same acronym: the Cybersecurity and Infrastructure Security Agency (CISA). (more)

International Research Security Policy & Resources

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

A firestorm implicating senior members of government has erupted over the collapsed prosecutions of two researchers in the United Kingdom. The Crown Prosecution Service (CPS) alleged that between December 2021 and February 2023 a Chinese intelligence officer commissioned from the first researcher at least 34 reports on topics of political interest, ten of which were deemed prejudicial to national security. According to the CPS, the reports reached top officials in China and included "sensitive" information supplied by the second researcher, who worked in the office of the chair of the House of Commons' Foreign Affairs Select Committee but did not have access to classified information. Both researchers were charged under the Official Secrets Act with providing information directly or indirectly useful to an enemy for a purpose prejudicial to the safety or interests of the State. The researchers maintained their innocence. Shortly before their trials were to start, in September 2025, the CPS dropped the prosecutions citing the withdrawal of a key government witness and the failure of the government to provide essential evidence. The US government has expressed concern about this outcome.

While much of the commentary about this episode has focused on its political dimensions, at least three critical lessons from it bear on research security. First, risk extends beyond the STEM disciplines that dominate the research security discourse; for example, social scientists and humanists, especially those who engage in policy work, may possess unclassified but nevertheless sensitive or non-public information about the proceedings of a meeting; the opinions and activities of an individual or office; the deliberations attending an important decision; critical social, political, and economic trends; and legislative and regulatory developments. Proper discretion may be tested when disclosure of such information is remunerated and out of the public eye.

Second, not all patrons are the same. Know your partner or beneficial client, particularly if the relationship involves professional services outside of your principal employment. Though such opportunities can be flattering and lucrative, they may be too good to be true, even when they arrive from established knowledge services firms, which may insist on preserving the anonymity of their clients when they hire outside academic consultants. Do not presume that a recruiter has performed adequate due diligence on their client or shares your risk preferences or interests. Inattention to such matters entails an assumption of risk that may yield adverse legal or reputational consequences.

Third, law enforcement is an essential but frequently unsatisfactory instrument for addressing research security incidents. Prosecutions generally occur only after alleged activities have transpired and are extraordinarily resource-intensive undertakings that cannot scale very far. Moreover, many incidents will involve behavior that falls short of illegality but nevertheless incurs harms, and the best response may not be to lower the bar by defining new crimes or expanding the scope of existing ones. Cases can turn on myriad factors. The present UK scandal and the mixed record of US research security prosecutions counsel humility about what law enforcement can achieve, and underscore the importance of adopting a layered, comprehensive, and proactive research security culture that begins at the grass roots and prevents, detects, and intervenes early in incidents well before they reach the level of potential crimes.

Research Security-Related Events & Conferences

COGR October 2025 Meeting:

Registration is now open for COGR's October 23-24, 2025, meeting in Washington D.C., at the Washington Marriott in Georgetown. Research security-related agenda topics include:

Thursday, October 23

3:45 – 4:45 pm: *Simplifying Research Regulations and Policies: Optimizing American Science – A NASEM Report*

Dr. Alex Helman, Senior Program Officer at the National Academy of Sciences, Engineering, and Medicine (NASEM), National Academies, Dr. Stacy Pritt, Associate Vice Chancellor for Research, Texas University A&M, and Dr. Lisa Nichols, Executive Director, Research Security, University of Notre Dame will discuss the new report.

4:45 – 5:45 pm: *Cybersecurity Implementation and Cybersecurity Updates from the University Perspective*

A panel of university representatives will provide updates on their institutions' efforts to implement level 2 Cybersecurity Maturity Model Certification (CMMC) requirements, including practical challenges, lessons learned, and strategies for compliance. The discussion will also cover related cybersecurity issues and how institutions are adapting to the evolving federal requirements. Panelists include Allen DiPalma, Executive Director, Office of Research Security & Trade Compliance, University of Pittsburgh, Kelly Hochstetler, Associate Vice President for Research, University of Virginia, and Thomas Burns, Associate Vice Provost, Research Compliance, Johns Hopkins University. Kevin Wozniak, COGR's Research Security & Intellectual Property Director, will moderate.

Friday, October 24

9:45 – 10:45 am: *Legislative Update & Outlook*

Joanne Carney, Chief Government Relations Officer at the American Association for the Advancement of Science and Tobin Smith, Senior Vice President for Government Relations & Public Policy at the Association of American Universities will discuss with COGR President Matt Owens the latest legislative developments and outlook for the rest of this year for federal research policy and funding. Among the issues to be discussed: FY26 appropriations for research, facilities and administrative costs reimbursement, research security, immigration issues, and more

Save the Date for ASCE 2026:

Mark your calendar 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. Registration opens November 1, 2025. (more)

NCURA 2026 Annual Meeting Call for Proposals, Due Nov. 21:
The National Council of University Research Administrators (NCURA) will hold its 68th annual meeting from August 1-4, 2026 in New York City, NY. The deadline for session proposals is November 21, 2025. (more)

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