NATIONAL ACADEMIES Sciences Engineering Medicine

Assessing Research Security Efforts in Higher Education

Convened May 22–23, 2025

Proceedings of a Workshop

Assessing Research Security Efforts in Higher Education: Proceedings of a Workshop (2025)

DETAILS

106 pages | 6 x 9 | PAPERBACK
ISBN 978-0-309-59915-3 | DOI 10.17226/29241

CONTRIBUTORS

Jennifer Saunders and Steven Kendall, Rapporteurs; U.S. Science and Innovation Policy; Policy and Global Affairs; National Academies of Sciences, Engineering, and Medicine

SUGGESTED CITATION

National Academies of Sciences, Engineering, and Medicine. 2025. *Assessing Research Security Efforts in Higher Education: Proceedings of a Workshop*. Washington, DC: The National Academies Press. https://doi.org/10.17226/29241.

NATIONAL ACADEMIES Sciences Engineering Medicine

NATIONAL
ACADEMIES
PRESS
Washington, DC

Assessing Research Security Efforts in Higher Education

Convened May 22–23, 2025

Jennifer Saunders and Steven Kendall,
Rapporteurs

U.S. Science and Innovation Policy

Policy and Global Affairs

PREPUBLICATION COPY—Uncorrected Proofs

Proceedings of a Workshop

NATIONAL ACADEMIES PRESS 500 Fifth Street, NW Washington, DC 20001

This activity was supported by a contract between the National Academy of Sciences and the Department of Defense. Any opinions, findings, conclusions, or recommendations expressed in this publication do not necessarily reflect the views of any organization or agency that provided support for the project.

International Standard Book Number-13: 978-0-309-xxxxx-x
Digital Object Identifier: https://doi.org/10.17226/29241

This publication is available from the National Academies Press, 500 Fifth Street, NW, Keck 360, Washington, DC 20001; (800) 624-6242; https://nap.nationalacademies.org.

The manufacturer’s authorized representative in the European Union for product safety is Authorised Rep Compliance Ltd., Ground Floor, 71 Lower Baggot Street, Dublin D02 P593 Ireland; www.arccompliance.com.

Printed in the United States of America.

Suggested citation: National Academies of Sciences, Engineering, and Medicine. 2025. *Assessing Research Security Efforts in Higher Education: Proceedings of a Workshop*. Washington, DC: National Academies Press. https://doi.org/10.17226/29241.

The **National Academy of Sciences** was established in 1863 by an Act of Congress, signed by President Lincoln, as a private, nongovernmental institution to advise the nation on issues related to science and technology. Members are elected by their peers for outstanding contributions to research. Dr. Marcia McNutt is president.

The **National Academy of Engineering** was established in 1964 under the charter of the National Academy of Sciences to bring the practices of engineering to advising the nation. Members are elected by their peers for extraordinary contributions to engineering. Dr. Tsu-Jae Liu is president.

The **National Academy of Medicine** (formerly the Institute of Medicine) was established in 1970 under the charter of the National Academy of Sciences to advise the nation on medical and health issues. Members are elected by their peers for distinguished contributions to medicine and health. Dr. Victor J. Dzau is president.

The three Academies work together as the **National Academies of Sciences, Engineering, and Medicine** to provide independent, objective analysis and advice to the nation and conduct other activities to solve complex problems and inform public policy decisions. The National Academies also encourage education and research, recognize outstanding contributions to knowledge, and increase public understanding in matters of science, engineering, and medicine.

Learn more about the National Academies of Sciences, Engineering, and Medicine at **www.nationalacademies.org**.

Consensus Study Reports published by the National Academies of Sciences, Engineering, and Medicine document the evidence-based consensus on the study's statement of task by an authoring committee of experts. Reports typically include findings, conclusions, and recommendations based on information gathered by the committee and the committee's deliberations. Each report has been subjected to a rigorous and independent peer-review process and it represents the position of the National Academies on the statement of task.

Proceedings published by the National Academies of Sciences, Engineering, and Medicine chronicle the presentations and discussions at a workshop, symposium, or other event convened by the National Academies. The statements and opinions contained in proceedings are those of the participants and are not endorsed by other participants, the planning committee, or the National Academies.

Rapid Expert Consultations published by the National Academies of Sciences, Engineering, and Medicine are authored by subject-matter experts on narrowly focused topics that can be supported by a body of evidence. The discussions contained in rapid expert consultations are considered those of the authors and do not contain policy recommendations. Rapid expert consultations are reviewed by the institution before release.

For information about other products and activities of the National Academies, please visit www.nationalacademies.org/about/whatwedo.

COMMITTEE ON ASSESSING RESEARCH SECURITY EFFORTS IN HIGHER EDUCATION: A WORKSHOP

CHRISTINE H. FOX (*Chair*), Senior Fellow, Johns Hopkins University Applied Physics Laboratory
DEANNA D. CAPUTO, Chief Scientist for Insider Threat Capabilities and Senior Principal Behavioral Psychologist, MITRE
AMANDA HUMPHREY, Chief Research Operations Officer, Northeastern University Research Enterprise Services, and Co-Director, Northeast Regional SECURE Center
BENJAMIN F. JONES, Gordon and Llura Gund Professor of Entrepreneurship and Professor of Strategy, Northwestern University
BRUCE A. JONES, Professor and Senior Vice President for Research, Howard University
ALAN E. KOHLER JR., President, Pamir Consulting
J. MICHAEL MCQUADE, Director, Program on Emerging Technology, Scientific Advancement, and Global Policy, The Belfer Center for Science and International Affairs, Harvard University Kennedy School of Government
DEWEY MURDICK, Executive Director, Center for Security and Emerging Technology (CSET), Georgetown University
LISA M. NICHOLS, Executive Director, Research Security, University of Notre Dame

Staff

STEVEN KENDALL, Project Director and Senior Program Officer, U.S. Science and Innovation Policy, Policy and Global Affairs
TOM WANG, Senior Director, U.S. Science and Innovation Policy, Policy and Global Affairs
KARLA HAGAN, Senior Program Officer, U.S. Science and Innovation Policy, Policy and Global Affairs
KARLA RILEY, Senior Program Assistant, U.S. Science and Innovation Policy, Policy and Global Affairs (*from June 2025*)
ZARIYA BUTLER, Senior Program Assistant, U.S. Science and Innovation Policy, Policy and Global Affairs (*until May 2025*)
JENNIFER SAUNDERS, Consultant Writer

Reviewers

This Proceedings of a Workshop was reviewed in draft form by individuals chosen for their diverse perspectives and technical expertise. The purpose of this independent review is to provide candid and critical comments that will assist the National Academies of Sciences, Engineering, and Medicine in making each published proceedings as sound as possible and to ensure that it meets the institutional standards for quality, objectivity, evidence, and responsiveness to the charge. The review comments and draft manuscript remain confidential to protect the integrity of the process.

We thank the following individuals for their review of this proceedings:

NORBERT HOLTKAMP, Stanford University
NAOMI SCHRAG, Columbia University
CAROLINE WAGNER, The Ohio State University

Although the reviewers listed above provided many constructive comments and suggestions, they were not asked to endorse the content of the proceedings, nor did they see the final draft before its release. The review of this proceedings was overseen by **ANN ARVIN,** Stanford University. She was responsible for making certain that an independent examination of this proceedings was carried out in accordance with standards of the National Academies and that all review comments were carefully considered. Responsibility for the final content rests entirely with the rapporteurs and the National Academies.

Acknowledgments

We would like to acknowledge the contributions of the following individuals who made presentations at the workshop:

Alexander Angert, Federal Bureau of Investigation
Tam Dao, Rice University
Amanda Ferguson, Huron Consulting
Jeremy Forsberg, The University of Texas at Arlington
Rebecca Spyke Keiser, National Science Foundation
Susan A. Martinis, University of Illinois Urbana-Champaign
Theresa Mayer, Carnegie Mellon University
Elisabeth Paté-Cornell, Stanford University
Bhaven Sampat, Arizona State University
Naomi Schrag, Columbia University
Lori Ann Schultz, Colorado State University
Jonathan Snowden, University of Missouri-Kansas City
Jason Owen Smith, Institute for Research on Innovation and Science
Sarah Stalker-Lehoux, National Science Foundation
Gregory F. Strouse, National Institute of Standards and Technology
Geeta Krishna Swamy, Duke University
Steven H. Walker, Lockheed Martin (retired)
Stephen Welby, Georgia Tech Research Institute
Kristin (Kris) West, COGR
Michael Witherell, Lawrence Berkeley National Laboratory and University of California, Berkeley

Contents

APPENDIXES

Acronyms and Abbreviations

AI	artificial intelligence
APL	Applied Physics Laboratory
ATA	annual threat assessment
CCP	Chinese Communist Party
COGR	Council on Governmental Relations
CUI	Controlled Unclassified Information
DARPA	Defense Advanced Research Projects Agency
DCSA	Defense Counterintelligence and Security Agency
DOD	U.S. Department of Defense
DOE	U.S. Department of Energy
F&A	facilities and administrative costs
FBI	U.S. Federal Bureau of Investigation
FDP	Federal Demonstration Partnership
IP	intellectual property
IRB	institutional review board
IRIS	Institute for Research on Innovation and Science
IT	information technology
LBNL	Lawrence Berkeley National Laboratory

MOE	meeting of experts
NIH	U.S. National Institutes of Health
NIST	National Institute of Standards and Technology
NSDD-189	National Security Decision Directive 189
NSF	U.S. National Science Foundation
NSPM-33	National Security Presidential Memorandum 33
ODNI	Office of the Director of National Intelligence
OSRD	Office of Scientific Research and Development
OSTP	White House Office of Science and Technology Policy
PI	principal investigator
PRC	People's Republic of China
R&D	research and development
RoRS	Research on Research Security
S&T	science and technology
SECURE	Safeguarding the Entire Community in the U.S. Research Ecosystem
STEM	science, technology, engineering, and mathematics
TRL	technology readiness level
TRUST	Trusted Research Using Safeguards and Transparency
UIUC	University of Illinois Urbana–Champaign
UTA	University of Texas at Arlington

1

Introduction

In recent years, concerns have grown about foreign actors exploiting the openness of the U.S. research ecosystem to misappropriate scientific and technological information to enhance their nations' scientific, economic, and military capabilities. In response, new and enhanced research security measures have been put in place to protect federally funded academic research.[1] Measures have been promulgated through legislation and executive actions.[2]

Research security requirements for academic institutions currently include research security training, disclosure of funding sources in

[1] For the purposes of this proceedings, *research security* is defined as "safeguarding the research enterprise against the misappropriation of research and development to the detriment of national or economic security, related violations of research integrity, and foreign government interference." See Joint Committee on the Research Environment Subcommittee on Research Security. 2022, January. *Guidance for Implementing National Security Presidential Memorandum 33 (NSPM-33) on National Security Strategy for United States Government-Supported Research and Development*, p. 24, https://bidenwhitehouse.archives.gov/wp-content/uploads/2022/01/010422-NSPM-33-Implementation-Guidance.pdf.

[2] See, e.g., various National Defense Authorization Acts, the CHIPS and Science Act of 2022 (https://www.congress.gov/117/bills/hr4346/BILLS-117hr4346enr.pdf?utm_source=chatgpt.com), National Security Presidential Memorandum 33 (NSPM-33) (https://trumpwhitehouse.archives.gov/presidential-actions/presidential-memorandum-united-states-government-supported-research-development-national-security-policy), and its implementation guidance (https://bidenwhitehouse.archives.gov/wp-content/uploads/2022/01/010422-NSPM-33-Implementation-Guidance.pdf).

applications for federal research and development (R&D) awards, and the development of comprehensive research security plans focused on cybersecurity, foreign travel security, insider threat awareness training, and export control training and compliance.[3] These requirements are being implemented, and additional requirements are being contemplated.

To consider the impacts of current and potential research security requirements, the National Academies of Sciences, Engineering, and Medicine convened, on September 16–17, 2024, a 2-day public meeting of experts (MOE) to scope out topics and issues for a workshop that would consider how best to assess the effects of research security efforts in higher education.[4] The MOE considered working definitions, types, and goals of research security; potential frameworks for understanding research security efforts in higher education; and lessons learned from other types of related assessments.[5]

This proceedings describes the presentations and discussions at the workshop, which was organized by a National Academies–appointed planning committee and held on May 22–23, 2025, in Washington, DC.[6] The event focused on potential measures of effectiveness and performance and the data needed to assess research security and protection efforts in higher education by a range of federal agencies.[7] While the primary focus of the expert meeting and workshop is research security and protection efforts required by the U.S. Department of Defense (DOD), initiatives at the National Science Foundation (NSF) and other federal agencies were also considered.

Using the workshop discussions as input, in September 2025 a follow-up public MOE will convey the views of individual experts on how DOD specifically might organize and conduct an evaluation of the effectiveness of its research security and protection initiatives, with reference to initiatives at other federal agencies, as appropriate.[8]

[3] https://www.aau.edu/sites/default/files/AAU-Files/Key-Issues/Science-Security/Actions-Taken-Research-Security.pdf.
In addition to implementing government research security requirements, academic institutions have independently moved to address research security issues.

[4] https://www.nationalacademies.org/event/43346_09-2024_assessing-research-security-efforts-in-higher-education-meeting-of-experts-1.
Conversations on this topic are ongoing.

[5] See Appendix A for the agenda of the September 2024 MOE.

[6] Workshop planning committee biographies are available in Appendix B.

[7] For the complete workshop agenda, see Appendix C. Speaker biographies are available in Appendix D.

[8] The meeting series was sponsored by the U.S. Department of Defense.

Christine H. Fox (Johns Hopkins University Applied Physics Laboratory [APL]) workshop planning committee chair, opened the workshop by identifying several themes related to U.S. research and research security. She noted that fundamental research (see Box 1-1) is a critical component of U.S. scientific and technical leadership and essential to both national security and economic security.

Fox said that there is general agreement that there are threats to the U.S. research enterprise, threats that pose a significant challenge, not only to research institutions, but to our national and economic security. The People's Republic of China (PRC), for instance, preferentially directs fundamental research toward military needs, making collaboration a national security concern. Other nations also seek to misappropriate R&D with the aim of challenging U.S. economic security.

BOX 1-1
Types of Research

"Fundamental research means basic and applied research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community."[a] *Basic research* is defined as research "directed toward greater knowledge or understanding of the fundamental aspects of phenomena and of observable facts without specific applications towards processes or products in mind."[b] *Applied research* is concerned with solving specific problems in real-world situations. Controlled, restricted, and classified research refer to research activities where access to information or participation is limited by various factors, often involving national security or other sensitive concerns. While they share similarities, they are distinct categories with specific implications for researchers and institutions. *Classified research*, for example, involves information that is deemed sensitive enough to national security that access is restricted and controlled. *Restricted research* typically encompasses research with limitations on publication, access, or dissemination of results. *Controlled research* refers to research involving Controlled Unclassified Information or other sensitive data that requires safeguarding and access restrictions.

[a] See National Security Decision Directive 189: National Policy on the Transfer of Scientific, Technical and Engineering Information (Sept. 21, 1985), https://irp.fas.org/offdocs/nsdd/nsdd-189.pdf.

[b] See https://www.niaid.nih.gov/grants-contracts/basic-research-definition.

Fox suggested that there is broad agreement that openness, transparency, and collaboration are fundamentally important to scientific discovery—and should be protected. Although research security is necessary to protect the U.S. research ecosystem from threats, research security efforts must preserve intellectual freedom and openness. This is a significant challenge with inherent contradictions, Fox said. Despite these contradictions, everyone recognizes that recipients of federal funding have a responsibility to protect U.S. research. There are, however, cultural barriers in the research community to security initiatives.

Fox said that many have suggested that research security initiatives are already causing a decline in the number of international students at our universities and that research security policies impose costs on research institutions, weighing heaviest on smaller universities.

How large are research security challenges?, Fox asked. "How significant is the threat? . . . And are any of these research security initiatives making a difference?"

Fox suggested that there is consensus about the need to assess the results of our current research security efforts in order to better understand what is being accomplished, identify areas for improvement, and mitigate potential harm that research security initiatives may be causing to the research environment. There is also a need to assess what is being achieved through these initiatives so as to navigate the inherent contradictions about the goals of research security efforts. To do this, measures of effectiveness and data are needed. Measures of effectiveness—and the data needed to support them—are the focus of the workshop, Fox said.

Fox emphasized that research conducted in the United States has led to important innovations. The United States, she said, is recognized globally as the world's leader in science and research, discovery, and innovation. Those accomplishments come out of a culture that values intellectual freedom and collaboration—but our research is not secure. Both the research and our research culture must be protected and defended, and we need the ability to assess our efforts in this regard, Fox said.

2

The U.S. Department of Defense, Research, and the Research Security Environment

During the first workshop session, panelists and event attendees discussed the current research and research security environment. Workshop planning committee member and session moderator **Alan E. Kohler Jr.** (Pamir Consulting) introduced the session by discussing his prior work in counterintelligence at the Federal Bureau of Investigation (FBI), where one of his passions was figuring out how the Bureau could do a better job supporting the research security community. Kohler suggested that "we are all in this research security rowboat . . . paddling away as hard as we can. Every time we look . . . all we see is water" and "we are not quite sure how far along we have gotten." Compared with 5 years ago, however, Kohler said that we are in a much better (though not perfect) place, and it is an appropriate time to take stock, assess, and move on and see where we can go with research security efforts.

The session's first panelist, **Jason Day** (DOD) said that there is an urgent need to understand the impact of research security policies. He discussed the *2025 DOD Component Decision Matrix to Inform Fundamental Research Proposal Mitigation Decisions*,[1] which informs agency decisions regarding the awarding of research grants. The matrix assists with the reviewing of proposals for fundamental research for potential conflicts of interest and conflicts of commitment (e.g., the receipt of funding from a

[1] https://basicresearch.defense.gov/Portals/61/Documents/Academic%20Research%20Security%20Page/2025%20DoD%20Decision%20Matrix%20to%20Inform%20Fundamental%20Research%20Risk%20Decisions.pdf

foreign country of concern or failure to disclose a patent application that resulted from research funded by the U.S. government but filed in a foreign country of concern) and describes conditions where mitigation is required or suggested prior to the awarding of a grant.

DOD funds basic research at universities and supports the rapid transition of those technologies to the private sector or the department, Day said. Protecting this process is critical to U.S. national security and the economy.

Several categories of risks are associated with research, Day explained. Foreign influence in the research process, for example, is a high-risk concern, particularly if the research is being used to improve defense research capabilities of near-peer competitor nations.

The U.S. research enterprise is increasingly internationally focused and requires a robust ecosystem to support collaboration and stimulate innovation. Day said that DOD encourages U.S. researchers to collaborate internationally but recognizes the need to preserve openness and simultaneously protect the U.S. research enterprise against nations that wish to undermine it. To foster openness and transparency, DOD requires researchers to disclosure information about current and pending financial support and collaborations.

DOD takes a broad view in its research security evaluations, Day continued, considering not only risks but the impact of security policies on research. A secure research environment ensures that the United States can maximize technological advantage for economic and national security goals.

The session's second panelist, **Rebecca Spyke Keiser** (NSF) said that the evaluation of research security efforts is top of mind for NSF, noting that it collaborates with agency partners to ensure consistency and harmonization in research security initiatives.

The evaluation of any type of governmental policy can be challenging, Keiser said, as policy implementation takes several years and the effects of policies may manifest over several more. Therefore, evaluation of research security initiatives needs to consider not only the outcomes of policies on those conducting research but the impact of research security efforts and how well

> We need to evaluate not only "the outcomes of what people do regarding research security, but the impact of those research security efforts." "We want to evaluate research security, but we also want to evaluate how much we are continuing to maintain an open research ecosystem."
>
> Rebecca Spyke Keiser

the United States maintains an open research ecosystem supportive of innovation. There is also a need to evaluate how well research security policies support maintaining and retaining beneficial international collaborations, she said.

Keiser noted that a 2019 JASON report, *Fundamental Research Security*,[2] outlined some concerning research security issues, including the misappropriation of research and undisclosed conflicts of interest and commitment. Such issues should be balanced against the need for a vibrant science, technology, engineering, and medicine (STEM) workforce in the United States as well as international collaborations that are critical to scientific innovation, she said.

Keiser said that the JASON report includes a list of helpful questions about how to assess risk in international collaboration. These include:

- Can you readily identify the contributions of both sides of a collaboration?
- Do you know where the funding of both sides of collaboration is coming from?
- How are data collected and disseminated as part of the collaboration?

Keiser suggested that these questions could be incorporated into evaluations to assess potential risks when collaborating.

Keiser also discussed a new NSF program called Research on Research Security (RoRS) that has the capability to collect data on research security in a rigorous, hypothesis-driven manner.[3] She asked that those seeking to quantify the effects of research security policies consider applying to the program for support for research that supports evaluations of the impact of these policies.

Keiser also discussed NSF's Safeguarding the Entire Community of the U.S. Research Ecosystem (SECURE) program.[4] SECURE supports

[2] https://nsf-gov-resources.nsf.gov/files/JSR-19-2IFundamentalResearchSecurity-12062019FINAL.pdf

[3] RoRS "supports interdisciplinary, evidence-based research to enhance understanding of security risks, practices and policies to safeguard the U.S. research enterprise and foster a strong academic field in research security." See https://www.nsf.gov/funding/opportunities/rors-research-research-security-program.

[4] SECURE's mission is to "share information and reports on research security risks, provide training on research security to the science and engineering community and serve as a bridge between the research community and government funding agencies to strengthen cooperation on addressing security concerns." See https://www.nsf.gov/news/nsf-backed-secure-center-will-support-research.

research security efforts in the research community, including by providing clarity regarding principled international collaboration in science. SECURE requires recipients of funding to conduct an internal evaluation of their research security program, including impacts on the research itself. SECURE can also assist in evaluating the impact of research security policies. NSF is funding SECURE through a cooperative agreement, which allows for engagement with multiple agencies, including on the development of evaluation measures.

Panelist **Alexander Angert** (FBI) said that "the U.S. has the most robust research ecosystem of anybody on the earth, and this has put us in the forefront of scientific discovery . . . generation after generation." This is "something we want to protect, not treat lightly. It's central to our national interests, including our security and economic prosperity. . . . If this is to continue, we need to be able to keep attracting the best and brightest talent from around the world to study here, work here, and hopefully even put down roots here." The United States, Angert said, needs foreign talent, including from China. Each Chinese researcher who is not tied to military civil fusion entities and who makes their home in the United States grows the talent pool.[5] Nevertheless, Angert said that the research security threat from China is real.

> "The U.S. has the most robust research ecosystem of anybody on the earth, and this has put us in the forefront of scientific discovery. . . generation after generation." This is "something we want to protect, not treat lightly. It's central to our national interests including our security and economic prosperity." "If this is to continue, we need to be able to keep attracting the best and brightest talent from around the world to study here, work here, and hopefully even put down roots here."
>
> Alexander Angert

Angert noted that, in the last 6–7 years, the United States has taken steps to protect its research ecosystem. He said that there are now far fewer Chinese Communist Party (CCP) researchers in the United States, including those with assessed military civil fusion ties. He noted that

[5] "Military-Civil Fusion," or MCF, is a national strategy of the Chinese Communist Party (CCP). Its goal is to enable the Peoples Republic of China "to develop the most technologically advanced military in the world." "A key part of MCF is the elimination of barriers between China's civilian research and commercial sectors, and its military and defense industrial sectors." See https://www.state.gov/wp-content/uploads/2020/05/What-is-MCF-One-Pager.pdf.

U.S. Presidential Proclamation 10043, which was signed by President Trump in 2020, has increased travel screening and security restrictions.[6] Universities have taken action to implement network security policy management efforts and are proactively identifying researchers who are not in compliance with research security requirements. Federal security requirements now make it harder for individuals to conduct illicit activities and easier to identify those who do (and to stop them). Angert pointed out that research security requirements also reduce the ability of Chinese students in the United States, who have a high risk of being exploited by CCP authorities, to operate as nontraditional collectors of intellectual property (IP). Angert noted, however, that as research security policies have evolved, threat actors seeking to exploit our open academic environment have developed new approaches to leverage the U.S. research enterprise to their advantage.

Angert said that China refers to U.S. research security measures as a technology blockade and is taking efforts to undermine the U.S. system. He asserted that China and other competitors have obscured government funding sources and obtained information about the products of U.S. research from third-party collaborators. Angert said China is conducting persistent and sophisticated cyber operations against the United States. Despite a 2015 U.S.–China cybersecurity agreement, the U.S. government is aware of efforts that, while not necessarily illegal, are unethical and nontransparent.[7] These include the unauthorized sharing of prepublication research data, obtaining advanced access to grant proposals, and attempts to influence the grant approval process.

Angert sees the FBI's mission as safeguarding science and the research and development ecosystem by raising awareness about the objectives of adversaries. The Bureau is working to empower the research community by educating it about how to identify and manage potential anomalies. It has academic coordinators in all 55 of its field offices. Angert said that these individuals are the linchpin of the Bureau's academic engagement efforts. In addition, he noted that the FBI's National Cyber Investigative Joint Task Force, which is co-led by DOD, has within its purview academic and other

[6] Trump, D. J. 2020, June 4. "Proclamation 10043—Suspension of Entry as Nonimmigrants of Certain Students and Researchers from the People's Republic of China." *Federal Register* 85(108): 34353–34355, https://www.federalregister.gov/documents/2020/06/04/2020-12217.

[7] As part of the agreement, the United States and China agreed to not conduct government-sponsored economic espionage in cyberspace. See, e.g., https://jsis.washington.edu/news/u-s-china-cybersecurity-cooperation.

research institutions and labs that work directly with their respective FBI field offices.[8]

Angert said that research security is a big undertaking, and federal agencies and academic institutions must be partners in this work. The FBI, he said, wants to support academia and other institutions in identifying any issues as they arise: "We have a common goal which is to ensure that great research can continue to happen in the United States and is not compromised by bad actors exploiting the openness that makes it possible."

Session panelist **Michael Witherell** (Lawrence Berkeley National Laboratory [LBNL] and University of California, Berkeley) said that LBNL, which is owned by the Department of Energy (DOE) but managed by the University of California, conducts unclassified work. He said that LBNL has a well-managed research environment with a robust research security program. Lab reviews, external partnerships, and technology transfer agreements support the goal of advancing U.S. economic competitiveness and national security.

Witherell said that Chinese researchers are well integrated into universities conducting military research, nonmilitary institutes, and private companies. He observed that Chinese nationals working at U.S. institutions are likely to be interrogated when they return home to renew their visa. This can create anxiety and hesitancy about their research in the United States and put a damper on their ability to contribute to innovative research.

As a laboratory director, Witherell said that he works with his senior leadership team on research security issues. Threats are managed using a layered approach, wherein information is available to individuals to assist in the management of research security procedures, tools, and infrastructure. Witherell said, when managed properly, R&D on critical sensitive technologies can be conducted in the same institution where unclassified and nonsensitive research is conducted.

All foreign nationals requesting access to LBNL are vetted, Witherell explained, and enhanced vetting is performed for individuals who have associations with nations of concern. Everyone "badges in" when entering and exiting research buildings.

[8] The National Cyber Investigative Joint Task Force was established in 2008 and includes more than 30 partnering agencies from across law enforcement, the intelligence community, and DOD. The Task Force coordinates, integrates, and shares information related to cyber threat investigations to support intelligence analysis for decision-makers. See https://www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force.

DOE labs have developed a science and technology risk matrix to identify and protect R&D on critical and emerging technologies.[9] It "uses a Red/Yellow/Green categorization scheme to quantify the risk associated with a given topic and the resulting level of controls that are required."[10]

Witherell noted that DOE is the only civilian science agency with its own counterintelligence program. LBNL participates in this program and DOE counterintelligence offices serve all national labs. The program monitors close calls which, in turn, inform evaluation efforts.

The final session panelist, **Stephen Welby** (Georgia Tech Research Institute), began his remarks by noting that the world is a competitive environment. Research capacity is fundamental to the United States and its economic and national security, he said. The United States's economic and national security strategies depend on maintaining technical advantage for economic development and national security.

Welby said that DOD "has a vested interest in ensuring that the research that it funds does not inadvertently advance the interests and ambitions of our competitors and adversaries. Beyond that . . . every American citizen has a right to expect an appropriate return on investment on . . . tax dollars that get invested into federally funded research and development." Return on investment is measured in terms of the advantage to the United States—not its competitors.

> "The Department of Defense has a vested interest in ensuring that the research that it funds does not inadvertently advance the interests and ambitions of our competitors and adversaries. Beyond that . . . every American citizen has a right to expect an appropriate return on investment on . . . tax dollars that get invested into federally funded research and development."
>
> Stephen Welby

Welby said that it is important to have strong metrics to assess research security, noting that current assessments of research security efforts may not capture their impact. Research security policies often focus on issues such

[9] The DOE's Science & Technology Risk Matrix is intended to "highlight areas of emerging and potential concern associated with economic and/or intellectual competitiveness." See https://www.directives.doe.gov/terms_definitions/science-and-technology-risk-matrix-s-t-risk-matrix. Research institutions are looking at such matrices as potential models for their own research security efforts.

[10] See DOE. 2022, December 17. *Introduction to the Science & Technology (S&T) Risk Matrix*, https://www.energy.gov/science/articles/science-technology-risk-matrix.

as conflicts of interest or affiliation with countries of concern but do not evaluate how they are affecting research or researchers directly.

Nearly all the U.S. R1 universities focus on fundamental research, the results of which are not subject to export control laws and regulations.[11,12] Agency requests for research proposals often begin with preambles that ask about the economic and national security impacts of the proposed research even if the research is described as fundamental, Welby said. Grantmakers must ensure, he said, that any designation for fundamental research that could significantly impact national or economic security is clear. If we are going to recognize the role of fundamental research in our competitive advantage in the United States, Welby said, it should be treated as such: unless "we're measuring that, we may be measuring the wrong thing."

DISCUSSION

Kohler asked panelists to comment on whether an understanding of research security varies based on where staff sit within an institution. In response, Witherell said that, while vice chancellors, vice presidents of research, and deans of research seem to have a strong understanding of research security issues, faculty may not. He emphasized the importance of being "explicit at the beginning what we're protecting, because if you try to protect everything, you protect nothing."

> "We have to be explicit at the beginning what we're protecting, because if you try to protect everything, you protect nothing."
>
> Michael Witherell

Welby said that it is important to identify sources of leakage in the U.S. R&D enterprise, noting that the FBI has identified individuals who have attempted to participate in the U.S. research ecosystem who are agents of foreign powers. We also need to pay continued attention to cybersecurity, the vulnerabilities of proprietary information, and national security information, he said.

Foreign involvement and ownership of critical technology firms is also an issue. If one were to examine and rank the risk associated with foreign

[11] R1 institutions have very high research spending and doctorate production.

[12] Welby defined *fundamental research* as research in science and engineering or mathematics that is typically published and shared widely within the research community without proprietary national security restrictions. For a discussion of fundamental and other types of research, see Box 1-1.

involvement and ownership of technology, it suggests that there are other areas where we should be investing resources preferentially, Welby said. "As we think about deploying resources to counter broader threats to our ecosystem, we should be asking what's the best way to get return on that investment."

> "As we think about deploying resources to counter broader threats to our ecosystem, we should be asking what's the best way to get return on that investment."
>
> Stephen Welby

Kohler noted that there have been discussions about the need for research culture to be more security minded, but that achieving such a culture change could involve additional requirements that would increase researchers' workload. Day said that DOD is mindful of the burden that research security policies may impose when it develops new research security policies, and the agency is trying to make its processes more transparent. One approach is to provide the university community with specific details about what DOD is looking for during research security reviews, Day continued. DOD has also developed training resources jointly with NSF on research security. The agency is also working to share anecdotes and information about research security to help faculty understand what DOD is seeking during proposal review.

The SECURE Center is an important resource for the university community, Kohler added. As a clearinghouse for information for the research community, the Center will encourage the sharing of reports on research security risks and offer related training. By doing so, its aim is to build trust and improve communication between faculty and university administrations and federal agencies.

Kohler asked panelists to identify research security measures that should be changed or specific data that might help inform decision-making. Day said that information about Ph.D. flows between other countries in high-talent STEM areas could help DOD assess the impact of research security policies. Angert said that more openness from universities about suspicious activity and anomalous indicators would be useful. Witherell added that universities need to develop tools to manage research security issues related to postdoctoral programs. Welby said that assessments of the effects of research security policies could measure costs associated with implementation. It is harder to measure awareness of research security issues, he said, but surveys could be used to assess researchers' situational awareness of research security challenges. Surveys could also be informative for developing metrics on resistance to research security policies, including

> "The hardest thing to measure is effectiveness. . . . I only know after the fact whether I've actually been able to mitigate a particular risk, and I have to prove a counter positive" (i.e., that something did not occur as a result of the risk mitigation measures. "And we've wrestled for a long time with how to be able to do that—we would use sampling or other processes and other measurement techniques [but] that's not viable in a large social system like this. . . . Ultimately, there is going to be the gap in terms of measuring how effective these tools are. It's kind of a losing proposition. You'll only know when you fail."
>
> Stephen Welby

about perceptions that policies are discriminatory.

"The hardest thing to measure is effectiveness," Welby said. "I only know after the fact whether I've actually been able to mitigate a particular risk, and I have to prove a counter positive" (i.e., that something did not occur as a result of the risk mitigation measures). "And we've wrestled for a long time with how to be able to do that—we would use sampling or other processes and other measurement techniques [but] that's not viable in a large social system like this. . . . Ultimately, there is going to be the gap in terms of measuring how effective these tools are. It's kind of a losing proposition. You'll only know when you fail."

Workshop planning committee member **Lisa Nichols** (University of Notre Dame) asked what kind of data the FBI was collecting on the unauthorized transfer of prepublication academic fundamental research. Angert said the agency has looked at data on the number of cases and prosecutions related to the theft of IP, but those data do not apply in this space. He said that, ideally, as research security policies and procedures are implemented, the research ecosystem will become more resilient and better able to stop threats. This will ultimately result in fewer cases of abuse.

Angert said that it is challenging for the FBI to collect data on the theft of fundamental research. However, academic coordinators in field offices with expertise in particular areas of research may have insight into key technologies that may be at risk.

Welby said that the "best measurement we could have is the impact of the things that we're doing on the behavior and perceptions of those who do not have our best interests in mind." This is a very difficult task. Workshop planning committee member **J. Michael McQuade** (Belfer Center for Science and International Affairs, Harvard University Kennedy School of Government) added that the research security community also needs to ask whether "we are having a negative impact on our ability to go fast and deliver."

> "The best measurement we could have is the impact of the things that we're doing on the behavior and perceptions of those who do not have our best interests in mind."
>
> Stephen Welby

Day said that research outflows are another area for evaluation. Where individuals go after they have completed their research and who they collaborate with are areas of critical interest. Angert suggested that adversaries may be more interested in fundamental research as it lays the foundation for technology development. When looking to protect AI, quantum, and aerospace technologies, fundamental research may need to be an area of focus, he said. For researchers at academic institutions or research centers, publications and data are important tools. If the researcher is a person of concern, access to such resources may need to be controlled.

Fox asked participants to comment on barriers to information-sharing on research security. Day suggested that it could be beneficial if DOD was able to release more information about the research reviews they conduct. Additional information from the counterintelligence community could also be beneficial, he said.

Welby noted that, since National Security Presidential Memorandum 33 (NSPM-33) was issued, the pattern of prosecutorial success on matters related to research security has not been significant.[13] Prosecutorial successes could be a metric, he said, if there were a significant number. What is clear and measurable is the cost implications of the implementation of research security policies on campus—though such costs are necessary to protect research, he said. He also noted that the costs of research security measures are showing up as indirect costs just as caps are being imposed on indirect cost recovery.[14]

[13] White House. 2021, January 14. *Presidential Memorandum on United States Government–Supported Research and Development National Security Policy*. Executive Office of the President. https://www.whitehouse.gov/wp-content/uploads/2021/01/NSPM-33-Research-Security-Memo.pdf.

NSPM-33 aims to protect U.S. federally funded research from foreign government interference and misappropriation while maintaining an open research environment. The memorandum mandates that research institutions receiving more than $50 million annually in federal research funding establish research security programs.

[14] NSF, DOE, and the National Institutes of Health have all announced policies to cap indirect rates on grants and cooperative agreements at 15 percent. See, e.g., https://www.nsf.gov/policies/document/indirect-cost-rate, https://www.energy.gov/articles/department-energy-overhauls-policy-college-and-university-research-saving-405-million, and https://grants.nih.gov/grants/guide/notice-files/NOT-OD-25-068.html.

Fox said that there is a need for trusted relationships between federal agencies and universities. She suggested that relationships could be improved through information-sharing between the federal government and universities.

Nichols said that it sounds as if DOD is tracking the number of security reviews, the number of proposals rejected, and risks that were identified. She expressed an interest in having that information made public and asked if DOD was tracking scientific and international research impact broadly.

Day said such tracking is challenging because it takes several years for these things to manifest. He noted, for example, that publications, a common metric to track, can appear as many as 5 or 10 years after a collaboration took place.

Kohler said that people are by far the most important aspect of research security. He suggested that research security is about innovating around our adversaries while our security apparatus holds them back. The focus, he said, should be protecting people and encouraging them to stay in the United States. It is important to talk about success stories and point to the numbers who come to the United States, remain here, and contribute to American society.

Welby said that a clear measure of success is the fact that the U.S. system of research remains attractive to the world's best and brightest researchers. A successful research enterprise is an accelerant and an enormous economic advantage. While difficult to quantify, success is apparent in the numbers of companies formed and the pace of research production. Day said that it is also important to account for those researchers the country is losing.

3

Research Security Policies and Requirements: Scope and Measures of Effectiveness

McQuade moderated a panel that discussed how to measure the effect of research security policies and requirements. He reiterated that the overall goal of the workshop was to examine the effectiveness of efforts to protect national security in the operation of federally funded research at universities. He also noted that that the previous session provided context for an examination of the DOD research security ecosystem and broader research ecosystem and said that the intention of the current panel was to consider how security outputs are to be measured or could be measured, the effectiveness of controls, and the impact of controls on the outputs of the U.S. research enterprise.

The first panelist, **Tam Dao** (Rice University), discussed how Rice approaches research security. He said that the university's goal in its research security efforts is to safeguard the means, know-how, and products that originate from its research ecosystem. This requires awareness, education, training, foreign influence risk assessment, and strong partnerships. Dao suggested that many in academia are unaware of research security threats.

Research security programs at Rice emphasize awareness, education, and training. The university's research security training focuses on foreign influence, Dao said. While there are many training programs available, he noted that effective training allows researchers to develop skills for identifying the best approaches for addressing potential research security risks.

Dao emphasized the importance of partnerships in research security. Rice University works closely with federal partners on research security;

Dao described an initiative where the FBI held classified briefings where individuals from the academic sector could provide input on (and provide examples of) research security issues of concern. In a manner similar to academic peer review, this allowed the agency to solicit expert input and feedback.

Dao discussed the university's work on foreign influence risk assessment. As faculty engage in many types of relationships, whether as part of a collaboration, partnership, or engagement with a visiting scientist, it can be complicated for them to navigate research security issues (see Figure 3-1). Faculty may not, for example, be sensitized to the possibility that their contacts are subject to foreign influence.

When it comes to research security, assessing risk is complicated, Dao said. There are no mathematical formulas to assess research security risk, and to be successful, he continued, a research security program must ensure that faculty have access to the information they need to make well-informed decisions about risks.

The second panelist, **Elisabeth Paté-Cornell** (Stanford University), discussed her work in risk analysis and scenarios, probabilities, and outcomes related to research security. She said that a consideration of uncertainty is particularly important for research security as nothing can be known for certain except what has been observed directly. In considering risks related to research security, Paté-Cornell said that it is important to consider:

- Who are the adversaries, what do they want, what might they get, how might they get it?
- What can adversaries do with it and how will it affect U.S. security and defense in particular?
- What can be done to prevent it?
- How effective are the current methods?
- How can we improve them?
- What can one expect by the results?

Paté-Cornell said her interest is in what a technology will do in a conflict and what will be the effect. To assess risk, Paté-Cornell said that we should consider which technologies are most critical to U.S. national and economic security. These may include semiconductors, quantum computing, artificial intelligence, bioengineering, nuclear engineering, and manufacturing methods. A next step would be to consider the potential utility of these technologies to Chinese industry and defense. It is particularly important, she said, to consider which technologies can be leveraged in conflicts as this can be helpful in identifying potential areas of risk.

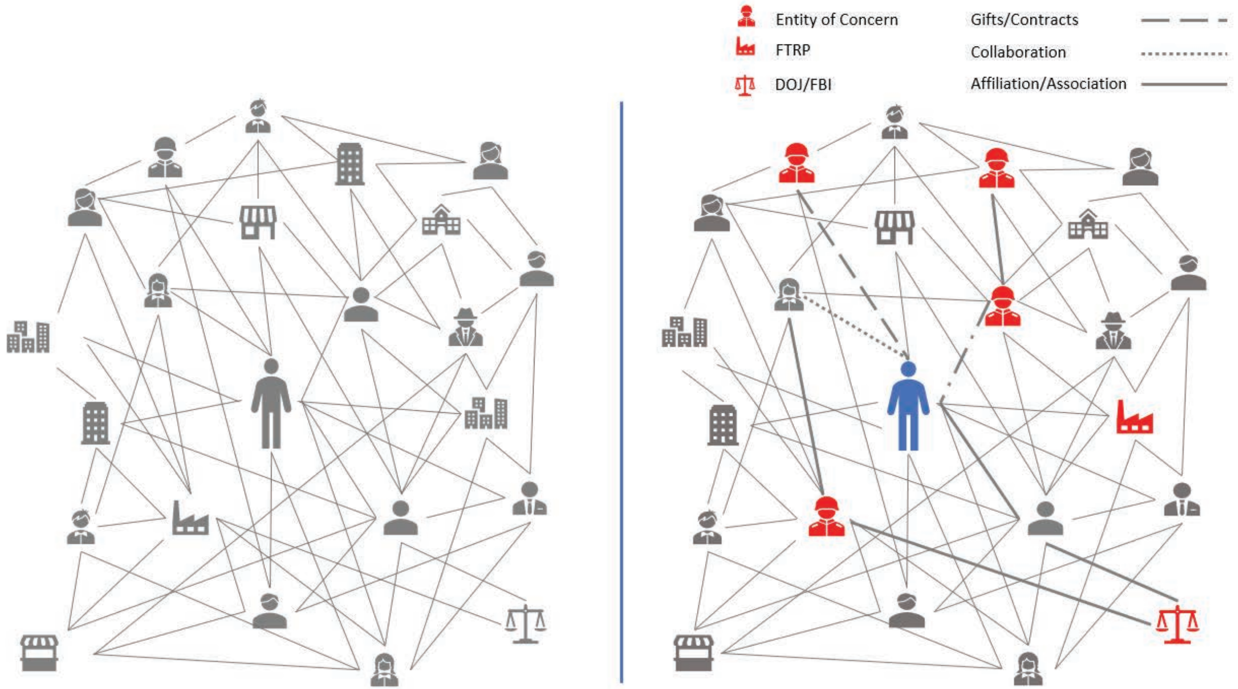

FIGURE 3-1 Foreign influence risk assessment.
SOURCE: Tam Dao, Associate Vice President, Campus Safety and Research Security and Baker Institute Rice Faculty Scholar, Rice University. May 22, 2024, Workshop Presentation.

Paté-Cornell said that it is important to consider how to protect research in instances where the United States leads in industry and academia. She suggested that, to support research security efforts, research results related to critical technologies need to be identified and classified, if necessary, and controls put on publications.

Risk analysis requires examining where critical problems arise, Paté-Cornell asserted. In one scenario, she noted, the Chinese conducted cyberattacks on U.S. quantum computing centers. These attacks carried significant security risks, slowed U.S. technology development, and had an adverse effect on U.S. military operations.

Panelist **Sarah Stalker-Lehoux** (NSF) said that the ideal measure of the effectiveness of research security programs would be reducing undue foreign interference in the U.S. research ecosystem. For Stalker-Lehoux, the question is how to reduce interference while also encouraging international collaboration. She said that, for national security reasons, it is critical that the United States remain the top science and technology destination in the world.

Stalker-Lehoux said that, while it may be possible to measure the effectiveness of research security policies, the U.S. research ecosystem is currently at a stage of implementing research security requirements.

Stalker-Lehoux said that cybersecurity is an important aspect of research security programs. In the fundamental research space, it is critical to establish cybersecurity standards. She said that the National Institute of Standards and Technology (NIST) has a research security program that uses a risk-based methodology to assign security countermeasures to adequately safeguard the agency's scientific research and IP. However, Stalker-Lehoux suggested that there is a need for more input from others in the scientific community on cybersecurity measures.

Stalker-Lehoux emphasized the importance of human capital and talent in discussions of research security. NIST will be working with National Academies' Federal Demonstration Partnership (FDP)[1] and EDUCAUSE[2] to assess human-capacity needs for research security. "Along the way,

[1] The FDP "is an association of federal agencies, research policy organizations and academic research institutions with administrative, faculty and technical representation." Its "mission is to streamline the administration of federally sponsored research and create resources that are available to the research enterprise regardless of membership status." See https://thefdp.org.

[2] EDUCAUSE is a is a nonprofit association whose mission is to advance the strategic use of technology and data to further higher education. See https://www.educause.edu.

through constant engagement and dialogue, we can continue to . . . pivot." But the ultimate goal is to develop "standards of measurements and success," she said.

While recognizing that it is hard to measure, Stalker-Lehoux said that increased awareness of research security could be a sign of the effectiveness of research security policies and requirements. She suggested that counting the number of research security trainings completed could be a way to gauge awareness. She cautioned, however, that it is not clear whether training is effective or sufficient.

Stalker-Lehoux said that researchers must understand the importance of openness and transparency in research. "These are the fundamental values that we all aspire to achieve in our research," she said, "but we have to be cognizant that the landscape has changed." She noted, for example, that researchers that have been coerced by adversarial governments into sharing research.

Stalker-Lehoux said that building awareness about research security is a responsibility of the agencies funding research. NSF recently instituted a review process for proposals to assess active appointments and research funding to identify institutions that might pose a research security risk. Stalker-Lehoux suggested that, if researchers decline to collaborate with foreign institutions that do not pose a risk, this will reduce our scientific and technological advantage.

Stalker-Lehoux said that research security "is a shared responsibility. We can't do it on our own. And empowering everyone to have the tools that they need and the knowledge that they need to say, 'Okay, this is the amount of risk in the situation, but it's okay, I'm going to be risk tolerant' or 'This is too much risk.'"

Stalker-Lehoux said that, while NSF funds 45,000 proposals annually, its research security unit has the capacity only to closely review quantum information science and some AI and dual-use research of concern-related proposals. Awareness-building and empowering institutions to support researchers in research security is critical, as is mitigating risk. The more that can be done to support those in the community that might be attracted to participate in foreign talent programs, the better.[3] This includes equipping them with information and resources.

[3] *Foreign talent programs* are initiatives that are organized, managed, or funded by a foreign government or entity for the purpose of recruiting subject matter experts. These programs often involve compensation for individual researchers in exchange for specific research activities or obligations that may create risks for the U.S. research enterprise.

Panelist **Steven H. Walker** (Lockheed Martin [retired]) noted that the global strategic environment has changed over the last 5–10 years, as the United States has moved toward military and economic competition with several peer adversary nations, particularly China.

Walker said that the PRC's spending on R&D grew from $14 billion in 1996 to about $670 billion in 2021 and that China is making significant investments in technology development. He noted that China uses technology for illicit purposes, such as to assist in the acquisition of foreign technologies.

Walker said that NSPM-33 was a good step forward and that the CHIPS in Science Act was helpful "in identifying at least a list of technologies that we need to be concerned about."[4]

The use of uniform disclosure forms across federal agencies helps to scale research security efforts consistently across agencies. Walker said that clear standards for research security training on cybersecurity, expert control, and foreign travel security are important. Eliminating conflicts of interest with foreign governments and ensuring that researchers understand conflicts of interest is a must.

Walker said that, while industry has largely been absent from conversations about research security, it could be a strong partner. Lockheed Martin and other industry partners have initiatives that evaluate the sensitivity of research awards to universities and consider whether the research is an area targeted by foreign adversaries. Hypersonics is one example of a targeted research area; Lockheed Martin works to ensure that any hypersonics research is conducted by trusted researchers. The company gives particular scrutiny to research projects that involve proprietary information. The company also trains employees who work with university researchers.

[4] The CHIPS and Science Act of 2022 (Public Law No. 117-167) includes several provisions aimed at enhancing research security across U.S. science and technology sectors. For example, the Act mandates that NSF maintain an Office of Research Security and Policy within the Office of the NSF Director, prohibits participation in foreign talent recruitment programs that pose a threat to U.S. research security, and requires that institutions receiving federal research funding provide training on research security for all covered personnel. Furthermore, the Act mandates the creation of a Research Security and Integrity Information Sharing and Analysis Organization to facilitate the sharing of information related to research security threats and best practices among research institutions. It also tasks NSF with developing an online resource containing up-to-date information tailored for institutions and individual researchers to support compliance with research security requirements as well as a program to support research on research security.

Conversations about research security have mostly been between government universities, Walker said, but industry should be more involved. "The more the government . . . can bring in industry to help with [research security] the better," he said. The connection to industry is critical for assessing the vulnerabilities of basic research

Walker noted that allowable university overhead rates are decreasing while government compliance requirements, including research security–related compliance requirements, are increasing. This is not sustainable, he said.

Walker said the university culture will need to change for research security to become a campus priority. "If you're going to be secure and protect information you're going to have to" change "culture and mindset," he said.

Walker said that the line between fundamental and applied research needs to be clearer. Security is important, but fundamental science should not be inhibited. "We do not want to slow down this engine of ingenuity and innovation," he said. More consideration is needed of how parties can work together to provide a secure environment for technological development.

DISCUSSION

McQuade asked Walker to comment on how current research security programs and policies build on earlier policies.

Walker said that the whole ecosystem has changed over time. Universities now play a more significant role in technology areas that are critical to national security, and there is a need to step back and consider research security in this new environment. He said that if universities are conducting applied research important to national security, it may be necessary to conduct such research at a secure facility or institute that can carefully vet researchers. He suggested that fundamental research should be conducted in unrestricted environments so that it may flourish as it always has. Paté-Cornell added that the Air Force Scientific Advisory Board[5] and the Army Science Board[6] could also contribute to conversations about the performance of applied and fundamental research as they often act as intermediates between the universities and the larger ecosystem.

Nichols asked how, if research is not restricted, the U.S. government would have institutions protect open fundamental research that ultimately will be published. Research institutions are not trying to restrict fundamental research, she said, and there are concerns about leakage in that space.

[5] See https://www.scientificadvisoryboard.af.mil/.

[6] See https://asb.army.mil/.

Walker suggested separating out fundamental research but identifying technology areas and research that can easily be moved into applied research.

McQuade said that the National Academies recently published a report that examined the protection of technologies that have strategic importance for national security.[7] The report raised a question about whether it is possible to conduct both open and restricted research simultaneously on university campuses. He said that, in many instances, academic institutions elect not to conduct sensitive research.

McQuade asked Dao and Stalker-Lehoux about measuring the effectiveness of research security policies and the data needed to do so. Dao said that Rice University has about 300 faculty and a team of five focused on research security. For Rice, one measure effectiveness is the number of times faculty or administrators engage with his office on research security issues. He added that the university is moving away from generic training and toward an approach that favors one-on-one interaction with faculty. When meeting one-on-one with faculty, he said, he and his staff develop a written research security technology plan to guide researchers as they conduct research. They also collect faculty feedback about research security issues, including via surveys. Data are reported to the university's executive vice president and used to determine whether research security efforts are helpful to the research community.

Stalker-Lehoux said that NSF is measuring the number of research security–related inquiries originating inside the agency, as the numbers provide an indication of awareness. The agency is also reviewing how many proposals require risk mitigation.

Stalker-Lehoux said that there is a need for data-sharing among federal agencies, including with DOD. NSPM-33 describes requirements around information-sharing that may be informative.[8] Shared data must be

[7] See National Academies of Sciences, Engineering, and Medicine. 2022. *Protecting U.S. Technological Advantage*. The National Academies Press, https://doi.org/10.17226/26647.

[8] NSPM-33 states, "Heads of agencies shall share information about violators (e.g., those who violate disclosure or other policies promulgated pursuant to this memorandum, participate in foreign government-sponsored talent recruitment programs . . . or whose activities clearly demonstrate an intent to threaten research security and integrity) across Federal funding institutions and with Federal law enforcement agencies, the DHS, and State, to the extent that such sharing is consistent with privacy laws and other legal restrictions, and does not interfere with law enforcement or intelligence activities. . . . Heads of agencies should consider providing notice to other Federal funding institutions in cases where significant concerns have arisen but a final determination has not yet been made. Where appropriate and consistent with applicable law and appropriations, funding agencies shall include within grant terms and conditions provisions that allow for such information sharing."

objective and factual because different agencies may make different decisions about risk mitigation based on the same information. Stalker-Lehoux said that developing data-sharing capacity has been a slow process, but that headway is being made.

Stalker-Lehoux said that agency differences in risk tolerance are a challenge. She challenged the research community to collect data to inform risk tolerance. While there may be great benefits to cooperation, that would be lost without a firm understanding of the risks. "We can benefit from that cooperation," she said, "even if it is with a researcher from a risky institution."

Kohler suggested that the NSPM-33 should have been accompanied by funding for universities to collect data. A key question is how much time an investigator spends on research security requirements versus core research. Dao said that it is not clear how much is being spent, as the question has not been studied. He surmised that much of researchers' time, particularly those receiving mitigation letters, is spent identifying past collaborations. Faculty who publish more frequently are more likely to be targeted for collaboration by foreign adversaries and those targeted by foreign adversaries are more likely to have been engaged in potential collaboration.

Nichols asked about how to address inconsistencies between agencies on research security policies, such as on risk tolerance. Stalker-Lehoux said that, when NSF was developing its risk framework, they asked DOD whether their framework should be consistent with DOD's. While the agency was advised to take a nuanced "NSF" approach, she said that it is only through information-sharing that agencies can appreciate different approaches and risk mitigation efforts.

Workshop planning committee member **Deanna D. Caputo** (MITRE) said that faculty may be hesitant to take research security training or do not want training, suggesting that language around training should emphasize education, awareness, and behavior change. Changing the culture around research security is critical, she said: "We cannot expect good measurement of effectiveness if we do not know how far that culture changed."

Paté-Cornell suggested that one approach might be to share examples of real cases where U.S. research has been given to the Chinese, what was done with it, and why the acquisition was bad for the United States. Stalker-Lehoux said that, when NSF presented an example to staff of a proposal that had a risk mitigation plan, it generated a lot of conversation.

Positive examples of successful research security measures will also incentivize people to be honest and forthcoming about research security. "Framing matters," Stalker Lehoux said. Rather than describing framing issues in a "scary, geopolitical context" where "everyone is going to get in trouble for collaborating," she suggested describing examples in a manner where individuals understand that there are always risks. Furthermore, it is important to be thoughtful and keep research transparent, open, and secure.

Workshop planning committee member **Amanda Humphrey** (Northeastern University and Northeast Regional SECURE Center) asked about data that might be available to help institutions calibrate how many staff are needed to support research security programs. Dao said that, to make decisions, universities can use a triage model that considers the needs of their institution, areas of expertise, whether work touches on critical infrastructure, the types of populations involved, and potential risk of the work.

Workshop planning committee member **Dewey Murdick** (Georgetown University) suggested that institutions are starting to make decisions about where to apply for funding on the basis of research security considerations. He asked if there are data on this or plans to capture these data. Walker said that, while he does not have data, this is a critical point. Stalker-Lehoux has heard anecdotally that some institutions do not want address research security restrictions and suggested that this is why NSF and others are trying to further "a risk-tolerant approach to research security."

Fox observed that session panelists talked about research security and risk in terms of type of research (e.g., fundamental or basic research versus applied research). As some areas of research present more significant risk than others, she asked for comments on how to conduct a risk analysis by research topic. Paté-Cornell suggested that there are not many with expertise in agencies to conduct risk analysis and that training is needed to fill this gap. Stalker-Lehoux noted that, while the 2019 JASON report recommended conducting risk assessments at the project level, she focuses on proposals in sensitive technology areas. For proposals dealing with sensitive technology, she "tries to make the assessment at the project level."

Audience member **Jim Belanich** (Institute for Defense Analyses) asked whether there are combined quantitative and qualitative metrics that can be used to evaluate research security initiatives. Stalker-Lehoux suggested that DOD may have these types of metrics and that combining qualitative anecdotal and quantitative data could be informative. Dao agreed that there is a need for combined qualitative and quantitative metrics. He said that Rice submitted a proposal to NSF to study sophisticated methods from social science, epidemiology, and economics to test whether anecdotal risks that have already been identified by the U.S. government can inform the development of research security metrics.

Audience member **David Biggs** (U.S. Department of State) asked how to convene all sectors to make decisions about evaluating research security. Dao said that, while the goals of research security are different for professors than they are for administrators or the government, it is important to begin to reach agreement on the goal of research security before developing policies, guidance, and evaluation efforts. Stalker-Lehoux suggested that all parties have the common goal of ensuring that there is no undue foreign interference across the U.S. research ecosystem.

A member of the online audience asked what, if any, assessment of student candidates or new hires is performed to evaluate potential foreign influence risks. Dao suggested that the underpinnings of such assessments come from the 2019 and 2024 JASON reports[9] and DOD and NSF models for risk evaluation. Risk assessment often follows what the agencies are looking for (e.g., entities of concern, contracts with foreign talent programs, denied entity collaboration, overseas patents)—assuming that these are accurate, reliable, and valid factors.

McQuade concluded the session by noting that the national security and economic value of leadership in science and technology has not changed. "We are," he said, "no longer in a landscape where we could afford to be magnanimous because we were ahead of everybody in almost all relevant aspects of science. It is no longer a landscape where we can make simple national security decisions and say, 'We need to protect that at all costs,' because in protecting at all costs, we damage economic security," he said. The fundamental question is "What level of throttle we want to put on the free exchange of information and collaboration, and how do we measure it?"

[9] JASON. 2019, December. Fundamental Research Security. JSR-19-2I. The MITRE Corporation, https://nsf-gov-resources.nsf.gov/files/JSR-19-2IFundamentalResearchSecurity-12062019FINAL.pdf; JASON. 2024, March 21. Safeguarding the Research Enterprise. JSR-23-12. The MITRE Corporation, March 21, 2024, https://nsf-gov-resources.nsf.gov/files/JSR-23-12-Safeguarding-the-Research-Enterprise-Final.pdf.

4

The Impact of Research Security Policies and Requirements on the Research Ecosystem

Workshop planning committee member **Benjamin F. Jones** (Northwestern University) moderated a panel focused on the impact of research security policies and requirements on the research ecosystem, including hidden potential costs as policies are implemented. He acknowledged the seriousness of research security issues and the loss of ideas abroad and asked whether our actions are creating possible other challenges or possibly slowing down our own success.

The United States, Jones said, is in a race where we need to stay ahead in technology. He likened the current situation to a bike race peloton, where others draft behind the frontrunner to their advantage. While the United States has historically been in the lead, other countries "are kind of drafting and taking some advantage from the United States—pushing hard against the wind of discovery. . . . Maybe that's not so great," Jones said, because this is like handing "a free lunch . . . to those chasing us, particularly as they increase their geopolitical competition with the United States." He continued, "On the other hand, if we put in policies that are trying to . . . prevent others from drafting on our leadership, we are also slowing down our own bike." Furthermore, he said, if we put "all sorts of extra equipment on our bike [and make] it heavier and harder to pedal . . . we lose the race because we're focused on the people behind us and forget to train and bike quickly ourselves."

The first session panelist, **Naomi Schrag** (Columbia University) said that her institution has about 30,000 full- and part-time students and 4,800 faculty members. The university has students, faculty, and researchers representing 149 countries.

Schrag said that, over the past 5 years, Columbia has taken multiple actions to develop research security measures. These include:

- building and updating websites,
- writing and revising policies,
- updating and purchasing information technology (IT) systems,
- creating and licensing online trainings,
- establishing cross-disciplinary working groups, and
- hiring and training staff.

Communicating with the research community has been key, Schrag said. Columbia has communicated about research security through targeted or broadcast emails, town hall meetings, webinars, department chair meetings, departmental faculty meetings, and one-on-one consultations.

Schrag said that each piece of research security infrastructure created causes some friction for researchers and suggested that such friction may deter researchers from entering the kinds of international collaborations that are important for advancing innovation. As an example, she noted that collaborations may begin with an act as simple as finishing a manuscript, but that researchers must be attentive to whether, at that stage or some later stage, the collaboration may require disclosure to funding agencies or other steps. The administrative burden associated with such requirements may deter the kinds of collaborations that we need to keep our research ecosystem healthy and vibrant.

The second session panelist, **Bhaven Sampat** (Arizona State University), provided a historical context for the workshop discussions. He said that World War II was the first time the United States invested in academic research other than agricultural research. This was necessitated by the need to confront the existential threat posed by Nazi Germany. In this period, scientific research for military purposes was coordinated by the Office of Scientific Research and Development (OSRD) led by Vannevar Bush. Although Bush and others were supportive of basic research and the free flow of knowledge, they understood the need to balance openness and security. While the free flow of information could speed the development of wartime technologies such as radar more quickly and effectively, access to information would also benefit U.S. adversaries.

To address security concerns, OSRD compartmentalized access to information. Scientists working on one project would not share information with scientists working on other projects. During this time, publication restrictions and patent secrecy orders were put in place.

After the war, President Roosevelt asked Bush to draft a blueprint for a postwar science and technology policy. In that document,[1] Bush noted that even in a national security context, the free flow of knowledge, or open science, offers substantial benefits (e.g., facilitating scientific collaboration and advancing innovation).

Sampat discussed his recent work examining the impact of secrecy orders on innovation during the war. He has found that these orders successfully kept sensitive technologies out of public view for a period of time. However, they led firms to shift their research away from restricted categories. Sampat said that follow-on effects on innovation in certain research areas persisted into the 1960s.

Panelist **Theresa Mayer** (Carnegie Mellon University) said that academic leaders need to do a better job engaging with faculty on research security and related challenges. In such discussions, she said, it is important to step back and recognize that this is a pivotal moment for the United States and the world. On top of the geopolitical competition, as the pace of innovation accelerates (in part because of AI), infrastructure needs are changing.

Mayer said the focus is often on the protection and distribution of sensitive information—but that we also need to consider the implications of restricting research to the point of hindering the efforts of the research community and science. The United States needs to both outpace and out-innovate adversaries.

Fostering an environment that enables and supports the inherent creativity and entrepreneurial nature of U.S. science is critical, Mayer said. Talent, structures, and culture play a significant role in this.

Mayer suggested that DOD has, over the past few decades, become increasingly risk averse in the research it funds. U.S. adversaries, on the other hand, are working quickly, taking risks, and learning from failure.

In considering the interplay between fundamental research, applied research, and controlled research, Mayer said that fundamental research

[1] Bush, V. 1945. *Science, the Endless Frontier: A Report to the President on a Program for Postwar Scientific Research*. U.S. Government Printing Office.

provides the foundation for other types of research and sits at the frontier of learning and discovery. She pointed to the Defense Advanced Research Projects Agency's (DARPA's) research program as an example of a program that funds both controlled and uncontrolled research. Thinking about the coupling of different types of research may require different ways of teaming and different approaches to addressing scientific problems, Mayer said

Mayer said that she has worked with faculty whose proposals to DARPA or the Advanced Research Projects Agency for Health have been flagged for security review. She said, "I think it is really important to say out loud that" security reviews create "extreme anxiety," especially for international researchers. Faculty want to do the right thing, but "they are being flagged for joint publications or joint collaborations and simply do not understand going forward what is acceptable and what is not acceptable."

The session's final panelist, **Susan A. Martinis** (University of Illinois Urbana-Champaign [UIUC]), described her research security work and noted the importance of developing relationships and trust. She said that UIUC is working with faculty to create a culture of disclosure.

Martinis emphasized importance of talent to innovation, national security, and competitiveness. She noted that talent has always been necessary for innovation, but that there is insufficient talent in the U.S. talent pipeline. "We are in a race," she said. "We need a rapid increase in talent to meet that race." Talent must be sophisticated and supported by investment—particularly in areas such as AI and hypersonics—and we must create a welcoming environment.

> "We are in a race. . . . We need a rapid increase in talent to meet that race."
>
> Susan A. Martinis

DISCUSSION

Jones asked panelists to consider the issue of talent and performance measures in the context of national security objectives.

Martinis said that, beginning in the 1980s, students from China who came to the United States to study wanted to remain here: today they want to return home. She suggested that metrics to determine whether the U.S. research environment is welcoming and whether students from other countries wish to remain in the United States could be developed. Mayer said that there are discussions about providing green cards or other methods to support promising talent and provide a pathway to permanent residency in the United States. Martinis was not aware of any quantitative measures to assess talent.

Most international students come to the United States with the intention of staying in industry and academia—and we have been beneficiaries of this talent, Sampat said. He added that, in most fields currently, research is collaborative and conducted with international partners. Almost every study he has seen suggests that interdisciplinary, cross-national collaboration has high impact. Measures to capture this type of collaboration could be useful, Sampat said.

Jones asked whether research security restrictions related to collaboration may dissuade talent from pursuing particular areas of research because they do not want to be subject to the additional scrutiny and whether this negatively impacts the research ecosystem. Schrag said that she has heard anecdotes to this effect, noting that anxiety around collaboration is high.

Martinis noted that NSF has developed algorithms that identify international collaborations. She suggested that collected data be mined to measure whether research collaborations have increased or decreased. Were these data aggregated at the university level, they could shed light on how collaboration has been affected by research security policies.

Sampat said there has been work examining the China Initiative's effects on research and researchers.[2] Philippe Aghion and others have suggested that the initiative negatively affected Chinese researchers with U.S. collaborators.[3] Xie and colleagues have suggested that the China Initiative had a negative impact on U.S. researchers with Chinese collaborators.[4] Scientific progress is cumulative, Sampat said. "If you close off the flow of information," if you "throw too many wrenches in the chain—whether

[2] The China Initiative was a U.S. Department of Justice program launched in November 2018. Its primary goal was to counter national security threats posed by the Chinese government, particularly with regard to economic espionage, trade secret theft, and violations of U.S. export controls and research integrity. The initiative was part of a broader U.S. strategy for addressing concerns about the CCP's efforts to leverage open American institutions for technological and strategic gains.

[3] Aghion, P., Antonin, C., Paluskiewicz, L., Stromberg, D., Wargon, R., Westin, K., and Sun, X. 2023. *Does Chinese Research Hinge on U.S. Co-Authors? Evidence From the China Initiative.* CEP Discussion Papers (CEPDP1936). London School of Economics and Political Science. Centre for Economic Performance.

[4] Xie, Y., Lin, X., Li, J., He, Q., & Huang, J. (2023). Caught in the Crossfire: Fears of Chinese-American Scientists. *Proceedings of the National Academy of Sciences of the United States of America*, *120*(27), e2216248120. https://doi.org/10.1073/pnas.2216248120

through patent or security restrictions—you'll slow down the cumulative process of scientific progress." He noted that effects may be disproportionate on some fields.

Schrag said that Columbia University conducts only fundamental research and its statutes do not allow researchers to enter into contracts that would grant a third party the right to censor or restrict the dissemination of research. A change from a more open to less open system could lead to further contraction of the university's work. It would be a tremendous cultural change to revise university statutes that go back decades, Schrag said.

In response to a prompt about how to encourage researchers to comply with research security policies and procedures, Schrag said that expectations should be made clear. Transparency about what the agency does with disclosed information is incredibly helpful. Further, DOD's risk matrix clearly describes what the agency is looking for in reviewing current and pending support and biographical sketches. Schrag appreciated that the matrix illustrates to faculty when they need to take action to address potential risks and makes clear that they may not receive funding if action isn't taken.

Sampat asked whether there is a way to roll out research security policies gradually in a manner that permits the evaluation of positive and negative effects, noting that doing so would require the objectives of research security efforts to be clear. He suggested that sunset clauses for research security requirements may be appropriate as these would trigger future reconsideration of whether the requirements are still necessary. Restrictions should be as narrow as possible, he said, focusing on specific funding streams or grants, for example. A one-size-fits-all approach to research security will not work for all institutions, Sampat said, given differences in environment, culture, research, and needs.

Mayer suggested that it is unrealistic to expect all faculty and students to remember all the regulatory details of research security policies. Practical examples of research security policies in action are useful and one-on-one engagement on research security topics lowers anxiety. There is value in training videos, but they cannot take the place of one-on-one interactions.

Martinis emphasized that the research ecosystem needs to be dynamic and flexible, moving quickly if needed. We can move fast (as was shown during the pandemic), and there is a race. "We need," she said, "to be able to really row really hard and pivot . . . very quickly" and we need a network to communicate with senior research security officers and faculty.

Humphrey said that other countries link research security and research integrity and that this allows for independent context and framing by discipline and for researchers to think about research security and integrity within the context of their discipline. Martinis said that faculty understand research integrity and much work has been done to develop policies and processes in the area. Schrag sees value in separating research integrity from research security, given research integrity's traditionally narrower focus on potential research misconduct (i.e., falsification, fabrication, and plagiarism) and objectivity of research. She said that there is risk to expanding the definition of research security to include research integrity—as doing so suggests that the same infrastructure that is used, for example, to investigate a research misconduct allegation should be used in a research security scenario.

Mayer said that, conceptually, it could be useful to develop a community of practice for different research areas. Carnegie Mellon's energetics program brought together faculty to discuss research security. The conversation was valuable because faculty were able to discuss feedback on grant proposals received from different parts of DOD.

Caputo asked about talent most at risk of leaving academia for venture capital opportunities. Martinis said that faculty are resilient and adaptable because they must constantly look for and apply for funding, but that graduate students, postdoctoral students, and assistant professors are most vulnerable given that their positions are typically less secure in the university system.

Jones suggested that universities are concerned about the physical sciences. He also suggested that the principal investigator (PI) model presents a challenge, given that a single PI is supported by postdoctoral and Ph.D. students and staff scientists. In such a structure, it is not possible for everyone to become a PI and, as a result, some leave academia.

Mayer said that, as we consider metrics, it may be difficult to identify the effect of research security policies. There may be multiple factors influencing decisions to leave the U.S. academic system. We may be assigning migration of academics to research security policies, when in fact the movement represents a normal ebb and flow of early career researchers. She noted, however, that other countries are making investments in research that make them more attractive for researchers who would have historically come to the United States.

Discussion moved to research security in the context of universities who conduct research for industry. Schrag said that Columbia has a significant amount of industry-funded research. While agreements with industry acknowledge that Columbia is an academic institution with the mission to disseminate the results of research, the university agrees to the sponsor's prepublication review of manuscripts for the sole purpose of enabling the sponsor to protect its own, preexisting IP developed by the sponsor before the collaboration. If any of the sponsor's preexisting IP is mistakenly included in a manuscript, the industry sponsor has the right to strike it. This is analogous to input versus output data in the export control context. In such an instance, the university might receive input data from outside the university that it will protect with a technology control plan. If the output of the research is not subject to export control, it would not be subject to restrictions.

Sampat said that universities recognize that narrow licensing of the results of research is not good for their institutions or the world, but that they have refined their review processes to improve their ability to distinguish between what should be broadly licensed and what should be narrowly licensed.

Murdick asked what DOD should prioritize when considering issues of research security, suggesting that award amount, research characteristics, and technology area might be considered. Schrag said that if a researcher intuitively understands that their research is important to, for example, national security, it is easier to move forward with compliance programming. Sampat said that funders should focus on particular funding streams.

Martinis and Mayer said that DOD's risk matrix could be helpful in defining research security priorities. "The risk matrix has been valuable, bringing clarity and consistency and recognizing that [research security] is an evolving area," Mayer said.

Martinis said that, when it became public that reviewers of National Institutes of Health (NIH) grant proposals were potentially inappropriately sharing proposal information with foreign entities, research security was elevated as an issue. Increased awareness of breaches could help to strengthen research security efforts and lead to the opening of communications channels between researchers and the government.

Mayer said that different offices within DOD have different definitions of research security. She called for consistency, particularly as there are researchers who may have research projects in several DOD program offices. It would be valuable to have DOD contracting officers and program managers available to discuss the scope of a research program and understand what part of the program carries restrictions.

Nichols asked how to assess the impact of research security initiatives and compliance requirements given a lack of metrics and long-term tracking data. Are conversations and convenings the right approach? Sampat said that there is both a need for data and a need to invest in the development of measures of effectiveness. "The funders or society needs to tell us what we mean when we say national security. And then we can think about the right surrogate outcomes for it, the right long-run outcomes for it," he said.

> "The funders or society needs to tell us what we mean when we say national security. And then we can think about the right surrogate outcomes for it, the right long-run outcomes for it."
>
> Bhaven Sampat

Martinis added that pilot programs could be useful to support areas where there is little information about the impact of research security policies and processes. Pilot programs allow for quick reflection and can be redirected if they are not producing the desired result. Mayer said that regular convenings to collect feedback are useful for collecting in-depth information.

Mayer said that questions often come up about foreign influence and international engagement. It is often unclear, she said, who at DOD should address such questions.

Fox recounted that she saw a demonstration of an AI-enabled program by a military command to expedite foreign disclosure information. The tool allowed researchers to identify problematic proposal elements. Fox inquired whether there is a role for technology in flagging risks. Martinis said that technology is a valuable tool: PIs spend about 40 percent of their time on compliance and using technology to reduce that burden would be beneficial.

Jones added that DOD should communicate research security requirements to universities prior to issuing them. "If you end up in a situation where PIs spend 40 percent of their time on regs and compliance, that tells me that we have to work with them and think efficient compliance."

Schrag said that Columbia has established cross-disciplinary research security working groups. The working groups meet regularly to discuss research compliance, technology transfer, sponsored projects, global travel, and international programs.

A member of the online audience asked about open versus closed science. Whether a system is open or closed has numerous implications on how universities evaluate faculty, scholarships, scientific credibility, research validation, research integration, and IP. Jones noted that an open system invites generic peer review and enables skepticism to weed out bad ideas and to challenge them. Schrag said that "the more open we are, the better prospect we have for regaining, promoting, and enhancing the public trust in what we do."

5

Advancing Research Security in the Research Community

Humphrey moderated a panel focused on advancing research security in the research community. She asked the panelists about the infrastructure needed to ensure compliance with research security policies and requirements, including any associated costs for researchers and research institutions.

Panelist **Jeremy Forsberg** (The University of Texas at Arlington [UTA]) said that federal agencies have been inconsistent in the implementation of research security requirements, including having a broad range of disclosure requirements for grant proposals. Given the significant paperwork required to comply with necessary disclosures, the energy and resources spent are high. Inconsistencies create extra burden and waste, but universities must comply with all requirements. Risks to universities for noncompliance are significant, including potential False Claims Act liability.[1]

Humphrey said that, according to NSF Higher Education Research and Development survey data,[2] between 2010 and 2023 federal research funding has dropped by $7 billion. At the same time, institutional investment in R&D has increased by $6.5 billion, in large part to cover the cost of various unfunded mandates. For institutions of higher education, research security is, in essence, an unfunded government mandate, Humphrey said.

[1] The False Claims Act (31 U.S.C. §§ 3729–3733) is a federal law that allows the U.S. government to sue individuals or companies that defraud government programs.

[2] Survey data can be found at https://ncses.nsf.gov/surveys/higher-education-research-development/2023.

This presents particular challenges for smaller institutions, she continued, noting that, at Northeastern University, one- and one-half full-time employees support research security compliance activities.

Forsberg noted that, in fiscal year 2023, the Council on Governmental Relations (COGR)[3] conducted a facilities and administrative cost (F&A) survey. For institutions receiving less than $50 million in federal grants, the actual F&A cost of facilities and administration is 76 percent. The government F&A rate is capped, on average, at 61.5 percent. As the negotiated rate for indirect costs is 53.3 percent, this means that institutions are responsible for an F&A shortfall of around 15 percent—which is untenable. There is, however, an opportunity to leverage other institutional functions to cover research security compliance costs.

Panelist **Geeta Krishna Swamy** (Duke University) said that dedicated staff at universities handling research security compliance must have content expertise and training on research security. She also noted that IT systems associated with compliance and related matters are expensive and represent a hidden cost. Panelist **Lori Ann Schultz** (Colorado University) agreed that there are hidden costs related to research security compliance work. Costs include those associated with research information management systems, the collection of bibliometric data, and the identification of faculty collaborating with external parties.

Humphrey suggested that research security is a whole-of-campus issue, touching everything from lab safety to IT, campus security, and the office of the general counsel. Each has competing priorities but there is a need to convey the importance of research security across an institution and negotiate boundaries around how much effort and funding can be applied to research security efforts. Schultz said that it is important to get buy-in from institutional leadership to advance research security efforts campuswide. Forsberg added that UTA integrates processes across multiple offices. Swamy said that, to achieve buy-in across an institution, it is necessary to develop partnerships that bring people together to create a secure environment.

Panelist **Jonathan Snowden** (University of Missouri, Kansas City [UMKC]) agreed that buy-in from leadership is critical. It is also important to build relationships with federal agencies such as the FBI. Snowden said

[3] COGR was "founded in 1948 to address the need for sensible federal research policy." It "provides a unified voice for U.S. research universities, affiliated medical centers, and independent research institutions" and advocates "for effective and efficient research policies and regulations." See https://www.cogr.edu/cogrs-purpose.

that his previous university has convened a research security integrity working group with representatives from across the university; it created an insider-threat working group to identify and mitigate research security risks.

Humphrey asked what funding would be needed to ensure that an institution's research security measures are effective. Forsberg said that institutions should explore ways to maximize direct charging for certain research security activities while finding efficient ways to implement research security requirements. Schultz suggested that institutional approaches to research security align with institutional culture and size. One of the hard things about research security is that it is difficult to measure its effectiveness, she said; addressing research security requires culture change, and cultural shifts are particularly challenging to measure.

Forsberg said that a recent NIH notice on foreign subawards introduced a new process and requirements.[4] He suggested that the requirements will have unintended consequences and may result in less foreign collaboration. Swamy said that the costs of research security are borne where research is performed and if the cost burden becomes too high, certain institutions will be unable to participate.

Humphrey said that there has been a shift in international collaborations because of research security requirements. In addition, there is data to suggest that foreign students have chosen not to return to the United States due a climate seen as unwelcoming to international scholars and the potential for enhanced vetting processes to meet research security protocols. Universities have become better at identifying risk on the basis of sanctions, export controls, and research security awareness, but continued improvement in these areas is needed.

Humphrey said that it is important to achieve a balance between open and closed research. Forsberg said that the boundary between open and sensitive research is fluid and that, in many instances, universities spend time evaluating risk in areas that are not sensitive scientifically in order to meet administrative requirements.

Humphrey said that it is important to develop research security training that resonates with faculty. This can be achieved by helping faculty understand the risks involved in their area of research. Snowden said that face-to-face interactions with faculty are important in helping faculty understand

[4] The new award structure, which went into effect on May 1, 2025, probits "awards to domestic or foreign entities (new, renewal or non-competing continuation), that include a subaward to a foreign entity." See https://grants.nih.gov/grants/guide/notice-files/NOT-OD-25-104.html.

research security issues. Schultz has found it helpful to frame educational opportunities as "increasing awareness of risk" rather than "training."

Schultz asked about pathways that enable everyone at institutions to learn more about research security. Swamy said that clearer guidelines, understanding, approaches, and harmonized content are needed.

Murdick said that, in light of federal proposals to lower indirect cost recovery, there are assumptions that reimbursable direct costs could become a line-item cost for universities. Direct costing would be time consuming and complicated. He asked panelists to comment on the information that would be needed to develop a direct reimbursable cost plan to cover research security activities. For smaller universities, would it be possible for direct costs to be aligned and provided by an independent clearinghouse or some organization that works on behalf of a collection of smaller institutions?

Swamy offered an example of the institutional review board (IRB) system at Duke University. Duke and other institutions participate in an IRB system run by Harvard University. This allows for the centralization of IRB activities as constituent institutions adopt a similar IRB structure and process. Swamy said that the NSF SECURE Center will be helpful as a centralized repository of informational and educational resources related to research security.

Forsberg said there is a need to collect information via surveys as well and a need to better understand the current costs of research security efforts. Surveys could collect the information needed to understand costs and provide a vehicle to assess models for covering these costs, particularly for smaller institutions. He noted that 34 percent of larger institutions have greater economies of scale on indirect recovery.

Snowden noted that UMKC has been examining opportunities for vendor support of research security–related activities. Over time, vendors have been able to make products that can help make research security activities more affordable for smaller schools. UMKC can use a vendor to help with hiring decisions for research security work, potentially eliminating the need to hire an additional full-time employee to work on research security issues.

Humphrey noted that other countries use different models to address research security issues. For example, in Canada each institution receives, based on the size of their research portfolio, funds that can be used for their research security program.

Fox asked panelists about their experience with Controlled Unclassified Information (CUI) programs. At Fox's institution, the requirements associated with CUI have been confusing to implement and often need to involve the participation of individuals with security clearances. Schultz said that she implemented a CUI program at a previous institution, and it was difficult to get faculty to understand what they need to be doing and why. She found success in treating CUI as a service like high-performance or research computing: "This is the environment, this is how you use it, this is what it costs," to be accessed similarly to other services. This makes more sense for faculty accustomed to working in a central IT environment. CUI was handled outside the university's research office (though the office was involved in defining what CUI looked like) and managed by individuals who understood how to protect data.

Forsberg said that it is expensive to work with CUI and that any expansion of CUI should be met with caution. He said that there is a need for simplification and noted that information has been incorrectly marked as CUI. Snowden said that more education about CUI is needed. Schultz said that safeguarding CUI within universities requires infrastructure that does not exist in most places. For example, providing faculty with a clean laptop is challenging because clean devices do not have in storage the information they need; establishing connections to secure IT systems requires a significant infrastructure and planning.

Snowden and Swamy said that coordinated effort on research security activities is necessary to leverage resources and streamline the work of institutions. Forsberg suggested that it might be helpful to calibrate research security expectations prior to centralizing research security measures within an institution.

Panelists discussed the use of outside expertise to support campus research security efforts. Snowden said that many in government do not understand what goes on in academia. He recounted an experience where a Defense Counterintelligence and Security Agency (DCSA) counterintelligence special agent conducted a role-playing training on research security. As an expert on counterintelligence, the agent knew how academic solicitation works, but by engaging faculty, was able to understand how solicitation is viewed in the academic environment.

Swamy suggested that universities be allowed to provide input as part of the development of a new rule. "Getting input before the rule comes out" is important, she said, because if institutions cannot understand it, they cannot explain it. Forsberg added that one way to gather input is for federal agencies to survey institutions about proposed regulations and ask questions about what will be effective.

Humphrey said that there is the potential to lose out on opportunities to pursue research collaborations if an institution does not have full information on risk because of a lack of understanding about how the government classifies operations or intelligence services. Swamy said that this is a challenge encountered at Duke.

Caputo said researchers know that measurement is really hard. While "we all love metrics and measures of effectiveness," she said, the goal is risk reduction. She asked how to know whether the research community is reducing risks and securing research more effectively. Forsberg said that UTA's first research security endeavor was the result of widespread attention being given to malign foreign-talent recruiting programs. The university conducted a risk assessment of all faculty interactions with China by examining travel records, funding, unfunded agreements, collaborations, and publications and interviewing faculty. Because of the campaign and changes in policies, faculty do not participate in foreign-talent programs anymore. Risks identified through transactional reviews have also led to increased awareness of potential threats and the need to protect information.

Snowden believes that faculty are more educated and aware of research security and potential threats, but to achieve true awareness, one-on-one interactions with faculty are necessary. Swamy has found that when administrative staff directly interacts with faculty, there has been more reporting about research security matters, particularly on issues that would not be considered misconduct. Faculty are also coming forward with questions, which demonstrates not only that they understand the importance of research security but that they know where to ask questions (and why).

Schultz said that one of the challenges of measurement is that universities do not know what they are measuring against. Institutions can track how many people took the training, completed conflict of interest disclosures, and filled out documents correctly. They can also track conversations that they have had with individual faculty at campus events and one-on-one meetings. But unless they know what the risk was to begin with, institutions cannot measure the scope of risk reduction.

Snowden added that DCSA collects data on research security reporting. He suggested that DOD might use collected information to support evaluations of the effectiveness of research security policies.

6

A Path Forward for the U.S. Department of Defense and Other Funding Agencies

Caputo moderated the final workshop panel session. The panel considered data that DOD and other funding agencies may need to collect to measure the effectiveness and performance of research security measures.

Caputo said that relevant data might include data on:

- people flows,
- where people go after their funding ends (e.g., abroad, industry, venture capital, remain in the United States),
- awareness or training,
- understanding of research security,
- understanding of risk reduction,
- understanding of foreign interference, and
- return applications for research funding.

With regard to the effectiveness of research security measures, data could be collected on:

- numbers of researchers asking for help,
- numbers of researchers who complete forms accurately, and
- mitigation success stories.

The session's first panelist, **Gregory F. Strouse** (NIST), discussed the agency's approach to research security and its research security publication

Safeguarding International Science: A Research Security Framework.[1] He said that stakeholders need to work together to create a clear, data-driven vision and strategy for research security. Data on research security are critical for institutional leaders and bench scientists.

Strouse said that NIST conducts a security review of everyone who works at the agency. This includes research associates, members of the research security team, subject matter experts, and agency leadership.

Strouse discussed National Security Decision Directive 189 (NSDD-189), a presidential directive that states, "To the maximum extent possible, the products of fundamental research [shall] remain unrestricted." Furthermore, the directive states, "Where the national security requires control, the mechanism for control of information generated during federally funded fundamental research in science, technology and engineering at colleges, universities and laboratories is classification."[2] Strouse said that both fundamental research and IP are targeted by countries of concern, noting that the U.S. critical emerging technology list[3] includes 18 technologies with 136 subcategories. "If you're doing research in [the emerging technology] space, you're a target," he said.

Strouse referenced a recent Chinese news article about a Chinese citizen (a U.S. professor who went to school in the United States) who was recruited back to China. The professor was quoted as saying: "I'm sending all of my students to the U.S. to collect all the intellectual property and bring it home to the motherland." Strouse asked whether the exchange of fundamental and applied research is as benign as it was when NSDD-189 was published in 1985. Benefits, he said, must outweigh risks. He noted that NIST's chief counsel has said that balkanizing federally funded research conduct and reporting could adversely affect R&D in the United States.

[1] The framework is "designed to enable organizations to implement a mission-focused, integrated, risk-balanced program through the application of research security principles and best practices that fosters the safeguarding of international science while mitigating risks to the integrity of the open collaborative environment" (Strouse, G. F., Saundry, C., Wood, T., Bennett, P., and Bedner, M. 2023. *Safeguarding International Science: Research Security Framework*. NIST Internal Report 8484, https://doi.org/10.6028/NIST.IR.8484nist.gov+2, p. ii).

[2] See White House. 1985, September 21. *National Security Decision Directive 189: National Policy on the Transfer of Scientific, Technical and Engineering Information*, https://irp.fas.org/offdocs/nsdd/nsdd-189.pdf.

[3] National Science and Technology Council. 2024, February. *Critical and Emerging Technologies List Update*. Executive Office of the President, https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/02/Critical-and-Emerging-Technologies-List-2024-Update.pdf.

Strouse sees NSDD-189, NSPM-33, and NIST internal reports 8484[4] and 8481[5] as working together in a positive way to accelerate science to safeguard our ability to have international science.

From a cost perspective, Strouse continued, the research community must never lose sight of the fact that the cost of the highest-end semiconductor is about half a billion dollars. The loss of that recipe before it goes into production is significant. Mitigating risk for researchers includes protecting knowledge prior to publication. Fundamental research, Strouse said, is being used to decide what standards to write. He said that competitor nations review fundamental research conducted in the United States, bet which research will result in commercial applications, and go to standards organizations to create "pre-monopolies in those technologies if they come to fruition." Strouse suggested that such efforts do not cost competitor nations much, but the endgame has a very important commercial benefit.

Strouse said that NIST's culture supports research security. The institute has operationalized the implementation of research security measures across five primary areas: foreign and domestic guest researchers, funding opportunities, collaborations and publications, "things that we sell," and foreign travel. Strouse said that nearly every NIST staffer understands that they are an important part of the research security team as they have learned from the agency about the importance of research security for their work.

Strouse measures the success of research security efforts by the numbers of researchers who come to him with questions or concerns about a potential research security issue. He said the numbers of interactions indicate that those conducting research for NIST are aware of research security issues and comfortable asking questions about them. "We're there to provide solutions." When individuals come to you and can accept that "this is a cultural change, not a compliance-driven change," we have been successful.

Session panelist **Jason Owen-Smith** (University of Michigan) said that to understand and mitigate research security threats it is necessary to start with a laser focus on people. Innovation flows through social networks and moves with researchers who carry know-how and expertise across boundaries.

[4] Strouse, G. F., Saundry, C., Wood, T., Bennett, P., and Bedner, M. 2023. *Safeguarding International Science: Research Security Framework*. NIST Internal Report 8484, https://doi.org/10.6028/NIST.IR.8484nist.gov+2.

[5] LaSalle, C., Howell, G., and Martinez, L. 2023, August 31. *Cybersecurity for Research: Findings and Possible Paths Forward*, NIST Interagency Report 8481, https://doi.org/10.6028/NIST.IR.8481.ipd.

Owen-Smith noted that discussions around research security frequently center around critical and emerging technologies. Such technologies evolve rapidly, and their development is challenging to monitor and track.

Owen-Smith said that it is challenging to identify the data needed to assess the effectiveness of research security measures, as "they're simultaneously everywhere and nowhere." This means that new measurement methods are needed. Furthermore, it is difficult to bound data, as data impact and complement each other: some data are upstream and other data are downstream.

Meaningful data may be collected from analysis of university technology transfer invention disclosures or patent applications filed with companies, government agencies, or universities. Data may also be mined from research citations. Owen-Smith noted, however, that such data are imperfect. He suggested that measurements should focus on people and networks, examining, for instance, stocks and flows of human and social capital. People carry frontier knowledge, he said, and they do it more effectively than documents. Novel findings travel through networks because, at the frontiers of knowledge, much that is important is intangible (e.g., physical skills). Oppenheimer, Owen-Smith recalled, famously said the best way to send knowledge is to wrap it up in a person. Owen-Smith suggested that shifting from talking about tracking ideas to talking about tracking people changes the meaning of privacy, confidentiality, and trust—particularly for academic communities. Risks follow people, he said, but so do opportunities.

Owen-Smith suggested that the research community be engaged in discussions about measurement and approach it as a research problem. Engagement with the research community will "help make sure you get it right. As you do that, you build trust because there is some transparency."

Owen-Smith said there are mechanisms and model infrastructure to support assessment efforts. For example, the Institute for Research on Innovation and Science[6] (IRIS) has gathered restricted transaction-level data from universities around the country on direct cost expenditures of every sponsored project from every funder (i.e., all federal agencies and foreign and domestic foundations and corporations). These data are linked to outcome information and data from usaspending.gov that describes grants

[6] IRIS is "a member consortium of universities anchored by an IRB [Institutional Review Board]-approved data repository hosted at the University of Michigan's Institute for Social Research. . . . IRIS collects record-level administrative data from its members to produce a de-identified dataset for research and reporting that will improve our ability to understand, explain, and improve the public value of research" (https://iris.isr.umich.edu/about).

funded by federal agencies. IRIS also utilizes partnerships with statistical agencies like the U.S. Census Bureau and the National Center for Science and Engineering Statistics and links to resources such as the Survey of Earned Doctorates[7] and the Longitudinal Employer-Household Dynamics Dataset.[8] Owen-Smith suggested that these data could be used to evaluate research security activities at universities. Using such a mechanism, he said, it would be possible to examine risk assessments conducted on past proposals or projects or employees and conduct a retrospective assessment. Such an assessment could help elucidate how various levels of risk played out under different policies in different fields in different conditions. The Federal Statistical Research Data Center system, operated by the U.S. Census Bureau, could support evaluations of the effectiveness of research security measures.

Owen-Smith proposed a framework for evaluation. The first step would be mining bibliometric and proposal text from universities or from agencies. He noted that the CHIPS and Science Act[9] includes a provision that requires all federal science funding agencies to send proposal data to the National Center for Science and Engineering Indicators. Owen-Smith suggested that if that information could be sent with, for instance, risk assessments, the material could be accessed for evaluative purposes.

Owen-Smith suggested that it might be possible to track leakage of IP by, for example, monitoring tacit knowledge flow from a leading group to others. While he acknowledged that there may be instances where discoveries are made simultaneously in different places, "if you can establish a baseline for a field, you can see when you have something like excess simultaneity and you may see more simultaneous discoveries from new places and . . . could validate that retrospectively against known risk risks or investigations in partnerships" with, for example, federal agencies. It may also be possible also to track PI career paths or measure shifts in knowledge from academic to commercial spaces. He also noted that research data could be made available and its use incentivized via partnerships and mechanisms such as the NSF RoRS program.

Panelist **Amanda Ferguson** (Huron Consulting) discussed the work of her consulting firm on research administration, compliance, and research security issues. She observed that effectiveness and success in research security "have different, though not entirely conflicting definitions across

[7] See https://ncses.nsf.gov/surveys/earned-doctorates/2023.

[8] See https://lehd.ces.census.gov.

[9] *CHIPS and Science Act of 2022*, Public Law 117-167.

> "We have at least four perspectives to consider: we have researchers; we have institutions that conduct research; we have federal funding agencies and the U.S. R&D enterprise. Effectiveness and success to me have different though not entirely conflicting definitions across the perspectives."
>
> Amanda Ferguson

the perspectives of federal funders, researchers, academic institutions, and the overall R&D enterprise." She suggested that it is important to consider the perspectives of each when considering how to assess the effectiveness of research security efforts.

Researchers want to do the right thing but do not want to be burdened by compliance requirements, including those that may impact their ability to collaborate with global peers and generate high-impact research. Institutions want to understand where risks are most likely to be present so they can take a risk-based approach to resource allocation and compliance. They also wish to be agile in securing funding for research.

Ferguson said that funding agencies are looking to steward taxpayer dollars, safeguard investments in research, promote U.S. military and economic competitiveness, and promote and protect science and innovation. The U.S. R&D enterprise does not want to be left behind, become isolated, or lose its ability to pursue and attract the brightest global minds. There is, however, a need to balance openness and security. Ferguson said that, while many policies support openness and transparency, other policies have created compliance burdens that do not have the desired protective effect. Some might put a chill on global collaboration to the point where the United States is no longer the premier destination for innovative science.

Ferguson said investment in U.S. R&D has decreased relative to the investments of some foreign nations. For example, according to an April 2025 publication of the American Association for the Advancement of Science, China has outpaced the United States in highly cited publications—a metric that can be used to approximate innovative findings.[10] Slippage is particularly evident in fields considered emerging technologies, such as AI and quantum and semiconductors, which are critical components of maintaining a military and economic advantage. Larger factors at play in the

[10] Zimmermann, A. 2025, April 30. *U.S. R&D and Innovation in a Global Context: The 2025 Data Update*, https://www.aaas.org/sites/default/files/2025-04/AAAS%20Global%20RD%20Update%202025_final.pdf.

U.S. R&D environment will make understanding the impacts of research security requirements difficult.

Ferguson said that funding agencies often look at publications and affiliations as proxies of trustworthiness. Several affiliations and collaborations can be problematic, but the nature of academia is such that publication measures of collaboration (such as co-authorship) do not always reflect the types of collaborations that lead to licit or illicit transfers. Furthermore, analysis of collaborations requires such significant resources for institutions and funding agencies that it can dissuade researchers from principled collaborations and might dampen innovation.

Ferguson said that the 2024 JASON report offers solutions on safeguarding the research enterprise. The report states that "risk mitigation must consider the spectrum of risk and be adaptable to changing trends in research. Resources should be concentrated on areas of maximum risk to ensure that the benefits outweigh the costs."[11] Ferguson suggested that it would be helpful to maintain lists of emerging technologies and have experts within the government who can advise funding agencies on, for example, the importance of those technologies to adversaries. Ferguson suggested that universities could conduct proactive open-source due diligence if they had more detail about what programmatic areas they should focus on, rather than broad categories such as machine learning. This knowledge could also help researchers understand how their collaborations might be perceived by the government and stimulate them to provide information to funding agencies proactively; this would, in turn, facilitate discussions about risk.

Ferguson noted that the 2019 JASON report[12] discussed technology readiness level (TRL) as an indicator by which to assess the necessity of implementing controls to effectuate national security.[13] She suggested that

[11] JASON. 2024, March 21. *Safeguarding the Research Enterprise*. JSR-23-12. The MITRE Corporation, March 21, 2024, https://nsf-gov-resources.nsf.gov/files/JSR-23-12-Safeguarding-the-Research-Enterprise-Final.pdf.

[12] JASON. 2019, December. *Fundamental Research Security*. JSR-19-2I. The MITRE Corporation, https://nsf-gov-resources.nsf.gov/files/JSR-19-2IFundamentalResearchSecurity-12062019FINAL.pdf.

[13] TRLs are a systematic method for assessing the maturity of a technology developed by NASA. TRLs range from 1 to 9, with 1 being the earliest stage of basic principles and 9 representing a fully developed technology. They are used to evaluate the progress of a technology as it moves from basic research to a marketable product. See https://www.nasa.gov/directorates/somd/space-communications-navigation-program/technology-readiness-levels/#:~:text=Catherine%20G.%20Manning,based%20on%20the%20projects%20progress.

TRL could be a useful metric to consider when evaluating success across perspectives. TRL can be assessed when a proposal is considered and regularly reevaluated via a standard progress reporting mechanism.

The session's final panelist, **Kristin West** (COGR), said that metrics on the negative, unintended consequences of research security measures are critical as the United States moves from an open system to a more closed system. She noted, however, that context matters as much as the metrics themselves and that metrics on the success of research security efforts are also important.

West said that the 2024 JASON report emphasized the importance of researcher mobility. She noted that a recent *Economist* article said that the United States is experiencing an academic brain drain. It reported a "32% increase in applications from U.S. researchers to jobs outside the U.S. and a 25% decrease in applications from researchers outside the U.S. for jobs in the U.S."[14] This, West said, is a problem.

West said that it is important to look at areas of science where the United States is not in the lead and "we have to quit looking at the easy metrics like collaborations and co-authorships and who got funding from who as always being surrogate end points or proxies for bad behavior. They're not." They can be proxies for the beneficial transfer of information in the United States. Both metrics and the context of the metrics matter, West said.

West said that the use of "gotcha" metrics can have a chilling effect on research. Avoiding security incidents is a common goal, but incidents happen. It is important to analyze incidents in order to understand "what we did right, what we did wrong, what we should do better," and no one wants to face the unintended consequences of a failure to report incidents. West suggested that it may be advisable to focus on developing a fair and just reporting culture akin to that in medicine where health care professionals feel safe and empowered to report errors, near misses, and hazardous conditions without fear of blame or punishment. That system empowers medical professionals, no matter what their rank, to acknowledge a problem and not face retribution or punishment. West suggested that training on (or awareness of) "near miss" incidents would be useful—as would education on collaboration with researchers in countries of concern.

[14] See *The Economist*. 2025, May 21. "America Is in Danger of Experiencing an Academic Brain Drain." https://www.economist.com/science-and-technology/2025/05/21/america-is-in-danger-of-experiencing-an-academic-brain-drain.

DISCUSSION

McQuade suggested that the development of metrics be approached as a research problem. Owen-Smith said that such an exercise could be designed as an iterative process that encourages engagement and collaboration. The research community could be engaged in validating tools or in bringing expertise into the initiative. Owen-Smith suggested that a tracking system for collecting evaluation data on, for example, people flow would likely need to build on a research base that the community was involved in.

Caputo said that there will be a need to provide tools to the research community to aid in identifying risk and performing due diligence in reviews. Caputo suggested that asking researchers to do due diligence implies that "the goal is to ensure or at least have some confidence that you are being trustworthy, that you deserve that trust and are reciprocating that trust."

Fox noted that many have commented on the need for a rheostat, the use (or inappropriate use) of proxies as flags for concerns that do not often pan out, and the notion that we can use lists of critical technology to help us focus these rheostats and to get away from these proxies. "I don't know," Fox said, "of any list of critical technologies where we're behind that could inform university thinking about where these kinds of collaborations are in the safe zone and where the dial should be set higher." West said that Trusted Research Using Safeguards and Transparency (TRUST) framework[15] will guide this type of work. The framework focuses on novel science and offers a better alternative to reviewing static lists of critical and emerging technologies.

Fox asked how to communicate to universities about research areas where collaboration is encouraged. Strouse said that working one-on-one with researchers and asking key questions can be valuable.

Strouse said that it is important to emphasize that "we're not just protecting national security. We're not just protecting economic security. We're protecting the economic security of the United States. And all those things put together are really critical."

West said that she has been involved in several studies related to compliance with research security measures. One survey estimated that, in the first year, it would cost a mid- to large-sized university an additional $445,000

[15] The TRUST framework was developed to guide NSF in assessing grant proposals for potential national security risks. See https://www.nsf.gov/news/nsf-enhances-research-security-new-trust-proposal.

to comply with the disclosure requirements enumerated in Section 2233 of the FY2021 National Defense Authorization Act and NSPM-33.[16]

Ferguson said that, given the movement toward multidisciplinary and transdisciplinary work, there is a need to raise awareness about research security across the board. She suggested starting with something simple that is faculty facing and doing something once a year in a way that feels more truly educational than just "take the training." And as we "kind of narrow down" into those discipline-specific levels, we can target the most basic administrative level.

Kohler said that the Chinese government produces 5-year plans that discuss critical and emerging technologies; these can inform researchers as they consider research security issues, he suggested. However, he said, most researchers have not read these plans. Strouse added that many resources are available to inform researchers about technologies that may be at higher risk (e.g., the Annual Threat Assessment [ATA] of the Office of the Director of National Intelligence [ODNI]).[17] He said that NIST IR-8484 also publishes a list of research security resources.[18] Biggs said that "we lock our cars in a mall parking lot, not because we expect someone to come break into them, but just in case someone's going to." He suggested that, as the PRC has created an academic system that promotes stealing research and fraudulent research, everyone should have the opportunity—even history professors—to check into the people they are working with to see if they have a history of stealing research. Setting that baseline, he said, makes everyone's lives easier.

[16] The Act outlines the following disclosure requirements: federal research agencies must require as part of any application for R&D award that each covered individual listed on the application disclose the amount, type, and source of all current and pending research support received by or expected to be received by the individual at the time of disclosure. Furthermore, any entity applying for an award must certify that each covered individual who is employed by the entity and listed on the application has been made aware of these requirements (*William M. [Mac] Thornberry National Defense Authorization Act for Fiscal Year 2021*, Public Law 116-283, https://www.congress.gov/bill/116th-congress/senate-bill/4049).

[17] The 2025 ATA is available at https://www.dni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf.

[18] See Strouse, G. F., Saundry, C., Wood, T., Bennett, P., and Bedner, M. 2023. *Safeguarding International Science: Research Security Framework*. NIST Internal Report 8484, https://doi.org/10.6028/NIST.IR.8484nist.gov+2, pp. 57–58.

7

Concluding Thoughts on Metrics and Data for Assessing Research Security Efforts in Higher Education

During the final workshop session, members of the workshop planning committee identified their key takeaways from the 2 days of the workshop. These appear below. Also included in this chapter are suggestions from workshop participants of potential metrics and data that could be used to assess research security efforts.

KEY TAKEAWAYS FROM WORKSHOP PLANNING COMMITTEE MEMBERS

Murdick identified four key takeaways. First, he said, “people are the most important part of anything we’re doing here—they’re the knowledge transfer mechanism.” Second, “we need a balanced set of measures that look for not only the success of any process that was going forward, but also the cost of it.” Third, we “need a robust national security emerging technology analyst capability that really does become a reservoir of knowledge that allows prioritization information” and “core infrastructure for some of the monitoring.” Fourth, it is necessary to adopt a cost sustainable model to pay for research security.

Caputo said the need for active data collection is ongoing. Passive data that measure whether research security initiatives are successful do not exist. Broader data-sharing is needed to facilitate holistic measurement of the effects of research security efforts. NSF has useful data on proposals, but DOD does not have access to that material. DOD has other metrics that can be useful, however.

- Recognize that people are the most critical part of the discussion.
- Create a balanced set of measures that assess both success and cost of research security.
- Develop a robust national security emerging technology capability to support prioritization of issues with core infrastructure for monitoring.
- Adopt a cost sustainable model for research security activities.

Dewey Murdick

The NSF SECURE Center will have data to support evaluation, but decisions will need to be made about data-sharing, Caputo continued. Research security is complicated to measure because it is related to so many other things. "The goal is to measure effectiveness of the programs, the know-how, the training, the awareness, the trust frameworks," she said. Challenges in measuring the effectiveness of research security efforts mirror those we face in improving cybersecurity.

Humphrey said that, in considering what data to collect and what to measure, there is also a need to consider the issue of trust—specifically, how to build trust into these metrics. She suggested that public trust in science is currently at an all-time low and that the public needs to trust the research in order to trust their investment in that research. "In thinking about research security and what we are measuring, we also have to tie it back to how can we also convey to the public that we are taking this issue seriously, that it matters to us, and that the data that we're putting out is quality data." Personal relationships are critical. "When we go out to talk to faculty about research security, we have to make it personal," she said, by, for example, demonstrating how research security is important to their field or discipline.

Jones said, "We're in a race. So, when you're in a race, that is directive to what we should measure." But it is also "a series of races," he said. "We're racing on AI. We're racing on quantum computing. . . . So, the question is, are we ahead of our competitors and how fast are we moving? How fast are we moving and how fast are they moving?"

Jones said measures on the output side (e.g., numbers of papers and patents) are needed. Another measure would relate to technological capability. What, for example, is state of the art for a particular technology? Other areas to consider are emerging critical technology, which could be measured using metrics such as number of patents and papers, as well as technological capability and industrial leadership.

On the input side, Jones suggested measures related to effort, including:

- How many people are working on research?
- How much are we spending on it?
- How fast are we moving?
- How fast are our adversaries moving?
- How much are we drafting or bleeding ideas to competitors?

"People are a key input to going faster in our race, but they're also the place where we have leakage," Jones said. He suggested that measures of people flow offer an opportunity to assess how much talent is being lost.

Jones suggested that "the key thing is to do research security and avoid unintended consequences because remember, the race is going fast. . . . What we're trying to win is the race. How fast are we going?" There is a need for the best talent in the world to come to the United States, and then we need to hold on to them. Any policy that dissuades people from coming to the U.S. is a bad policy unless it has some other strong features."

Regarding compliance efforts, Jones advocated for choosing "what areas we're going to do this on and then really go for openness otherwise." Closed systems "will slow our adversaries, but [also] . . . slow ourselves."

Jones suggested that, as regulators move forward, agencies need to think about design partnerships. Policies need to be implemented in a nimble and cooperative way with an awareness of unintended consequences. "If I look behind in the race, you might see some drafting. I see a lot of potential. We're going to win that race because we pull in the best and the brightest in the world." Greater efficiency is needed "not because we're going to have more savings dollars, . . . not because we have more people," but because the U.S. research community has better people and does it better.

Kohler agreed that people are the most vital component. The research community needs, he said, "to find ways to get the smartest people to come to the United States and stay in the United States and contribute to society, and our innovation here. That's just the bottom line." Universities and the research environment must, however, adapt to the way the world really is today as opposed to where the world was 20 years ago. Policies by China and other countries have created friction and competition with the United States and an unfair playing ground. The U.S. government has reacted to that. Those who are "key to innovation are between a rock and a hard place and they're getting ground up by these two superpowers that can't figure out how to get along and how to make this work."

It is up to us to educate others on how to better manage the situation so that universities remain innovative powerhouses, Kohler said.

McQuade said that the United States ran the world's best foreign talent acquisition program for 75 years. The illicit extraction of technology is a real issue, he said. But the bigger issue is the creation of a talent base in China. Thus, he continued, it should come as no surprise that China is following the U.S. model of trying to get the best people to come and work in China. "We will pay a significant price for no longer being the world's best foreign-talent acquisition program."

McQuade said that, while there is a need for what CUI does, CUI is unregulated and lacking in specifications. As a result, it is ultimately arbitrary and ineffective.

From a measurement point of view, McQuade called for focus on measuring the United States's competitive position in the technologies that matter. Is the United States competitive in the places it needs to be competitive? While the country can also measure people flow, collaborations, near misses and events, "if we do not have an assessment of where we are competitively and have a set of goals to change [our position], none of those other measurements really matter to us."

According to McQuade, the world is "vastly different than 1945. We have a peer competitor. We're not in front of everybody else. . . . We need to start to say where we want to be competitive. We, as a society, will determine how much money we want to spend on research to be competitive."

Fox said that, while effective ways to collaborate need to be developed so that the United States wins the race, we need to understand our current national goal. Do we want to collaborate and allow for good collaboration, or is the goal to start to pull away from collaboration? Measures of effectiveness are difficult to establish, she said, without really understanding that alignment question.

SUGGESTIONS FROM WORKSHOP PARTICIPANTS OF POTENTIAL METRICS AND DATA FOR ASSESSING RESEARCH SECURITY EFFORTS

Throughout the course of the workshop, event participants suggested metrics and data that might be used to assess research security efforts in higher education. Box 7-1 provides a summary of their suggestions of potential metrics and Box 7-2 provides a summary of their suggestions of potential data.

BOX 7-1
Workshop Participant Suggestions on Potential Metrics for Assessing Research Security Efforts in Higher Education

Core Principles for Metrics and Evaluation

- Effective assessment should include both positive outcomes (e.g., reduced risk) and unintended consequences (e.g., talent loss, collaboration decline).
- Metrics should consider protection (e.g., preventing foreign interference) and preservation (e.g., maintaining openness and innovation).
- Metrics should reflect variation by field, institution type, risk profile, and national strategy (e.g., whether to lead collaboratively or decouple strategically).
- Metrics should avoid over-reliance on proxy indicators (e.g., co-authorship, nationality).
- Metrics should be calibrated, meaningful, and minimally distortionary.
- Metrics should be aligned with strategic national goals, such as competitiveness in emerging technologies.

A coherent, effective research security evaluation strategy should:

- Be people-centered, risk-informed, and evidence-based;
- integrate behavioral, operational, and strategic dimensions; and
- promote national competitiveness without stifling the innovation ecosystem.

Categories of Metrics and Indicators

A. People and Talent Flows

- Who enters, stays, or exits U.S. research institutions
- Retention of international postdocs and graduate students
- Shifts in proposal submissions
- Participation in or withdrawal from federal funding

B. Behavioral and Cultural Indicators

- Faculty-initiated disclosures, consultations, or training engagement
- Conference and travel behavior, risk perception, and trust

(continued)

BOX 7-1 Continued

- Uptake of institutional training and follow-up awareness
- Near-miss reporting as evidence of embedded awareness

C. Operational and Institutional Metrics

- Research time spent on compliance
- Costs associated with compliance (e.g., costs associated with research security program staff hires)
- Case tracking, emergency outreach
- Effectiveness of scenario-based planning and vetting tools
- Use of risk matrices, technology readiness levels, or technology transfer safeguards

D. National Security and Innovation Impact

- Adversary access to or replication of U.S. research
- Slowing of innovation, publication rates, or technology transfer
- Changes in collaboration with flagged institutions/entities
- Long-term reduction in verified security breaches

Tools, Frameworks, and Evaluation Approaches

A. Methodological Frameworks

- Probabilistic risk analysis (estimate technology loss, adversary intent, consequences of loss)
- Triage/tiered risk models (by technological readiness level, technology domain, or researcher status)
- Pilot programs (phased rollouts with review checkpoints and sunset clauses)
- Just culture models (focus is on proactive, non-punitive reporting and cultural learning)

B. Technology-Enhanced Tools

- AI-supported proposal screening and decision tools
- Bibliometric and network analysis
- Platforms such as IRIS and NSF SECURE Analytics for federated data-sharing

C. Best Practice Models

- DARPA Security Checklists
- NIST Risk-Balanced Culture Model

BOX 7-1 Continued

Challenges and Gaps

A. Measurement Difficulties

- Theft of fundamental research is often invisible and unquantifiable
- Case counts do not reflect actual risk or prevention success
- Training metrics do not equal awareness or behavior change
- Inconsistent agency guidance and classification systems
- Data collection can drive behavior (e.g., lead to the minimization or maximization of numbers to align with a desired outcome)

B. Systemic and Infrastructure Barriers

- No unified or standardized national evaluation framework
- Lack of tools for scalable institutional risk categorization and monitoring
- Poor visibility into:
  - Compliance cost trade-offs
  - Cultural resistance or disengagement
  - Impact of policy on research productivity

BOX 7-2 Workshop Participant Suggestions on Potential Data for Assessments of Research Security Efforts in Higher Education

People and Talent Flows

Tracking human capital is essential, as people are vectors of both innovation and potential risk.

- Mobility and Retention
  - People flows, including between other countries in high-talent STEM areas
  - Where PIs, postdocs, and graduate students go after federal funding ends

(continued)

BOX 7-2 Continued

  - Numbers of students from other countries seeking to remain in or leave the United States
  - Whether researchers are remaining in the United States, moving abroad or to the private sector and startups
  - Whether researchers are avoiding federal funding due to compliance
- Demographics and Participation
  - Who is applying for funding (nationality, career stage, discipline)
  - Changes in international student and faculty retention rates
  - Participation in and withdrawal from foreign talent programs
- Security Incidents Involving People
  - Disclosures of affiliations or conflicts of interest
  - Investigations, self-reported concerns, or "near misses"
  - Pre- and post-travel briefings and their outcomes

Research Activity and Behavior
Understanding how research behavior shifts under security policy pressure.

- Proposal and Funding Trends
  - Changes in submission rates to federal agencies
  - Shifts in collaboration patterns (international co-authorship, subcontracting)
  - Funding streams
- Collaboration Dynamics
  - Institutional tracking of international engagements, contracts, memorandums of understanding
  - Engagement with entities on proscribed or sensitive lists
- Compliance Indicators
  - Timeliness and accuracy of disclosure forms
  - Number of faculty-initiated consultations or requests for clarification
  - Institutional response rates to new federal security protocols
  - Number of risk mitigation plans required by funding agencies

BOX 7-2 Continued

Institutional Practices and Culture
Evaluating infrastructure, awareness, and adaptability within institutions

- Training and Awareness
  - Completion rates and effectiveness of research security training
  - Number and quality of scenario-based or peer-led educational events
  - Culture assessments (e.g., surveys on trust, awareness, engagement)
  - Faculty understanding of research security, risk reduction, and foreign interference
  - Number of queries about research security issues
- Administrative Capacity
  - Staffing levels in research security offices
  - Rates in which research security staff engage with faculty or the administrators
  - Cross-functional coordination (IT, legal, travel, international offices)
- Policy Integration
  - Implementation of risk-tiered frameworks (e.g., technology readiness level-based controls)
  - Use of tools such as risk matrices, export control flags, and vetting procedures
  - Application of “light touch” vs. restrictive approaches based on project risk

Outcomes and Impact on Innovation
Measuring security effectiveness and unintended consequences.

- Research Outputs and Spillovers
  - Changes in publication rates, citation impacts, and patent filings
  - Delay or redirection of research due to security restrictions
  - Migration of research to private sector or foreign institutions
  - Scientific impacts, international research impact, and impact on disciplines
  - Research areas where the United States is not in the lead

(continued)

BOX 7-2 Continued

    - Number of patents, papers, technology capabilities in emerging technology areas
    - Return applications for funding, including federal funds
    - Award amount, research characteristics, technology area
- Loss Prevention and Detection
    - FBI/DOD/Central Intelligence Agency reports of known leaks, IP theft, or foreign exploitation
    - Faculty reporting suspected knowledge misappropriation
    - Use of bibliometric tools to detect "excess simultaneity" (duplicate discoveries)
    - Rates of drafting or bleeding ideas to competitors
- Innovation Health Indicators
    - Retention of global talent in sensitive fields
    - Comparative metrics versus competitors (e.g., China, European Union)
    - University participation in dual-use and critical technology areas
    - Number of proposals requiring (or not requiring) risk mitigation
    - Number of patents filed by academic institutions
    - Number of patent licenses issued by academic institutions

Strategic Alignment and Policy Evaluation

Assessing policy coherence, effectiveness, and alignment with national goals.

- Policy Consistency
    - Harmonization of guidance across federal agencies
    - Clarity of fundamental versus restricted research boundaries
- Metrics of Effectiveness
    - Reduction in incidents or vulnerabilities
    - Case studies of successful mitigation (qualitative and quantitative)
    - Surveys on perception of policy fairness, fear, and engagement
- Cost-Benefit Analysis
    - Costs associated with implementation of research security initiatives
    - Administrative burden versus security gains
    - Opportunity costs (e.g., lost collaborations, innovation slowdown)
    - Funding overhead adequacy and sustainability

Appendix A

September 2024 Meeting of Experts Agenda

Assessing Research Security Efforts in Higher Education

A Meeting of Experts

National Academy of Sciences Building
Room 125
2101 Constitution Avenue, NW Washington, DC 20418

September 16–17, 2024

AGENDA

Monday, September 16, 2024

8:30 am*	**Breakfast Available**
9:00 am	**Welcome, Introductions, Purpose of Meeting**
	Steven Kendall, Project Director and Senior Program Officer, Policy and Global Affairs, National Academies of Sciences, Engineering, and Medicine

*All times U.S. Eastern

Tom Wang, Senior Director, U.S. Science and Innovation Policy, Policy and Global Affairs, National Academies of Sciences, Engineering, and Medicine

Kristopher E. Gardner, Director for Science and Technology Protection, Office of Science and Technology Program Protection (S&TPP), Office of the Under Secretary of Defense for Research and Engineering, U.S. Department of Defense

9:15 am **Research Security Defined**

Framing and Questions:

The NSPM-33 implementation guidance[1] defines research security as "safeguarding the research enterprise against the misappropriation of research and development to the detriment of national or economic security, related violations of research integrity, and foreign government interference."

Given this definition (and considering the types of research security policies and requirements currently in place), when thinking about achieving research security goals:

- How should we think about effectiveness?
- How should we think about the impacts of research security policies and requirements on the U.S. research and innovation ecosystem?
- What *is not* being considered when we think about research security (where are the holes)?

Speaker:

Kelvin K. Droegemeier, Professor of Atmospheric Science and Special Advisor to the Chancellor for Science and Policy, University of Illinois at Urbana-Champaign (*virtual*)

[1] Joint Committee on the Research Environment Subcommittee on Research Security, *Guidance for Implementing National Security Presidential Memorandum 33 (NSPM-33) on National Security Strategy for United States Government-Supported Research and Development*, January 2022, p. 24.

9:45 am **Break**

10:00 am **Ensuring Research Security While Advancing the Progress of Science, Engineering, and Medicine – Perspectives from Federal Funding Agencies**

Scope:

Taking the NSPM-33 implementation guidance definition of research security as our default, *consider what successful research security looks like* (bearing in mind that the *impact* of research security policies and requirements is different than the *effectiveness* of research security policies and requirements).

Questions:

- What can we do/should we be doing to achieve the goals of research security policies and requirements?
- What is your current thinking regarding measurements of the success (or effectiveness) of our research security efforts?
- Beyond policies and requirements, are other mechanisms needed to reach research security goals?
- Are there systemic or unintentional impacts of research security policies that affect the research and innovation ecosystem (e.g., creative ideas that are not being developed)?
- Are we able to distinguish between the *impacts* of research security policies and requirements and the *effectiveness* of research security policies and requirements?
- When making decisions about which research to fund, how does your agency look at risk?
- How does your agency use information collected on research security efforts?
- How are research security policies and requirements affecting the type of research proposals being put forward to your agency?
- What are your expectations regarding the establishment and operation of research security programs outlined in the OSTP *Guidelines for Research Security Programs at Covered Institutions?*[2]

[2] White House Office of Science and Technology Policy, *Guidelines for Research Security Programs at Covered Institutions*, July 9, 2024.

Facilitator:

Steven Kendall, National Academies of Sciences, Engineering, and Medicine

Discussants:

Sara Barber, Science Policy Advisor, Office of the Chief of Research Security Strategy and Policy, National Science Foundation
Jeremy Ison, Senior Advisor for Research Security, Office of Science, U.S. Department of Energy
Michael Lauer, Deputy Director for Extramural Research, National Institutes of Health
Bindu Nair, Director of Basic Research, U.S. Department of Defense

12:00 pm **Lunch**

1:00 pm **Institutions of Higher Education: Impacts of Research Security Policies and Requirements on the U.S. Open Research Ecosystem**

Scope:

Consider:

1. the impacts if we *do not* address research security; and
2. the overall impact of research security policies and requirements on an open research ecosystem.

Questions:

- What performance indicators should we pay attention to when measuring the health of the (open) research ecosystem? (These might include entrance rates, startups, patents, publications, impacts on university operations [e.g., a "chilling effect" on research], effect of agency denial of a research grant, etc.)
- What are the indicators that the (open) research ecosystem is out of balance?
- How is the research security "overlay" affecting the health of the (open) research ecosystem?

- What are the current (and expected) types of impacts of research security policies and requirements on research and education in higher education institutions?
- How does the impact of research security policies and requirements vary across fields/types of research?

Facilitator:

Tom Wang, National Academies of Sciences, Engineering, and Medicine

Discussants:

Deborah Altenburg, Vice President for Research Policy and Advocacy, Association of Public and Land Grant Universities (APLU)
Toby Smith, Vice President for Policy, Association of American Universities (AAU)
Sarah Spreitzer, Vice President and Chief of Staff, Government Relations, American Council on Education (ACE)
Kevin Wozniak, Director of Research Security and Intellectual Property, Council on Governmental Relations (COGR)

3:00 pm **Break**

3:15 pm **The Impacts of Implementing Research Security Policies in Academia**

Scope:

Consider:

1. the challenges of complying with research security policies; and
2. requirements and the capacity of research institutions to comply.

Questions:

- How are academic institutions "doing research security"?
- How are institutions handling the process requirements of research security policies?

- What is being lost when research security policies and requirements are implemented?
- How are research security policies and requirements affecting the type of research proposals being put forward to funding agencies (e.g., numbers of proposals, types of collaboration, choices of co-PIs, etc.)?
- How innovative is the research coming out of academia? How much is fundamental research and how much is "follow-on" science? What creative ideas are not being developed?

Facilitator:

Steven Kendall, National Academies of Sciences, Engineering, and Medicine

Discussants:

Chaouki Abdallah, Professor of Electrical and Computer Engineering, Georgia Institute of Technology
Holly Bante, Associate Vice President, Research Security and Ethics, University of Cincinnati
Dan Engebretson, Vice President for Research and Sponsored Programs, University of South Dakota
Kevin Gamache, Chief Research Security Officer, Texas A&M University System/Academic Security and Counter-Exploitation Program (ASCE)
Mark Haselkorn, Professor of Human Centered Design & Engineering, University of Washington *(virtual)*
Michele Masucci, Vice Chancellor for Research and Economic Development, University System of Maryland
Sonya T. Smith, Executive Director, Research Institute for Tactical Autonomy (RITA), Howard University

5:15 pm **Adjourn**

Appendix B

Workshop Planning Committee Biographies

The Honorable **Christine Fox** is a senior fellow at the Johns Hopkins University Applied Physics Laboratory (JHU/APL). She also serves on many governance and advisory boards for both government and private industry including the National Infrastructure Advisory Board, the Strategic Competitive Studies Project, the Atlantic Council, and Palantir Technologies. Previously, Fox was the assistant director for policy and analysis at JHU/APL, a position she held from 2014 to early 2022. Before joining APL, she served as Acting Deputy Secretary of Defense from 2013 to 2014 and as director of Cost Assessment and Program Evaluation (CAPE) from 2009 to 2013. As director of CAPE, Fox served as chief analyst to the Secretary of Defense. Prior to her Department of Defense positions, she served as president of the Center for Naval Analyses from 2005 to 2009, after working there as a research analyst and manager since 1981. Fox holds a bachelor's degree and Master of Science degree from George Mason University.

Deanna D. Caputo is chief scientist for insider threat capabilities and senior principal behavioral psychologist at the MITRE Corporation, applying deep expertise in the behavioral sciences to insider risk and threat efforts in government and critical infrastructure industries, including higher education. Caputo is an internationally recognized expert in insider threats, and the intersection of cybersecurity and behavioral science. She has 30 years of experience designing, conducting, and analyzing research with human participants using experimental, quantitative, and qualitative analyses.

In 2008 she built and led MITRE's human behavior and cybersecurity capability and team focused on insider risk, usable security/technology adoption, cyber risk perceptions/awareness, and cybersecurity exercise assessment. Caputo built and now leads MITRE's insider threat research and solutions capability and multi-disciplinary team. She created and pioneered development of insider threat applied research with 20 IP disclosures, and an air-gapped, secure MITRE Insider Threat Lab. She uses behavioral methodologies and analytics to reduce insider threats by analyzing how human behavior manifests in human, organizational, and cyber sensors, and developing solutions to identify and change employee attitudes, intentions, and/or behaviors. Caputo holds a bachelor's in psychology from Santa Clara University and doctorate in social and personality psychology from Cornell University.

Amanda Humphrey is codirector of Safeguarding the Entire Community of the U.S. Research Ecosystem and chief research operations officer for Northeastern University. Humphrey oversees the research security, export compliance, and training programs, as well as contributing to compliance and operational objectives for the university. She is an active member of the Federal Demonstration Partnership, National Council of University Research Administrators (NCURA), and the Council of Governmental Relations. Humphrey received an NCURA Global Fellowship in 2019 and visited Aalto University in Finland. She holds the designation of Certified Research Administrator and has degrees from Smith College, University College London, and Northeastern University, where she worked full-time while completing her Master of Business Administration.

Benjamin F. Jones, Ph.D., M.Phil., is the Gordon and Llura Gund Family Professor of Entrepreneurship and a professor of strategy at Northwestern Kellogg School of Management. An economist by training, Jones studies the sources of economic growth in advanced economies with an emphasis on innovation, entrepreneurship, and scientific progress. He also studies global economic development, including the roles of education, climate, and national leadership in explaining the wealth and poverty of nations. His research has appeared in journals such as *Science*, *The Quarterly Journal of Economics,* and *The American Economic Review* and has been profiled in media outlets such as *The Wall Street Journal*, *The Economist*, and *The New Yorker*. A former Rhodes Scholar, Dr. Jones served in 2010–2011 as the senior economist for macroeconomics for the White House Council of Economic Advisers and earlier served in the U.S. Department of the Treasury. He is a non-resident senior fellow of the Brookings Institution, a research associate of the National Bureau of Economic Research, where he codirects the Innovation Policy Working Group, a senior fellow of the Institute for Progress, and a member of the Council on Foreign Relations.

Bruce A. Jones is the senior vice president for research at Howard University. Jones holds more than 30 years of academic and administrative experience in higher education and the nonprofit sector. Over the course of his career, he has held two endowed chair professorships. As the Ewing Marion Kauffman Endowed Chair for Teaching and Leadership at the University of Missouri, he engaged in statewide research on best leadership practices in education reform in partnership with the Missouri State Department of Education, Ewing Marion Kauffman Foundation, and the Danforth Foundation. At the University of Missouri system level, Jones founded and led the Consortium for Educational Policy Analysis (CEPA), which was housed on three campuses of the University of Missouri System. Through his research at CEPA and with the support of the Peter Herschend Foundation, Ewing Marion Kauffman Foundation, the Hall Family Foundation, and the Danforth Foundation, he launched Missouri's first statewide comprehensive assessment of student achievement. At the University of South Florida (USF), Jones served as the David C. Anchin Endowed Professor of Education and director of the David C. Anchin Center. Under his leadership, the external grant portfolio of the David C. Anchin Center grew from an estimated $625,000 when he arrived at USF to a record high of more than $30 million. Jones also served as the Associate Dean for Research in the College of Education. At the University of Houston, he served as professor, vice provost for academic programs, and dean of the Graduate School. Prior to joining the academy, Jones worked extensively with philanthropic institutions on program funding strategies, strategic planning, evaluation, and executive/board decision-making. He currently serves on the board of the Northern Israel Center for the Arts and Technology and has served on the boards of Family Services America; the Alliance for Children and Families; the National Association of Partners in Education; and the National Policy Board in Educational Administration. Jones holds a Ph.D. in political science from Columbia University in New York City.

Alan E. Kohler, Jr. is the president of Pamir Consulting. He retired from the Federal Bureau of Investigation (FBI) in 2023 after 27 years dedicated to counterintelligence and national security matters. His career included every role a special agent can have within the Counterintelligence Program of the FBI, starting as a street agent in Washington, D.C. and finishing in executive roles including Assistant Director of the Counterintelligence Division and Acting Executive Assistant Director for the National Security Branch. As an executive, Kohler led the FBI's effort to protect critical research and engaged extensively with universities and associations across the country. He is a recipient of the Attorney General's Award for Exceptional Service, the FBI Director's Award for Outstanding Counterintelligence Investigation, and the Office of the Director of National Intelligence's George Washington Spymaster Award for lifetime achievement. Kohler serves on the advisory board of the International Spy Museum and is an adjunct professor for the Johns Hopkins School of Advanced International Studies. He holds M.S. and B.S. degrees in ceramic engineering from Rutgers University.

J. Michael McQuade is the inaugural director of the Program on Emerging Technology, Scientific Advancement, and Global Policy at the Harvard Kennedy School's Belfer Center for Science and International Affairs. The program tackles policy challenges that arise at the intersection of technology and geopolitics and trains the next generation of leaders to be fluent in both technology and policy domains. He previously served as special advisor to the President of Carnegie Mellon University (CMU), where he provided strategic counsel on the university's research endeavors and advocated for the importance of science, technology, and innovation on both national and global scales. From 2019 to 2021, McQuade held the role of Vice President for Research at CMU, collaborating closely with academic leaders and faculty to propel forward innovative research initiatives across the institution. Before his tenure at CMU, he spent over a decade at United Technologies Corporation (UTC), serving as Senior Vice President for Science & Technology. In this capacity, McQuade provided strategic oversight for research, engineering, and development endeavors across various business units, focusing on innovative solutions for the global aerospace and building systems industries. Prior to UTC, he held senior research and general management roles at 3M, Imation, and Eastman Kodak. McQuade has contributed his expertise serving government advisory boards, including the President's Council of Advisors on Science and Technology, the Secretary of Energy Advisory Board, and the Defense Innovation Board. His academic background includes a Ph.D., M.S., and B.S. in physics from Carnegie Mellon University, with his doctoral research conducted at the

Fermi National Accelerator Laboratory focusing on charm quark production in experimental high-energy physics.

Dewey Murdick is the executive director at Georgetown University's Center for Security and Emerging Technology, where he oversees daily operations and strategic initiatives. Previously, he served as director of science analytics at the Chan Zuckerberg Initiative, deputy chief scientist at the Department of Homeland Security (DHS), and co-director of the Anticipating Surprise Office/Program Manager at the Intelligence Advanced Research Projects Activity. Murdick's experience in the public, private, and academic sectors spans artificial intelligence policy, emerging technology analysis, data science, machine learning application development, technology foresight, and research and development portfolio oversight. He pioneered work in anticipatory intelligence via high-risk, high-payoff research programs supporting national security missions. Murdick's work has directly informed U.S. and international policymakers on critical technology issues. His contributions have been recognized with multiple honors, including the DHS Under Secretary's Award for Outstanding Collaboration, the Office of the Director of National Intelligence's Exceptional Achievement Award, and the Distinguished Analysis Award for Excellence in Intelligence Community Collaboration. Murdick holds a Ph.D. in engineering physics from the University of Virginia and a B.S. in physics from Andrews University.

Lisa Nichols is executive director of research security at the University of Notre Dame where she has oversight for research and information security, export controls, and conflict of interest. She previously held roles at the University of Michigan, National Institutes of Health, National Science Foundation (NSF), the White House Office of Science and Technology Policy (OSTP), and the Council on Governmental Relations (COGR). At COGR, Nichols engaged with federal agencies on research security concerns on behalf of institutions of higher education and at OSTP in the development of National Security Presidential Memorandum-33. She served as principal investigator on an NSF cooperative agreement to develop research security training for the U.S. research community and currently serves as principal investigator on a Safeguarding the Entire Community in the U.S. Research Environment Center subaward to develop research security resources using a community-centered approach. Nichols holds a Ph.D. in neuroscience from Purdue University and is a former American Association for the Advancement of Science Science and Technology Policy Fellow.

Appendix C

Workshop Agenda

Assessing Research Security Efforts in Higher Education

A Workshop

National Academy of Sciences Building
Room 125
2101 Constitution Avenue, NW
Washington, DC 20418

May 22–23, 2025

AGENDA

Thursday, May 22, 2025

8:30 am* **Breakfast Available**

9:00 am **Welcome, Introductions, Purpose of Meeting**

Workshop Planning Committee Chair:
Christine H. Fox, Johns Hopkins University Applied Physics Laboratory

***All times U.S. Eastern**

9:15 am **Session 1: The U.S. Department of Defense, Research, and the Research Security Environment**

Moderator:
Alan E. Kohler, Jr.,** Pamir Consulting

Speakers:
Jason Day, U.S. Department of Defense
Alexander Angert, Federal Bureau of Investigation
Rebecca Spyke Keiser, National Science Foundation (*virtual*)
Stephen Welby, Georgia Tech Research Institute
Michael Witherell, Lawrence Berkeley National Laboratory and University of California, Berkeley

10:00 am **Discussion with Committee**

10:45 am **Q&A with Audience**

11:00 am **Break**

11:15 am **Session 2: Research Security Policies and Requirements - Scope and Measures of Effectiveness**

Moderator:
J. Michael McQuade,** The Belfer Center, Harvard University Kennedy School of Government

Speakers:
Tam Dao, Rice University
Elisabeth Paté-Cornell, Stanford University
Sarah Stalker-Lehoux, National Science Foundation
Steven H. Walker, Lockheed Martin (retired)

12:00 pm **Discussion with Committee**

12:45 pm **Q&A with Audience**

1:00 pm **Lunch**

****Member of the workshop planning committee**

2:00 pm **Session 3: The Impact of Research Security Policies and Requirements on the Research Ecosystem**

Moderator:
Benjamin F. Jones,** Northwestern University

Speakers:
Susan A. Martinis, University of Illinois Urbana-Champaign
Theresa Mayer, Carnegie Mellon University
Bhaven Sampat, Johns Hopkins University
Naomi Schrag, Columbia University

2:45 pm **Discussion with Committee**

3:30 pm **Q&A with Audience**

3:45 pm **Adjourn**

Friday, May 23, 2025

8:30 am **Breakfast Available**

9:00 am **Welcome and Summary of Day 1**

Workshop Planning Committee Chair:
Christine H. Fox, Johns Hopkins University Applied Physics Laboratory

9:15 am **Session 4: Advancing Research Security in the Research Community**

Moderator:
Amanda Humphrey,** Northeastern University and Northeast Regional SECURE Center

Speakers:
Jeremy Forsberg, University of Texas at Arlington
Lori Ann Schultz, Colorado State University
Jonathan Snowden, University of Missouri, Kansas City
Geeta Krishna Swamy, Duke University

****Member of the workshop planning committee**

10:00 am **Discussion with Committee**

10:45 am **Q&A with Audience**

11:00 am **Break**

11:15 am **Session 5: The Path Forward for the U.S. Department of Defense and Other Funding Agencies**

Moderator:
Deanna D. Caputo,** MITRE

Speakers:
Gregory F. Strouse, National Institute of Standards and Technology
Jason Owen-Smith, University of Michigan
Amanda Ferguson, Huron Consulting
Kristin West, COGR

12:00 pm **Discussion with Committee**

12:45 pm **Q&A with Audience**

1:00 pm **Concluding Thoughts from Workshop Planning Committee**

Speakers:
Christine H. Fox, Johns Hopkins University Applied Physics Laboratory
Deanna D. Caputo, MITRE
Amanda Humphrey, Northeastern University and Northeast Regional SECURE Center
Benjamin F. Jones, Northwestern University
Alan E. Kohler, Jr., Pamir Consulting
J. Michael McQuade, The Belfer Center, Harvard University Kennedy School of Government
Dewey Murdick, Georgetown University

1:30 pm **Adjourn (Lunch Available)**

****Member of the workshop planning committee**

Appendix D

Workshop Speaker Biographies

Alexander Angert has served as the Federal Bureau of Investigation (FBI) Senior National Intelligence Officer for Counterintelligence since 2020. He has spent almost 20 years working on national security matters for the FBI, including in the Counterintelligence Division and the New York field office. In his current role, Angert collaborates extensively with the Office of the Director of National Intelligence and the rest of the U.S. intelligence community on combating intelligence threats to the United States. Prior to joining the FBI as a Presidential Management Fellow, he worked in think tanks in New York and Washington, DC. He earned a B.A. in political science from Columbia University and an M.Sc. in international relations from the London School of Economics.

Tam Dao serves as the assistant vice president for research security at Rice University, where he is responsible for formulating and executing the institution's strategy for research security. His role involves collaborating with faculty, staff, and students across the university to protect the intellectual property, knowledge, and outcomes originating from Rice University's research endeavors against both foreign and domestic threats. Before joining Rice University, Dao held various positions at the Federal Bureau of Investigation (FBI). In 2020, he was promoted to oversee the FBI's Counterintelligence Task Force, leading initiatives to expose, prevent, and investigate economic espionage. Dao has conducted over 300 classified briefings for senior White House staff, members of Congress, heads of

U.S. federal funding agencies, and university administrators. His 2014 investigation into malign foreign talent programs resulted in the identification of over 400 instances of foreign influence on extramural research and the recognition of more than 200 scientists at more than 65 academic institutions with foreign influence concerns. Dao is a subject matter expert on research security, economic espionage, and foreign influence on federally funded research. He is also a certified FBI Hostage Negotiator and regularly instructs at the FBI's Crisis Negotiation Unit and the FBI's Counterintelligence Training Center. In 2021, he was honored with the FBI's Medal of Excellence for his contributions to counterintelligence. Prior to his tenure at the FBI, Dao held a tenure-track professorship at the University of Houston. He has authored over 50 scientific articles and book chapters on personality assessment. He holds a bachelor's degree in psychology from the University of Texas at Austin, a master's from the University of Pennsylvania, and a doctorate from Florida State University. He also completed a postdoctoral fellowship in advanced psychology and psychiatry at the Michael E. DeBakey Veterans Affairs Medical Center in Houston.

Jason Day is the research policy director in the Basic Research Office within the Office of the Under Secretary of Defense for Research and Engineering of the U.S. Department of Defense (DOD). In this role, Day manages research security policy for fundamental research, policy for assistance awards, open access policy, technology transfer, scientific integrity, and other related issues. He also manages several programs for DOD including the Global Competitive Analysis Team program, and he has oversight responsibilities for the Multidisciplinary University Research Initiatives program. Prior to his role with DOD, Day served as the Legislative Director in the Office of Congressman Daniel Lipinski, where he supported the Congressman's role on the House Committee on Science, Space, and Technology. Day holds a Ph.D. in atomic, molecular, and optical physics from the University of Wisconsin–Madison.

Amanda Ferguson is a senior director on Huron's Research Compliance team and leads its research security team. Through this work, Ferguson works with universities and academic medical centers to evaluate, establish, and strengthen research security programs. She frequently supports institutions with developing and implementing policies and procedures, delivering training, and deploying best-in-class technology solutions in order to establish holistic control environments that are responsive to both research security regulations and threat environment. Her team also frequently manages research security operations on behalf of major R1 universities, some of which are large defense contractors and operate highly specialized and sensitive facilities, such as one of two quantum computers on American university campuses. In 2024, Ferguson supported the U.S. Department of State's Cooperative Threat Reduction office as an implementer on a project to build capacity related to research security in Sub-Saharan Africa. Huron developed and delivered a workshop on protecting sensitive and dual-use technology, which was attended by academic and government leaders from Kenya and Nigeria. Ferguson has led international trainings on conflicts of interest and commitment disclosures for several global campuses and is a frequent speaker on research security topics.

Jeremy Forsberg is the associate vice president for research at the University of Texas at Arlington, where he oversees research administration. He has more than 30 years of experience in managing sponsored projects, audits and investigations, research compliance, research integrity and conflicts of interest, and research security. Forsberg serves as the export control officer and research integrity officer for the university. In January of 2025, he was appointed chair of the Council on Government Relations' Costing & Financial Compliance Committee. Forsberg has directed multiple research projects to create efficient policy framework models for various regulatory requirements.

Rebecca Spyke Keiser is the chief of research security strategy and policy (CRSSP) at the National Science Foundation (NSF). Keiser is the first CRSSP, a position established in March 2020 to ensure the security of federally funded research while maintaining open international collaboration. In this role, Keiser provides the NSF director with policy advice on all aspects of research security strategy. She also leads NSF's efforts to develop and implement efforts to improve research security and the agency's coordination with other federal agencies and the White House. Until March 2020, Keiser was the head of the Office of International Science & Engineering at NSF, a position she held since coming to NSF in 2015.

Susan A. Martinis is vice chancellor for research and innovation at the University of Illinois at Urbana–Champaign, where she provides leadership for the campus-wide interdisciplinary research institutes, promotes new research initiatives, and oversees the administrative and business processes that ensure the safe, ethical, and productive conduct of research at Illinois. Martinis, the Stephen G. Sligar Professor of Molecular and Cellular Biology and professor of biochemistry, studies the mechanisms, evolution, and biomedical applications of protein synthesis and RNA-protein interactions. She is a successful researcher, engaged in entrepreneurial activities and corporate partnerships; a committed educator; and an experienced administrator.

Theresa Mayer is the vice president for research at Carnegie Mellon University, supporting the research, creativity, and entrepreneurship that drives its mission and working with partners across the public and private sectors to bring the benefits of this work to all of society. Mayer has been an active advocate for the critical role that science, technology, and innovation play in driving economic prosperity and security both nationally and globally through her testimonies before the U.S. House of Representatives' Science, Space, and Technology Committee and the House Armed Services Committee and her service on boards such as the Engineering Research Visioning Alliance and National Defense Industry Association. She earned her B.S. in electrical engineering from Virginia Tech, and her M.S. and Ph.D. in electrical engineering from Purdue University.

Elisabeth Paté-Cornell is the Burt and Deedee McMurtry Professor in the School of Engineering, and a professor and founding chair of the Department of Management Science and Engineering at Stanford University (2000–2011). Previously, she was the professor and chair of the Stanford Department of Industrial Engineering and Engineering Management and an assistant professor of civil engineering at the Massachusetts Institute of Technology (MIT). Her specialty is engineering risk analysis with application to complex systems (seismic risk, space systems, medical procedures and devices, offshore oil platforms, cyber security, etc.). Paté-Cornell's earlier research focused on the optimization of warning systems and the explicit inclusion of human and organizational factors in the analysis of systems' failure risks. Her more recent work is on the use of game theory in risk analysis with applications that have included counterterrorism and cyber security. She is a member of the National Academy of Engineering where she chairs the section of Interdisciplinary Engineering and Special Fields of the French Académie des Technologies and of the NASA Advisory Council. Paté-Cornell is co-chair of the National Academies' committee on risk analysis methods for nuclear war and nuclear terrorism. She is the author of more than 100 publications, with several best paper awards, and the co-editor of *Perspectives on Complex Global Problems* (2016). Paté-Cornell was a member of the Board of Advisors of the Naval Postgraduate School, which she chaired from 2004 to 2006, and of the Navy War College. She was also a member of the President's (Foreign) Intelligence Advisory Board (2001–2008), of the board of the Aerospace Corporation (2004–2013) of Draper Laboratory (2009–2016), and of InQtel (2006–2017). She holds a B.S. in mathematics and physics from Marseille (France), an engineering degree (applied math/cs) from the Institut Polytechnique de Grenoble (France), an M.S. in operations research and a Ph.D. in engineering-economic systems, both from Stanford University.

Bhaven Sampat is a professor in Arizona State University's (ASU's) School for the Future of Innovation in Society and School of Public Affairs, and Research Associate at the National Bureau of Economic Research (NBER). He is based at ASU's Consortium for Science, Policy, and Outcomes in Washington, DC. An economist by training, his research focuses on the economics and political economy of innovation and innovation policy. Among other topics, Sampat has studied U.S. and global life science patent policy, the politics and economics of publicly funded science, the roles of the government in pharmaceutical innovation, and the economic history of the U.S. biomedical research enterprise. An overarching theme in his research is how science and technology policies can best be designed to contribute improvements in health and other socio-economic outcomes. Before joining ASU in 2023, he was assistant, associate, and full professor at the Department of Health Policy and Management at Columbia University's Mailman School of Public Health. Sampat held visiting positions at New York University (NYU) Law School and NYU's Wagner School of Public Service, among other institutions. He is a founding member of NBER's Innovation Information Initiative (I3), a data collaborative for open innovation data and related analytics, tools, and metrics, a member of the editorial advisory board of the *Milbank Quarterly*, a leading health policy journal, and an affiliated professor in the Abdul Latif Jameel Poverty Action Lab Science for Progress Initiative. Sampat received his B.A., M.A., M.Phil., and Ph.D. (all in economics) from Columbia and did a postdoctoral fellowship through the Robert Wood Johnson Foundation's Scholars in Health Policy Research program at the University of Michigan.

Naomi Schrag is the vice president for research compliance, training, and policy in the Office of the Executive Vice President for Research at Columbia University. She is also the university's research integrity officer, overseeing work on issues such as research security, data management, export controls, research misconduct, and conflict of interest and commitment. Schrag collaborates closely with offices across the university to develop integrated approaches to compliance and training. Before joining Columbia in January 2006, she practiced law for nine years, focusing on regulatory compliance and litigation involving biomedical research with clients including pharmaceutical companies and not-for-profit organizations. Schrag also clerked in the Court of Appeals for the Second Circuit. Before entering law school, she worked on an oral history of the Holocaust for the Museum of Jewish Heritage. She graduated from New York University School of Law in 1995.

Lori Ann Schultz is the assistant vice president for research administration at Colorado State University and Co-director of the National Science Foundation Safeguarding the Entire Community of the U.S. Research Ecosystem Center Southwest Region. She has worked in research administration for more than 30 years and supports faculty researchers through policy, process, research security, and a host of topics related to external funding. Schultz works on evidence-based policies, marshaling research data in the service of the institution and the faculty who do research, and using data to forecast and plan strategies for a resilient future for research. She has conducted presentations and training on research, data, and technology topics at the Association of American Universities, Association of Public and Land-grant Universities, National Council of University Research Administrators (NCURA), Society of Research Administrators International, the Federal Demonstration Partnership, the Council on Governmental Relations (COGR), and Educause. Schultz is on the Board of Directors of the Open Researcher and Contributor ID, COGR, and NCURA. She has many years of experience in research, software development, non-profit board leadership, and data management and analysis. She has a particular passion for using data to improve the working lives of the researchers who help us understand the world.

Jonathan Snowden is the facility security officer (FSO) at the Office of Research Security at the University of Missouri–Kansas City (UMKC). He is responsible for ensuring UMKC's most sensitive research is properly protected from theft and malign exploitation as defined by federal regulations and research security guidelines. Snowden also works closely with the UMKC and University of Missouri System's research security officers (RSO) in the development, analysis, and implementation of policies and enforcement of the full range of federal and state guidelines. Snowden has been engaged in research security for eight years. He was previously the FSO and initial RSO for Kansas State University (K-State), where, as the chair of the university's Research Security and Integrity Working Group, he guided a cross-functional team in the prioritization, identification, implementation, and education of policies and procedures across the university for the faculty and staff to protect their and K-State's research and reputation. Snowden is also a veteran of a 24-year career in the United States Air Force.

Jason Owen Smith is co-founder and executive director of the Institute for Research on Innovation and Science. He is also professor of sociology and research professor in the Institute for Social Research, and associate vice president for research of institutional capabilities and research intelligence at the University of Michigan. Smith's research examines how complex networks among people and organizations shape knowledge-work and innovation. He is particularly interested in the workings and social and economic impact of research universities, as well as the dynamics of scientific collaboration networks. Findings from this research have been published in outlets including *Administrative Science Quarterly*, the *American Journal of Sociology*, the *American Sociological Review*, *Cell*, *Cell Stem Cell*, *Higher Education*, *JAMA Surgery*, *Management Science*, *Medical Care*, *Nature Biotechnology*, *Nature Methods*, *Organization Science*, *Research Policy*, *Science*, and *Social Studies of Science*. Smith is the author of the 2018 book *Research Universities and the Public Good: Discovery for an Uncertain Future.* He received his M.A. and Ph.D. degrees in sociology at the University of Arizona and a B.A. in sociology and philosophy from the New College of Florida.

Sarah Stalker-Lehoux is deputy chief of research security strategy and policy at the National Science Foundation (NSF). Stalker-Lehoux came to NSF with a wealth of experience focused on protecting U.S. technology. She was most recently a senior compliance specialist in the Directorate of Defense Trade Controls at the U.S. Department of State. While at the State Department, Stalker-Lehoux spent a one-year detail from February 2021 through March 2022 at the National Security Council (NSC) as a director for technology and national security. While at the NSC, she worked on multiple interagency policy committee (IPC) processes related to research security, countering foreign malign influence, the Committee for Foreign Investments in the United States, data security, and critical and emerging technology and export controls. These IPC processes included those related to National Security Presidential Memorandum 33 on protecting U.S. government-supported research and development against foreign government interference and exploitation. Prior to her term at the State Department, Stalker-Lehoux spent nine years at the Department of Commerce's Bureau of Industry and Security where she held various roles, ranging from intelligence analyst to senior export compliance specialist, as well as serving for two years as the special assistant to the Under Secretary for Industry and Security. She has a B.A. degree in psychology and political science from the State University of New York at Albany and an M.P.A. degree with a concentration in international business management from American University.

Gregory F. Strouse is the research security director and the senior advisor to the associate director for laboratory programs at the National Institute of Standards and Technology (NIST). Since 1988, Strouse has been a research physicist at NIST and a fellow of the Washington Academy of Science. His past research of expertise includes the thermodynamic areas of temperature, humidity, pressure, and vacuum with a focus on chip-scale quantum sensors, cold-chain management for vaccines, and the Boltzmann constant determination. Strouse is recognized as a world-leading expert in temperature measurement and the realization and dissemination of the International Temperature Scale of 1990. As the director of NIST research security, he is responsible for research security reviews at NIST and Creating Helpful Incentives to Produce Semiconductors research and development programs. He led the development of the NIST Safeguarding Science Research Security Framework, a risk-based balanced review approach that enables a transparent process that promotes international research science while recognizing the importance of research security. Additionally, Strouse is a founding member of the Office of the Director of National Intelligence Safeguarding Science Roundtable and co-developer of the Safeguarding Science Toolkit.

Geeta Krishna Swamy, M.D., is Haywood Brown, M.D., Distinguished Professor of Women's Health and professor of obstetrics and gynecology, Duke University, having served as director of the Duke Perinatal Research

Center and vice chair for research and faculty development in the Department of ObGyn. She has achieved international acclaim as a clinician researcher and expert in the field of maternal immunization and perinatal infection. As a consultant to the World Health Organization, Swamy contributes her knowledge to advance international work to evaluate the immunogenicity, safety, and efficacy of vaccines in pregnant women. The American College of ObGyn has grown to be the collective voice for women's health, and Swamy has been a leader within that organization for the last two decades. She currently serves as the co-principal investigator for the National Institutes of Health National Institute of Allergy and Infectious Diseases Vaccine Treatment and Evaluation and Center for Disease Control and Prevention Clinical Immunization Safety Assessment. In addition, Swamy has been a leader at Duke and nationally in promoting a culture of scientific integrity and transparency in research. She has been instrumental in developing and leading the School of Medicine's research initiatives in administration, regulatory oversight, and compliance. In 2018, she became vice dean for scientific integrity in the School of Medicine and associate vice president for research for Duke University. In these roles Swamy oversees the Duke Office of Scientific Integrity, which houses the Advancing Scientific Integrity, Services, & Training initiative, conflict of interest, clinical quality management, incident response in research, and research misconduct. She also oversees the Duke Office of Research Initiatives, the Duke Health institutional review board, Office of Research Administration, and Office of Research Contracts.

Steven H. Walker is an independent consultant providing expertise to industry, academia, and government on defense technology development and strategic innovation. Walker recently retired from his position as vice president and chief technology officer of Lockheed Martin, where he was responsible for the company's technology strategy, internal R&D investments, strategic partnerships, and laboratories. Previously, he held the positions of director for the Defense Advanced Research Projects Agency from 2017 to 2020 and deputy assistant secretary of the Air Force for Science, Technology and Engineering from 2010 to 2012. Walker was awarded fellow of the American Institute of Aeronautics and Astronautics (AIAA) and member of the National Academy of Engineering for his nationally recognized work in hypersonic systems. He is a board director for SRI International and is a parent member of the Defense Science Board. Walker holds a Ph.D. and B.S. in aerospace engineering from the University of Notre Dame.

Stephen Welby is deputy director of research for the Sensors and Intelligent Systems Directorate at the Georgia Tech Research Institute. Formerly, Welby was assistant to the president for science and technology policy and former deputy director of national security, White House Office of Science and Technology Policy. Welby previously served as assistant secretary of defense for research and engineering and chief technology officer for the U.S. Department of Defense (DOD) and the principal advisor to the secretary on all matters relating to science, technology, research, and engineering. He also served as deputy assistant secretary of defense for systems engineering where he was responsible for establishing and executing engineering policy and oversight across the department. Welby's responsibilities included engineering design, development and manufacturing of complex military systems, and the engineering review, analysis, and technical risk assessment of the department's portfolio of major acquisition programs. He provided functional leadership to more than 40,000 technical professionals in the DOD engineering and production and quality and manufacturing workforce. Welby also served as the defense standardization executive, directing the DOD program to develop and maintain defense-critical government and commercial technical standards. Welby has more than 28 years of government and industrial experience in technology and product development, including senior leadership positions at the Defense Advanced Research Projects Agency. His experience includes the development of leading-edge aeronautical and space systems, robotics, advanced weapons, high-performance software, and military sensor systems. Welby holds a Bachelor of Science degree in chemical engineering from The Cooper Union for the Advancement of Science and Art, a master's degree in business administration from the Texas A&M University, and master's degrees in computer science and applied mathematics from Johns Hopkins University.

Kristin (Kris) West is the director for research compliance and ethics at the Council on Government Relations (COGR), an association of research-intensive universities, colleges, independent research institutions, and health care institutions that supports its members in the areas of research compliance, administration, financial oversight, and intellectual property. She provides information, regulatory analysis, policy perspective and advice to COGR's members concerning research compliance in the areas of human and animal subjects research, conflicts of interest and commitment, research security, research integrity, and biosafety/biosecurity. West helps lead

COGR's efforts to understand and quantify the impact of research security regulations on the academic research enterprise. Prior to joining COGR, she worked at Emory University for over 30 years, first at an attorney in the Office of the General Counsel and later as Emory's chief compliance officer. West is member of the State Bar of Georgia and serves as an adjunct professor at Loyola University Chicago's School of Law. West is an attorney, and she also holds an M.S. degree in drug regulatory affairs. West holds degrees from the University of Maryland, Mercer University School of Law, and University of Florida College of Pharmacy.

Michael Witherell is an American particle physicist and laboratory director. He has been the director of the Lawrence Berkeley National Laboratory since 2016. Witherell served as director of Fermi National Accelerator Laboratory from 1999 to 2005. He also served as vice chancellor for research at the University of California, Santa Barbara from 2005 to 2016. Witherell received the 1990 Panofsky Prize from the American Physical Society for his research in experimental particle physics. He is a member of the National Academy of Sciences (NAS) and the American Academy of Arts & Sciences. Since 2023, he has served on the NAS Council and on the governing board of the National Research Council. Witherell received his B.S. from the University of Michigan and his Ph.D. in experimental particle physics from the University of Wisconsin.