NSF SECURE Center Research Security Briefing

Vol. 1 No. 18: October 30, 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

Professional Association Resources & Meeting Reports

COGR October 2025 Meeting: Research Security Highlights

The Council on Governmental Relations (COGR) held its October 23-24, 2025, meeting in Washington D.C. Meeting materials from the event are now available.

COGR Session: Simplifying Research Regulations and Policies – Optimizing American Science: A NASEM Report

The COGR meeting included a briefing of the recently released National Academies report, *Simplifying Research Regulations and Policies: Optimizing American Science* which presents options for federal actions to improve regulatory efficiency affecting researchers and their institutions. Dr. Alex Helman, Study Director, National Academies of Sciences, Engineering, and Medicine, served as the moderator. Speakers included committee members Dr. Lisa Nichols, University of Notre Dame, and Dr. Stacy Pritt, Texas A&M University System.

Additional details regarding the information presented in this session, including options for reducing administrative burden in the area of research security, can be found in SECURE Center Research Security Briefing Number 13. In her remarks, Dr. Helman indicated that the report has been favorably received by Congress and federal agencies and offices.

COGR Session: Cybersecurity Implementation and Cybersecurity Updates

The Council on Governmental Relations (COGR), a higher education association, held the session "Cybersecurity Implementation and Cybersecurity Updates from the University Perspective" at their October 23-24 meeting. The presentation can be found here.

Allen DiPalma, Executive Director, Office of Research Security & Trade Compliance, University of Pittsburgh (Pitt); Kelly Hochstetler, Associate Vice President for Research, University of Virginia (UVA), and Thomas Burns, Associate Vice Provost, Research Compliance, Johns Hopkins University (JHU) joined Kevin Wozniak, COGR's Research Security and Intellectual Property Director for this panel presentation. Panelists provided "updates on their institutions' efforts to implement level 2 Cybersecurity Maturity Model Certification (CMMC) requirements, including practical challenges, lessons learned, and strategies for compliance" as well as related cybersecurity issues and how institutions are adapting to evolving federal requirements.

The session began with an audience poll, which indicated the following:

- 28% of institutions plan to meet CMMC compliance for Level 1 only, 31% Level 2 self-certification, 34% Level 2 third-party assessment, and 7% eventually Level 3.
- Current readiness for CMMC compliance: fully ready 10%; active planning or assessment 70%; haven't started implementation 15%.
- Regarding implementation of CMMC Level 1: contract- or project-specific 19%; dedicated

enclaves 24%; dedicated cloud environments 20%; institution-wide 15%; more than one of these options 21%

- Number of Level 1 environments that will be registered with SPRS (Supplier Performance Risk System): Only 1 31%; 2-5 15%; 5-10 3%; unsure 51%
- Institutions biggest challenge in preparing for CMMC: Funding and resource allocation, 38%; understanding applicability and scope, 9%; coordinating across multiple departments, 44%; limited staff expertise, 5%; communicating requirements to researchers, 5%
- Who currently owns responsibility for CMMC: Central IT/information security 54%; research compliance 16%; no designated owner (yet) 22%; unsure 7%

Panelists noted that the timeline for implementing DFARS 252.204-7021 is 3 years, beginning November 10, 2025. The detailed CMMC implementation timeline is included in the slides. Initial impacts will include solicitations and vendor profiles requiring CMMC.

The UVA panelist indicated that their CMMC Level 2 preparedness was approximately 95%, while their CMMC Level 1 preparedness was to be determined. UVA has not scheduled their audit but suggested they are close regarding Level 2. Options under consideration for moving forward included the possibility of skipping Level 1 and not pursuing FCI and engaging on a project-by-project basis, using the Level 2 environment for all. They suggested that defining an environment that included physical security didn't seem possible at the institutional level. SPRS certifications will be project-by-project (with approximately 35 contracts). It was noted that prime recipients sometimes flow down CMMC terms even when the subrecipient is only conducting fundamental research (FR). Institutions need to determine their comfort level when FR is involved, but the CMMC clause is still included in the contract.

There was discussion on defining the group of central assets to include in scope and who takes ownership. It was suggested that administrative systems would be in scope if deliverables were placed there. It was noted that no single office is responsible for CMMC. The VPR's office (contracts, compliance, research security), deans and provosts, and IT are generally involved.

The JHU panelist indicated that they have a secure, compliant environment via CMMC Level 1 and 2 self-assessments but have not yet done the independent audit. They are handling classified and restricted work, but there are separate CAGE codes and management teams. At the school and department level they are not NIST compliant; however, they don't store controlled unclassified information (CUI) here (not in scope), including NIH data subject to 800-171. The need for clear governance and reporting lines was noted.

The Pitt panelist suggested that many FR institutions now have exception processes that allow for restricted research/CUI. They thought they would do something on premises. They had an experience where DoD wanted to review and approve the technology control plans that included system security plans with the 110 controls. This represented a large amount of work. Pitt also suggested that on premises gets very expensive because of manpower. They decided to step back and consider

alternative solutions, landing on use of Microsoft Azure GCC High, which is in place now.

Pitt is currently preparing for CMMC Level 2 certification with plans to initiate the process in December 2025. Their estimated five-year cost for certification and maintenance of a CUI environment is $3,287,000 (see details in the slides). They have outsourced a lot of this work. This is for one specific enclave. It represents base costs, not variable costs like computing time. They want to develop a cost model to charge back as much as possible and are working with COGR on a FAIR model along these lines. It was suggested that clear messaging is needed from leadership that researchers must use this one enclave and need to understand the limits and parameters.

Regarding offboarding the data, Pitt noted that GCC High is cloud-based and very expensive. There will be costs for the faculty member. They may look for funding at the department level. UVA set up GCC High and found it was too expensive. They ended up just using it for calls. They decommissioned that environment due to the costs for the one program which were not being recovered from the associated DoD contract. The institution still has a number of responsibilities if GCC High is used, such as training, policy, and checking logs, across different offices and functions.

An audience member noted that every system that touches CUI is in scope. This includes authentication systems if used enterprise-wide (or, alternatively, to stand up a separate system). There are pros and cons that need to be thought through. It was noted that when a project ends, CUI is still CUI. For CMMC, it was suggested that an archival solution may not be required, but the CUI implications remain.

There was a question about who serves as the institution's affirming official. Panelists suggested it must be someone at a senior level, potentially the CISO and/or CIO. They are seeing Presidents and Provosts signing. As noted previously, it impacts many areas of the institution. UVA will roll-up certifications, so the ultimate signer feels comfortable, which is likely the VPR. At Pitt, IT will do this, as they're responsible for the scoring (i.e., the CISO or Vice Chancellor who is also the CIO). At JHU, it's likely the CISO, and the panelist thought this would be the right approach, but it is not yet resolved. Background materials linked to the session description included the following:

COGR's September 2025 Update

Department of Defense Cybersecurity Maturity Model Certification 2.0

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.

Uncertainty Swirls as CMMS Rollout Nears (Defense News, 10/20/2025)

A report on how the Department of Defense's Cybersecurity Maturity Model Certification (CMMC) program is set to begin its first phase on November 10, 2025, with full implementation by 2028. The initiative aims to ensure defense contractors meet standardized cybersecurity requirements to

protect sensitive information across the defense industrial base. However, uncertainty remains, as many contractors and acquisition offices may not be fully prepared, and a shortage of certified assessors could slow compliance efforts. While some expect initial disruption, officials emphasize that the rollout will proceed as planned following years of preparation. (more)

Trump's Crackdown on Chinese Students Ignores a Startling New Reality (*The New York Times*, 10/19/2025)

Guest authors from the Australian Strategic Policy Institute argue that U.S. efforts to restrict Chinese students from studying strategic technologies at top American universities are counterproductive.

The lawmakers' rationale is that allowing Chinese nationals to study advanced science and technology in the U.S. could help China surpass America. However, the authors state that this fear ignores the reality that China has already overtaken the United States in many areas of cutting-edge scientific research.

Based on their analysis of millions of peer-reviewed papers, China ranks first globally in 57 of 64 critical technologies, dominating the top 10 institutions in most of them. Tsinghua University leads worldwide in multiple areas, including artificial intelligence and autonomous systems, while MIT, the best U.S. performer, ranks first in only two fields. If China's Academy of Sciences were included, it would be the top global institution in 28 technologies. (more)

Similar data has been reported in the 2025 Research Leaders: Leading Institutions, released in June 2025. Based on Nature Index data of "high-quality research outputs" produced from 1/1/2024 through 12/31/2024, the data show that:

- Eight out of the top ten leading institutions, globally, are Chinese.
- Harvard University, ranked at number two, is the only U.S. institution included in the top ten leading institutions.
- 25 U.S. universities were included in the top 100 leading institutions. Except for the University of Chicago (+1.9%), all of these U.S. universities experienced a decrease in output from the previous year's data, ranging from -3% to -18%.

U.S. anti-science 'Cultural Revolution' fuels unease (South China Morning Post, 10/23/2025)

A number of Chinese American researchers have noted, either independently or in interviews with the South China Morning Post, what they perceive as similarities between the Chinese Cultural Revolution and the current state of scientific research in the United States. Instigated by Mao Zedong in 1966, the Cultural Revolution sought to consolidate power and purge the nation of "bourgeois" influences. The researchers note that, while the U.S. has not seen the widespread violence associated with the China's Cultural Revolution, the potential long-term impacts to higher education and the scientific enterprise are similar. (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.

Research Security-Related Events & Conferences

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. Proposals are being accepted through noon (CST) on August 31, 2025 (more)

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 sign up for weekly briefings?

Sign up Here!