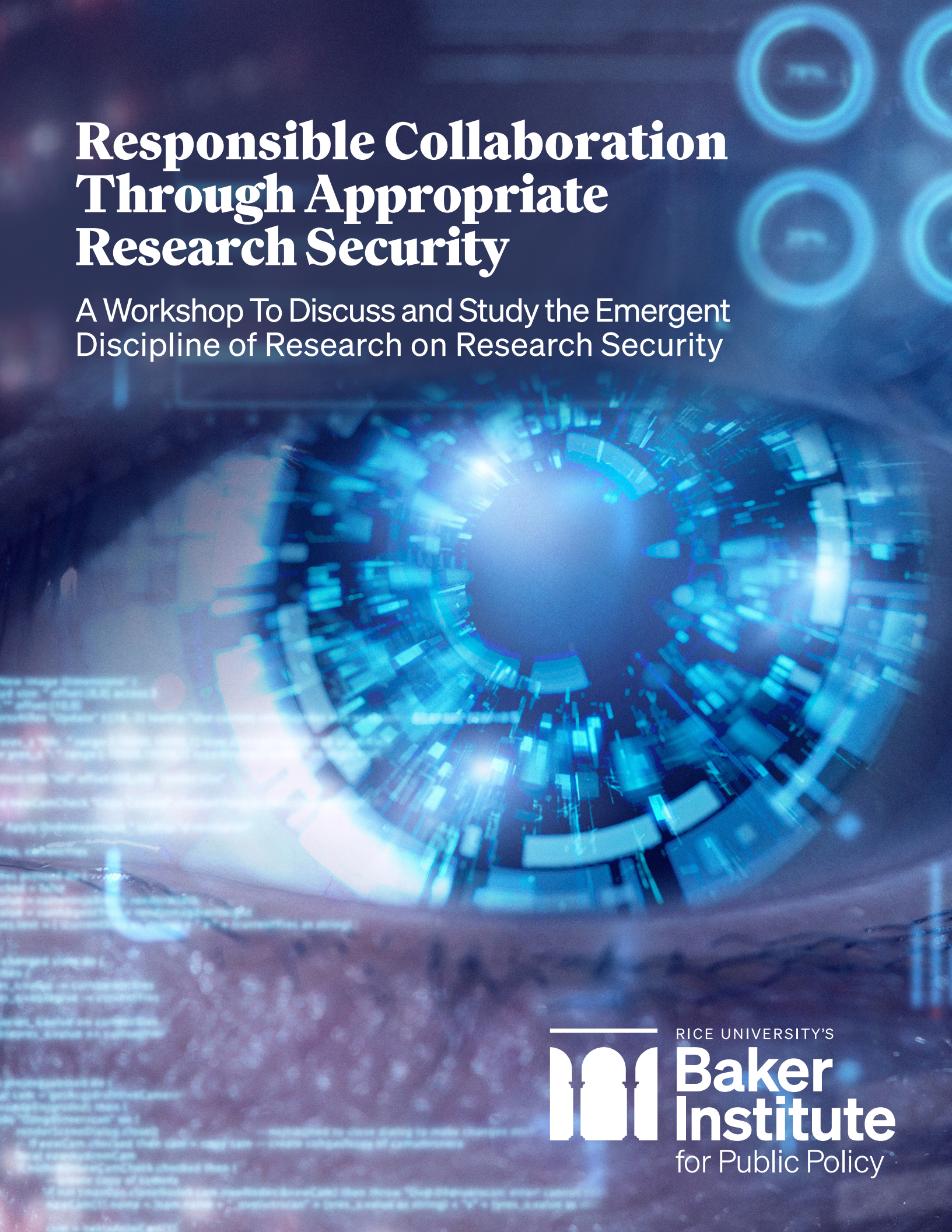
Responsible Collaboration Through Appropriate Research Security

A Workshop To Discuss and Study the Emergent Discipline of Research on Research Security



RICE UNIVERSITY'S
Baker Institute
for Public Policy

Acknowledgements

This workshop and report were funded by NSF OIA #2348714, with supplemental funding from Rice University's Office of Research. The organizing committee would like to thank John Marsh, Neethu Pottackal, Soumya Somani, Jordan Traylor, and Manna Treviño for serving as notetakers.

We would also like to offer special acknowledgements to Paul Zukas for his help organizing and facilitating the conference along with Phyllis McBride and Neal F. Lane for their comments and feedback to strengthen the clarity and consistency of the report.

Finally, we would like to extend our gratitude to Baker Institute staff Laura Hotze, Rachel Dehesa, Serena Storm, and the rest of the Baker Institute staff for their support of the event.

Authors

Tam K. Dao
Kenneth M. Evans
Michael D. Shannon
Christopher Bronk
Claudia Neuhauser
Evan Roberts

Addendum A
Mark P. Haselkorn
David Ribes

Addendum B
Tommy Shih

This publication was produced in collaboration with Rice University's Baker Institute for Public Policy. Wherever feasible, this material was reviewed by outside experts before it was released. Any errors are the authors' alone.

Cover Image by Yuichiro Chino via Getty Images.

Image by Andriy Onufriyenko via Getty Images.

Table of Contents

1 Executive Summary

A topic largely forgotten after the Cold War, research security has reemerged as a top national security concern for academia and the government. The renewed attention on research security issues was brought into sharp, public focus in 2018, when the National Institutes of Health raised concerns about foreign governments using systematic programs to compromise the U.S. research ecosystem as part of the Department of Justice's China Initiative. Foreign covert programs aim to illegally acquire U.S. federally funded research, which is built on a tradition of openness, transparency, impartiality, respect, and fairness (Collins 2018). That research is the bedrock of the current and future U.S. economy in which a rules-based order protects against the theft of innovations produced by sponsored research.

These concerns were addressed in new research security policies enacted under the United States Government-Supported Research and Development National Security Presidential Memorandum (NSPM-33) as well as the research security provisions of the Creating Helpful Incentives to Produce Semiconductors (CHIPS) and Science Act of 2022. This policy is designed to strengthen protections of U.S. government-supported research and development against foreign interference and exploitation. Standing in the way of policy implementation is a poor understanding of what constitutes research security. Compounding the problem is a dearth of research on the pervasiveness of perceived risks; nature of the potential threats; and effective mitigation and prevention strategies. The shortage of research on research security and available data has led to a general lack of awareness among researchers and administrators on foreign influence and its associated risks to individuals and their home institutions.

To advance the field of research security, the U.S. National Science Foundation (NSF) announced its Research on Research Security (RoRS) program in July 2023. RoRS sponsors research in research security as required in the CHIPS and Science Act 2022. Initial thinking on the study of research security came in the form of a 2022 JASON report (JSR-22-08). The commencement of NSF funding has enabled actors in academia and industry to conduct scientific inquiry on this topic and in turn address unanswered questions in the field. NSF's June 2023 issuance of a Dear Colleague Letter (DCL) opened the door for it to receive proposals to host a workshop that would bring together researchers who conduct or have an interest in conducting research in this domain. A workshop proposal was submitted to raise RoRS program awareness and develop a community of practice that includes institutions of higher education, industry, governmental entities, and nonprofit organizations conducting this highly interdisciplinary research. It was awarded to a team led by Rice University in Houston, Texas.

Workshop funding from NSF allowed Rice University and its Baker Institute for Public Policy, the University of Houston, IPTalons, Inc., and the Society of Research Administrators International, to host a two-part invitation-only workshop titled, "Responsible Collaboration Through Appropriate Research Security: A Workshop to Develop the Future Direction of the National Science Foundation's Research on Research Security (RoRS) Program." The workshop allowed the facilitators to assemble national and international academic experts and government and industry leaders across scientific disciplines and sectors of the research community who conduct or have an interest in conducting research on research security.

The results of the workshop generated four main research clusters along with the most pertinent research questions, potential research methods and approaches to address those questions, and associated challenges and hurdles facing the field of research security.

1.1 Findings

RESEARCH CLUSTERS

Workshop discussion generated four broad, interrelated clusters of greatest importance to participants: 1) national security, 2) policy and governance, 3) the research enterprise, and 4) domestic and international collaboration. The importance of access to relevant research security data permeated all four clusters. This relationality is crucial for examining the research questions generated in discussions and measuring the impact of research security policies.

RESEARCH QUESTIONS

Numerous research questions were developed at the workshop, and they were also categorized into four broad groups.

1. What is the importance of research security data, and how can researchers access sensitive data?

2. What is the relationship between stakeholders (i.e., institutional leaders, researchers, research administrators, and the federal government) in maintaining the U.S. competitive advantage in science and technology while promoting and engaging in international collaboration?

3. What is the relationship between research security governance/policies and their intended outcomes?

4. How can researchers increase international collaboration while maintaining a secure and effective research environment?

METHODS AND APPROACHES FOR RESEARCH ON RESEARCH SECURITY

1. There is a need for RoRS to adopt social science methods, particularly from the disciplines of psychology, political science, sociology, and economics.

2. An interdisciplinary research toolkit is essential to answer the most fundamental and important questions in the field of research security.

3. Traditional methods face significant limitations when addressing sensitive topics, such as foreign influence, economic espionage, and research security. Indirect questioning techniques combined with experimental designs can provide anonymity while establishing base rates on sensitive research security topics.

4. Research methods and approaches from the social sciences, such as path analysis and quasi-experimental regression designs can be used to evaluate causal models between the variables of interests and to assess the impact of research security policies.

CHALLENGES AND HURDLES TO RESEARCH ON RESEARCH SECURITY

1. The access to relevant research security data was a frequent discussion point among workshop participants and appeared to be one of the main barriers facing the field of research security.

2. Artificial intelligence and machine learning technologies can enhance existing techniques, such as data masking and data anonymization.

3. There were genuine concerns from workshop participants on whether research security policies, mandates, and consequences are consistently applied and effectively creating the desired outcomes.

4. Creating and maintaining a robust research community of practice encompassing more diverse disciplines that has the research and technical expertise to enhance the field of research security is essential.

5. There is an evident need for well-developed theories on research security that encompass research security concepts and definitions and highlight the complex relationships, both anticipated and unanticipated, between the research security variables of interest.

1.2 Recommendations

The RoRS program should fund novel, interdisciplinary research that addresses the questions generated and challenges identified during the workshop. The workshop offers the following recommendations:

1. The RoRS program should build on this workshop to promote research security support networks. These proposed networking activities should occur regularly and should center on specific clusters, such as those identified during the workshop, to foster communication and new collaborations among social, natural, and medical scientists, engineers, computer scientists, and educators who share a common interest in developing and advancing the new field of research on research security.

2. In line with NSF's review criteria, the RoRS program should fund research that both advances the nascent field of research on research security and addresses broader societal concerns. In particular, funded proposals should produce policy-relevant data, analysis, theory, and tools that inform current and future decision-making on U.S. research security.

3. The RoRS program should align with the core mission of NSF's Directorate for Social, Behavioral, and Economic Sciences (SBE) — to understand human and social behavior — to attract scholars from related disciplines and address researcher motivations. Drawing on this expertise, RoRS-sponsored projects should support and inform the activities and funding of all of NSF's directorates.

4. Although the RoRS program was developed in response to current geopolitical concerns related to China, China should not be the sole focus of funded proposals. Indeed, the program should establish a longer-term vision for addressing future research challenges beyond the immediate policy risk landscape.

5. The RoRS program should serve as a resource for information sharing through the Safeguarding the Entire Community of the U.S. Research Ecosystem (SECURE) Center, the NSF-sponsored clearinghouse for information and training on research security.

6. The RoRS program should explore pathways for stimulating international collaboration on research on research security. This effort should build on the strong participation of both NSF and international partner organizations at the workshop, such as the Commonwealth Scientific and Industrial Research Organization (CSIRO), Japan Science and Technology Agency (JST), Natural Sciences and Engineering Research Council of Canada (NSERC), and UK Research and Innovation (UKRI).

1.3 Conclusion

This report presents the findings of the workshop, including a description of the workshop format, objectives, presentations, and the discussions generated during the workshop and through follow-up interviews with additional subject matter experts. The findings from the workshop and subsequent interviews with subject matter experts reveal several distinct research clusters and pressing questions that are most concerning to the community and that should be addressed through the RoRS program. To tackle these concerns, a broader community of practice needs to be established, encompassing diverse groups of experts, particularly in psychology, political science, sociology, and economics. Widely used methodologies in the social sciences should be employed to address some of the fundamental research questions highlighted at the workshop. The workshop also identified several challenges that were reframed into research questions that can be addressed by the RoRS program.

2 Introduction

The U.S. science and technology (S&T) research and innovation ecosystem is unparalleled, and its contribution to the economy and national security is indisputable. Its success is rooted in the core commitment to having a research environment that emphasizes collaboration, honesty, transparency, objectivity, integrity, fair competition of ideas, and the protection of intellectual capital. The ecosystem is further enhanced and strengthened when people from different parts of the world come together to collaborate to generate new ideas and foster innovation. Research security policy is intended to protect both American S&T innovation, as well as all students, scientists, and other research professionals working and living in the United States.

Unfortunately, as first demonstrated in 2018 by the National Institutes of Health (NIH) as part of the Department of Justice's China Initiative, some foreign governments, including those of China and Russia, do not share these same values and principles and are working to acquire U.S. S&T research and innovation through both licit and illicit means (Collins 2018). Specifically, NIH communicated concerns with undisclosed sources of foreign research support, undisclosed conflicts of interest, and violations of peer review integrity policies. Since then, there has been a growing interest from the federal government, including federal key S&T funding agencies, in safeguarding the U.S. research enterprise from interference from adversarial foreign governments, while maintaining as open and collaborative of a research environment as possible through responsible foreign collaborations (Portman 2019).

The intelligence community (IC) has documented the various types of foreign influence on the U.S. research enterprise, which include offering rewards, theft of intellectual property, and facilitating deception (The Mitre Corporation 2019). Reward can come in many forms. The most concerning and often cited reward mechanism by the IC is the foreign talent recruitment programs (Lauer 2019), which are designed to entice foreign researchers or U.S researchers with cash, a high salary, living accommodations, prominent title, or research funds or facilities to encourage foreign nationals to return to their home country, or to encourage U.S. researchers to apply their skills and provide access to information that will improve the foreign nation's research enterprise. A malign foreign talent recruitment program — as defined in the CHIPS and Science Act of 2022 — is different from other foreign talent recruitment programs in that it encourages unethical or criminal behaviors. Deceptive practices in research include deliberately concealing or omitting information to gain advantage, which is the most widespread type of influence (The Mitre Corporation 2019).

To address these concerns, the federal government issued the NSPM-33 and associated supporting documents and the CHIPS and Science Act 2022 research security provisions to protect U.S. security and openness. These mandates are intended to strengthen protections of U.S. government-supported research and development and to counteract the foreign interference and exploitation strategies employed by some foreign governments (Prabhakar 2024; Subcommittee on Research Security Joint Committee on Research Environment 2022). The implementation of these policies has faced significant challenges due to a general lack of understanding from the research community of what research security entails, the pervasiveness of the problem, and the nature of the potential threats. There is little understanding about effective mitigation and prevention strategies, especially within academia, and a lack of awareness among researchers and administrators about the risks associated with foreign interference.

The need for clarity along with congressional mandates (e.g., CHIPS and Science Act 2022) led NSF to initiate the RoRS program in July 2023. The program is designed to launch and fund the field of research on research security and to increase public understanding of research security in a way that will lead to positive strategies and inform policy that ensures international research collaborations are as open as possible and secure as needed. With support from NSF, Rice University, and the Baker Institute for Public Policy, in collaboration with the University of Houston, IPTalons, Inc., and the Society of Research Administrators International, hosted a two-part invitation-only workshop titled, "Responsible Collaboration Through Appropriate Research Security: A Workshop to Discuss and Study the Emergent Discipline of Research on Research Security" to bring national and international academic experts together with industry leaders across scientific disciplines and sectors of the research community, including members of the government and nongovernment organizations who conduct or have an interest in conducting research in this domain.

3 Workshop Description

3.1 Objectives

The primary objectives of the workshop were: 1) to bring together a diverse array of national and international experts from an equally diverse array of public and private organizations in various disciplines, 2) to identify and discuss current clusters, major issues, and challenges in further developing the field of research on research security, 3) to identify future directions and to develop a vision and roadmap for future research for NSF's RoRS, and 4) to analyze and collate responses from the virtual and in-person workshops and share the workshop outcomes across all sectors of the research community.

3.2 Format: Virtual and In-Person Components

The workshop consisted of two components: one virtual and the other in-person. This two-part format allowed participants to attend a virtual workshop on May 2, 2024, from 1–3 pm (CST), followed by an in-person workshop on May 23–24, 2024, at Rice University's Baker Institute for Public Policy in Houston, Texas. Appendix B provides the agenda for both workshop components along with descriptions of the mini-presentations and the breakout sessions.

3.2.1 Virtual Workshop: Recruiting, Format, Purpose, and Outcome

Recruitment — The organizing committee recruited participants for the virtual workshop through social media (e.g., LinkedIn, X), targeted email campaigns, and partnerships with well-established organizations, and provided individuals who expressed an interest in participating with a Zoom invitation.

Format — The virtual workshop's format consisted of an opening 40-minute presentation to socialize participants to the research security landscape as well as a follow-on set of moderated breakout group discussions, all of which were facilitated by a chair and co-chair.

Purpose — The purpose of these breakout group discussions was to enable participants to collaborate as they generated a list of preliminary research clusters and topics.

Outcome — All breakout group discussions were compiled and summarized into a document that the organizing committee used to refine the in-person workshop agenda and pin down a range of topics to be explored in that workshop. Those who attended the virtual workshop were encouraged to attend the in-person workshop.

3.2.2 In-Person Workshop: Recruiting, Format, Purpose, and Outcome

Recruitment — The organizing committee recruited participants for the in-person workshop by working with multiple organizations, including the Society of Research Administrators International, the Council on Governmental Relations, and APA Justice.

Format — The in-person workshop's format consisted of two keynote addresses, four mini-presentations, four structured breakout sessions moderated by workshop co-chairs, and one unstructured breakout session.

Purpose — The purpose of the in-person workshop was to offer participants an opportunity to discuss research security clusters and topics at a deeper level and to assist them in identifying approaches that could be used to qualitatively and/or quantitatively study such clusters and topics.

Outcome — Participants' diverse viewpoints and academic backgrounds offered an independent, nonpartisan strategy for advancing research on research security and the impact of current and future research security policies on U.S. science, technology, and innovation as well as on the lives and careers of U.S.-based scientists. All breakout sessions had an official note taker and were audio-recorded.

3.3 Demographics

A total of 95 participants attended the two workshops. Participants came from various regions across the U.S.: 25 from the Eastern region, 5 from the Western region, 39 from the Southern region, and 7 from the Midwest region. International participants hailed from Tunisia, the Netherlands, the United Kingdom, Japan, Sweden, Australia, and Canada. Nearly 50% of the participants were from Carnegie classified Research 1 (R1) universities (Carnegie 2024). The remaining participants represented Carnegie classified Research 2 (R2) universities, federal agencies, health universities, for-profit organizations, and nonprofit organizations.

Participants' roles included researchers, research security administrators, institutional leaders, and government officials. Academic disciplines of participants varied, including:

- Research security administrators (21%)
- Natural science and engineering disciplines — computer science, physics, biology, chemistry, engineering, and information technology (24%)
- Social scientists — economics, public policy, psychology, social work, and Chinese culture (25%)
- Professionals from intelligence, legal, and investigative fields (30%)

4 Workshop Findings

4.1 Workshop Research Clusters, Questions, and Identified Challenges

The discussions at the workshop generated four broad yet interrelated clusters that workshop participants considered the most germane: national security, policy and governance, research enterprise, and domestic and international collaboration. Below is a broad summary of these clusters, key research questions, and challenges identified during the workshop. Appendix D provides a detailed breakdown of these four clusters across the different perspectives.

4.1.1 National Security

National Security emerged as one of the main workshop clusters discussed by the participants. A primary discussion point was on the roles of various stakeholders — such as institutional leaders, researchers, research administrators, and the federal government — in maintaining the U.S.' competitive advantage in science and technology while promoting and engaging in international collaboration. A consistent point raised by workshop participants was the need for the field to access, collect, and verify research security incident data. This data is crucial for studying the relationships between research security stakeholders, research security incidents, and their impact on national security.

NATIONAL SECURITY RESEARCH QUESTIONS

1. What indicators or metrics, such as scientific publications, citations, patents, grants, and workforce data, can be developed and used to measure domestic and international research and innovation productivity?

2. How can the social, economic, and cultural effects of "brain drain" be empirically measured using these indicators?

3. Are there methods for quantifying the economic and security risks of licit and illicit transfer of basic research conducted on academic campuses through international collaborations?

4. Who is the ultimate beneficiary of this research?

5. How do risk factors differ across countries, scientific disciplines, and types of institutions?

4.1.2 Policy and Governance

Policy and governance emerged as another major theme during both the virtual and in-person workshop components. Organizations and individuals are subject to complex regulations and resource allocation limits. Policies that researchers perceive as overly stringent can push researchers to seek funding abroad, potentially undermining U.S. domestic research and innovation. Effective policy hinges on balancing oversight limitations with incentives, fostering compliance and collaboration, while streamlining systems and adaptive frameworks to reduce administrative burdens and ensure institutional accountability supporting the U.S.' competitive edge in research and innovation. For this balance to be established, research security policies need to be developed and implemented consistently across the federal government, institutions, and research disciplines.

POLICY AND GOVERNANCE RESEARCH QUESTIONS

1. What are the psycho-social effects on foreign researchers who are subjected to strict reviews and scrutiny upon entering the U.S. or who are employed in the U.S.?

2. How does research security policy and its implementation influence the willingness of U.S. or foreign researchers to collaborate with one another?

3. How do different countries approach research security from a policy and procedural perspective, and what can be learned from these differences?

4. What are the commonalities and divergences in research security practices across various national contexts?

5. What criteria can be developed to better assess the significance and integrity of international research publications without stifling collaboration?

4.1.3 Research Enterprise

The U.S. research enterprise needs to balance the high cost and burden of compliance with the need for innovation and productivity, where regulatory constraints can divert resources and hinder progress. Effective research security requires both internal self-regulation and external oversight, supported by technological tools to reduce administrative burdens, thereby ensuring accountability while fostering collaborative and innovative environments.

RESEARCH ENTERPRISE RESEARCH QUESTIONS

1. What strategies can be developed to make research security awareness, adherence, and compliance appealing to research faculty?

2. How can we measure the burden of regulatory compliance related to research security at academic institutions?

3. How do real and perceived risks in international collaborations differ, and what impact do these perceptions have on the research environment?

4. What are the best practices for establishing, managing, and monitoring foreign satellite campuses to ensure compliance with existing and future research security protocols?

5. What factors influence the decision-making process of international students when choosing where to pursue their research and professions, and how can global talent from adversarial countries be attracted to and retained in the U.S.?

4.1.4 Domestic and International Collaboration

International and domestic collaborations across scientific disciplines enhance innovation and effective global problem-solving, but could increase risks of exfiltration of sensitive information. Building a culture of collective interest rather than individualist approaches fosters stronger organizational ties and personal accountability. Understanding talent growth patterns helps sustain a vibrant research community, and regularly gauging researchers' sense of support and security can inform policies designed to balance openness and protection.

DOMESTIC AND INTERNATIONAL COLLABORATION RESEARCH QUESTIONS

1. How has international scientific collaboration evolved over the last two decades in light of recent and continuing technological and policy developments?
2. What characteristics of research collaborations can inform the creation of a safe and effective future research security environment?
3. How can lessons learned from past successful or unsuccessful collaborations be applied to enhance research security practices and policies?
4. What criteria can be developed to better assess the significance and integrity of international research publications without stifling collaboration?
5. What are the indicators of a "good" international research collaboration?

4.1.5 Identified Challenges

The challenges identified during the workshop have been converted into the following research questions, each addressed in a corresponding subsection of section 4.2:

1. Are there best practices or techniques for collecting sensitive data to establish research security base rates?
2. How can research help with overcoming fear, bias, and policy overreach?
3. How can scholars access relevant data on research security incidents?
4. How can scholars be effectively engaged in research on research security — a field that may make them wary?
5. How can a general theory of research security be developed?

4.2 Methods and Approaches in RoRS

The discussions throughout the virtual and in-person workshops, along with follow-up interviews with participants, highlighted the need for RoRS to adopt social science methods, particularly from the disciplines of psychology, political science, sociology, and economics, to help understand the complex relationships between human behavior and research security policies, and how these constructs impact the U.S. research ecosystem and national security interests. The discussions led to the realization that an interdisciplinary research toolkit is essential to answer the most fundamental and important questions in the field of research security. This section of the report presents potential research methods that will help address the themes and research questions identified in the workshop. The first method addresses the key issue of determining the prevalence of research security issues, while the second method provides a means to examine the causal relationships of the research security variables of interest.

4.2.1 Methods for Establishing Research Security Base Rates

The workshop discussions generated crucial research clusters and questions that need to be addressed in the near term. Understanding the scale and scope of research security issues involving undue foreign influence — as highlighted by Congress, the White House, the intelligence community, and federal funding agencies — proved to be the most pressing issue facing the field. Despite the significance of identifying key research questions, there is an urgent need to understand the prevalence of various research security issues, such as undue foreign influence, theft of intellectual property, and malign foreign talent participation. Currently, there has been no comprehensive effort by any stakeholder group to empirically measure the frequency of these behaviors or experiences within the U.S. research and innovation ecosystem. Establishing base rates for research security incidents and their predictors will aid in developing rigorous risk and protective factors, reducing potential bias in decision-making, increasing transparency in research security policies and guidance, and determining if proposed interventions are effective.

A failure to establish base rates for research security behaviors can lead to flawed reasoning patterns. As one participant noted during a follow-up interview, cognitive errors like the base rate fallacy can occur when individuals or society ignore statistical information in favor of irrelevant information. For example, if two individuals from the same country of origin engage in behaviors that pose research security concerns, one for not disclosing international travel reimbursement funds they received from a foreign collaborator and the other for participating in a malign foreign talent program, a base rate fallacy occurs if the latter is deemed at higher risk without considering the overall prevalence of each behavior.

Examining base rates in research security requires effective analytical methods. While comparative analyses and observational studies using surveys and interviews are common, the use of control group studies are rare. These survey methods face significant limitations when addressing sensitive topics, such as foreign influence, economic espionage, and research security. Recently, research security has become contentious, especially regarding reports of stolen or illegally transferred U.S. intellectual property and federally funded U.S. research being unduly influenced by foreign governments, notably the Chinese government. Despite the federal government's decision to end the China Initiative in 2022, concerns persist among many individuals, particularly those with ancestral ties to China, about racial profiling and presumptions of guilt based on ethnicity and affiliation. Consequently, directly questioning participants on research security matters may lead them to conceal their true attitudes, beliefs, or behaviors out of fear of incrimination and unwarranted law enforcement scrutiny.

UNMATCHED COUNT TECHNIQUE

Social scientists often use surveys to estimate and analyze the prevalence of sensitive attitudes and behaviors. To mitigate biases in self-reported data, social scientists have developed various indirect questioning techniques, such as the unmatched count technique (UCT), to provide more anonymity (Dalton et al. 1994). In UCT, respondents are randomly assigned to control or treatment groups. The control group receives a list of nonsensitive items, while the treatment group receives the same list plus a sensitive item. Respondents indicate how many items apply to them without specifying which ones. The prevalence is estimated by calculating the difference in means between the two groups. Table 1 provides an example of UCT lists that can be used in a survey administered online to estimate the prevalence of research security-related behaviors.

Table 1 —Example of UCT Lists

Control Group	Treatment Group
I have always disclosed my outside employment, whether compensated or uncompensated.	I have always disclosed my outside employment, whether compensated or uncompensated.
I have always disclosed all nonhost institution appointments, both foreign and domestic.	I have always disclosed all nonhost institution appointments, both foreign and domestic.
	I have participated in a foreign talent recruitment program.

Source: Created by authors.
Note: An example of UCT lists that could be delivered online to estimate prevalence of research security-related concerns.

"THREE-CARD METHOD" TECHNIQUE

The General Accountability Office (GAO) developed a similar method called the "three-card method" technique for collecting sensitive data in large-scale surveys (Droitcour 2001; GAO 1999). This method was developed to collect data on immigration but might also be useful for the research security field, where the collection of data has, thus far, been elusive. In this method, three independent representative samples are generated, each of which is selected to be representative of the population. All individuals are presented with three boxes: Box A contains one of the less sensitive answer categories; Box B combines the sensitive category with a number of other less sensitive categories; and Box C contains all other categories. Respondents are asked to report which box applies to them and are instructed not to share which categories applied to them if Box B was their answer. The logic of this method is that if the categories listed in Box A, B, and C are mutually exclusive and, taken together, are exhaustive, they should total 100 percent. As such, subtracting the percentage estimate of the less sensitive categories from 100 yields a remainder that represents an indirect estimate of the percentage in the sensitive category, which in this case would be research security.

CROSSWISE MODEL

Research studies have demonstrated that conventional estimators can be biased when respondents are inattentive. The crosswise model is an increasingly popular design to control for this bias. It helps mitigate the tendency of these instruments to be biased due to inattentive respondents (Atsusaka and Stevenson 2023). In the crosswise model, respondents are asked to read two statements whose veracity is known only to them and to decide if any of the statements are true.

To make this relevant to research on research security, Table 2 provides an example of a crosswise model question to study the prevalence of U.S. professors' participation in a malign foreign talent program. Statement A is the sensitive statement, while Statement B is a nonsensitive statement whose population prevalence is known to the researcher. Respondents are asked whether "both statements are true, or neither statement is true," "only one statement is true," or "don't know." This method helps protect respondents' privacy while allowing researchers to estimate the prevalence of sensitive behaviors accurately.

Similar to the UCT and the three-card method, the crosswise model was developed to protect respondents' privacy when answering sensitive questions. In this method, respondents' answers do not directly reveal whether they agree or disagree with the sensitive statement. Instead, the crosswise model method combines a sensitive statement with a nonsensitive statement and asks respondents to indicate whether both statements are true, neither statement is true, only one statement is true, or they don't know. This approach ensures that individual responses remain confidential. The crosswise model allows researchers to use a statistical formula to determine if the sensitive and insensitive statements are statistically independent. By analyzing the combined responses, researchers can estimate the proportion of respondents for whom the sensitive statement is true, while preserving individual privacy.

Table 2 — Example of Crosswise Model Question

Statement A (Sensitive)	I have participated in a foreign talent recruitment program.
Statement B (Nonsensitive)	I have traveled outside of the country in the past year.
Crosswise Question	How many of the following statements are true? • Both statements are true, or neither statement is true. • Only one statement is true. • I don't know.

Source: Created by authors.
Note: Example of crosswise model question to assess for participation in a foreign talent recruitment program.

The UCT, three-card method, and crosswise model are valuable research methods that enhance the accuracy of data collection, particularly on research security topics like conflicts of interests, conflicts of commitment, or participation in talent programs, by reducing social desirability bias and encouraging truthful responses. UCT, the three-card method, and the crosswise method have been applied successfully to study a wide range of topics, including abortion, anti-immigration, plagiarism, voting, hunting behaviors, medical diseases, immigration status, plagiarism, substance abuse, risky sexual behaviors, infection with rare diseases, tax/fee evasion, antisocial behavior, prejudice, and corruption (Dalton, Wimbush, and Daily 1994; Droitcour, Larson, and Scheuren 2001; Neal 2024; Schnell and Thomas 2023). The use of these methods across sensitive topics suggests that these methods could be adapted to study research security and to establish base rates for various research security-related matters (e.g., participation in foreign talent recruitment program or malign foreign talent recruitment program, nondisclosures, theft of intellectual property, exposure to coercive practices by foreign governments) that are essential to the field. Accurate base rates are necessary to assess the impact of research security policies.

4.2.2 Measuring the Impact of Research Security Policies

There were genuine concerns from workshop participants on whether research security policies and mandates, such as the National Security Presidential Memorandum-33 and the Department of Defense Risk-Based Security Review Process for assessing foreign influence on research project proposals, are consistently implemented and effectively creating the desired outcomes. These concerns have been widely reported from different organizations, including Asian American Advancing Justice (2021). One of the key challenges in assessing the impact of research security policies and mandates has been the lack of available, relevant data and the absence of theoretical frameworks that attempt to conceptualize foreign influence, particularly as it relates to research security.

Randomized controlled trials are the gold standard research methods for hypothesis testing and for measuring the effectiveness of a policy. However, this method may not be ideal given the difficulty of conducting a prospective study to assess research security policies. Through workshop discussions and follow-up interviews with professors in statistics, economics, and political science, participants highlighted approaches such as path analysis and quasi-experimental regression designs that may be used to evaluate causal models between the variables of interests and to assess the impact of research security policies. Path analysis involves construction of an input path diagram in which the relationships between all the variables of interest and the causal direction between these variables are identified. Using a series of statistical analyses, a researcher would then construct an output path diagram that illustrates the relationships as they actually exist. Structural equation modeling (SEM) is one specific form of path analysis and regression discontinuity design (RDD) is one commonly used method of a quasi-experimental regression design.

STRUCTURAL EQUATION MODELING

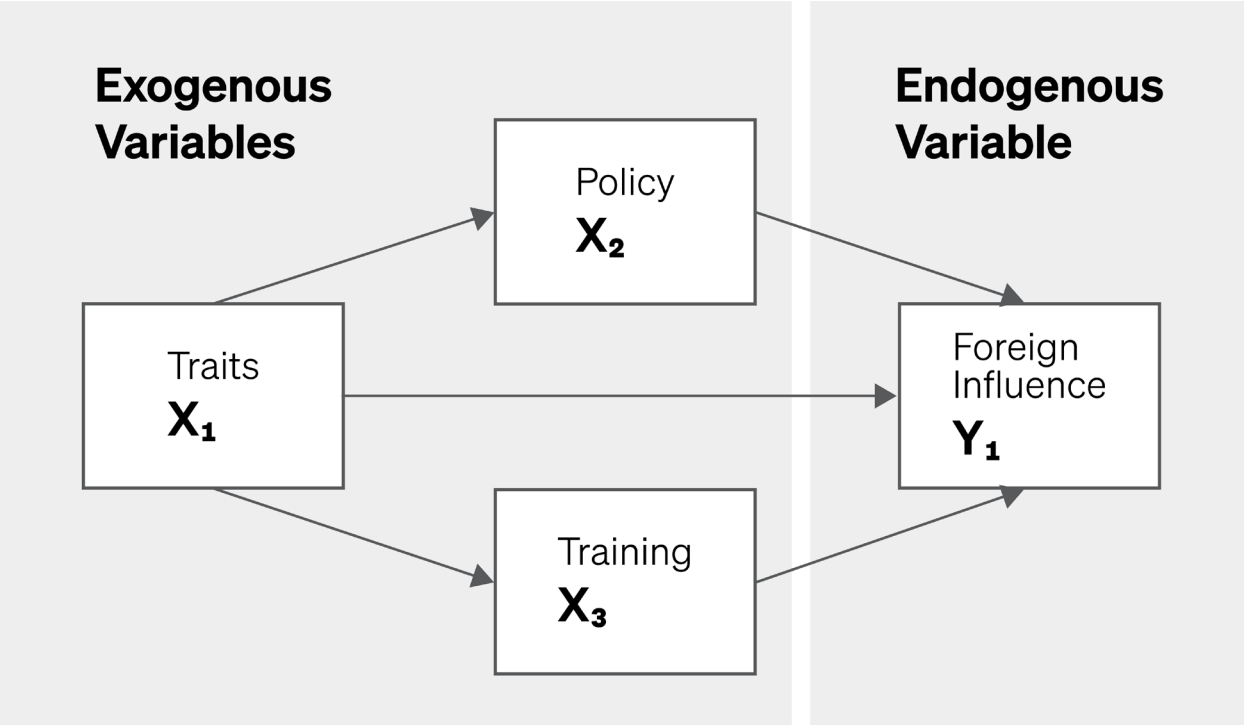
SEM provides a mechanism for researchers in the field of research security to conceptualize how various research security themes and clusters fit together in a network. SEM could assist researchers in proposing hypothesized research security models consisting of a network of direct and indirect causal links among the variables of interest based on theory, experience, and the literature. Such models are currently lacking in the field. Using SEM, coefficients in the hypothesized model are estimated, and the resulting model is evaluated against relevant data from a sample drawn from the population of interest. If the model is not acceptable, the researcher may consider one or more revisions of the model based on experience. If a theoretically credible model with acceptable fit is obtained, the associated estimated direct, indirect, and total causal effects will be described. By employing structural equation modeling, researchers in the research security field are forced to conceptualize a hypothesized model. Based on the themes and research questions identified in the workshop, it is clear that there is a need for a comprehensible research security model that first explains how the themes and clusters are related and can then be tested.

Example: Using one of the themes and clusters identified in the workshop as an example, a researcher in the field of research security might want to develop and test a theory explaining the outcome of research security policies on the modes of foreign influence. JASON reviewed evidence from the intelligence community for foreign influence in the U.S. research enterprise and highlighted four types of influence: reward, deception, coercion, and theft. Using these four types of influence, the researcher specifies the important direct causal determinants of the ultimate outcome, followed by hypothesized causal links among the determinants.

Figure 1 provides a simplified example of a research security path model that illustrates a hypothetical model with research security variables of interest. Variables that are explained by the model are referred to as endogenous variables, while variables that are not explained by the model are called exogenous variables. One approach to developing a model starts with the endogenous variable of interest, such as the four types of influence, and works backward. Thus, based on experience and associated literature, a researcher first specifies the important direct causal determinant of the ultimate outcome. Next, hypothesized causal links among these determinants are specified, creating one or more additional variables. The process continues until the model reflects the scope of the theory desired.

In this example, three exogenous variables — psychological traits, the number of research training sessions offered, and the number of research security policies in place — are the only direct determinants of foreign influence. That is, it is assumed that any other causes of foreign influence will operate only through their effects on these three variables. The endogenous variables are represented with Y's; in the current example, Y_1 is foreign influence. Foreign influence can be measured as the total number of malign foreign talent program participants or any other outcome variable of interest. Exogenous variables are represented with X's, with X_1 being psychological traits, X_2 being research security policies, and X_3 being research security training.

Figure 1 — Example of a Hypothesized Model with Exogenous and Endogenous Variables



Source: Created by authors.
Note: Example of a hypothesized model examining the impact of personality traits, research security training, and policies on foreign influence.

Once model parameters are estimated, SEM allows a test of a hypothesized causal model with correlational data obtained from a sample drawn from a population of interest. The researcher will be able to test the hypothesized model for direct, indirect, and total effects on a collection of data drawn from the population of interest. One of the strengths of using SEM is that it will allow for the researcher to test if the model "fits the data." If the data do not support the hypothesized theory, SEM allows for model revisions by the addition of one or more paths to the initial model. As such, SEM or other causal inference models offer researchers in the field of research security an approach that will generate testable theories consisting of a network of direct and indirect causal links among variables that have been associated through anecdotal data with research security.

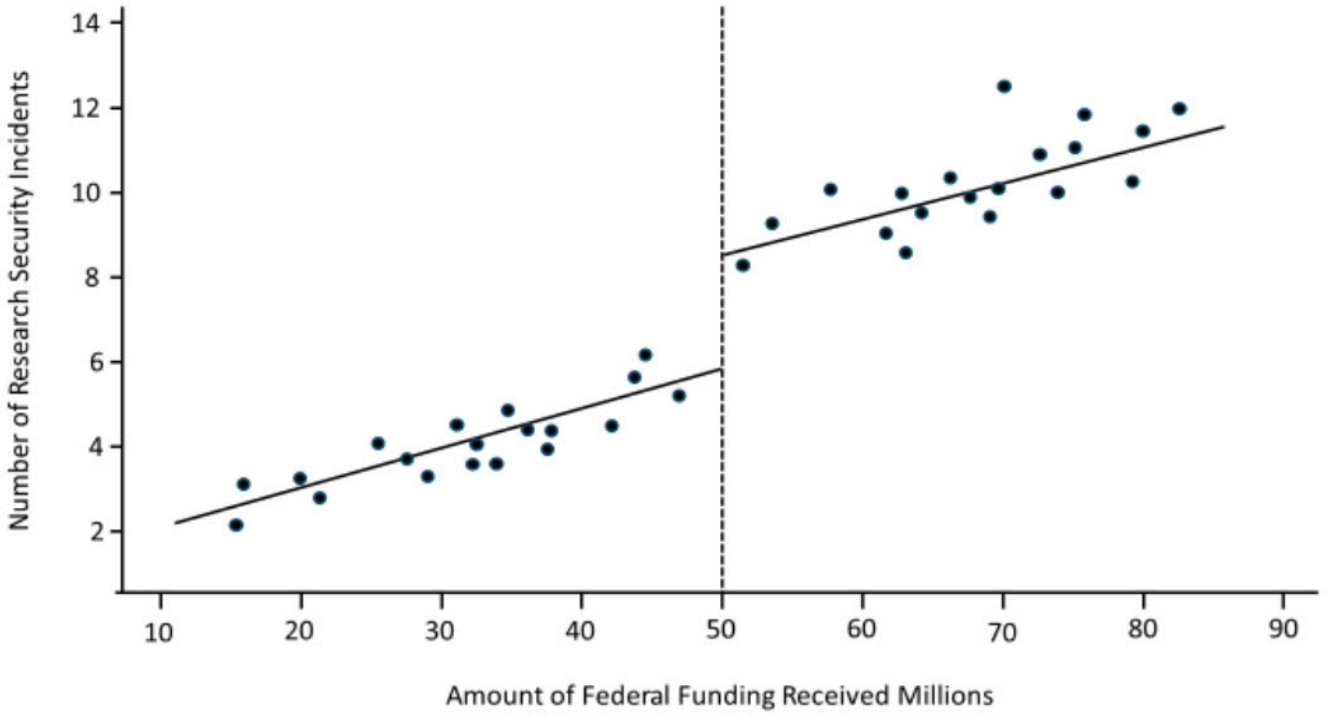
REGRESSION DISCONTINUITY DESIGN

RDD is an impact evaluation method employed by economists and political scientists using a quasi-experimental pretest-posttest design to assess programs. It uses a continuous index that provides the researcher with the ability to assign a cutoff or threshold value, allowing a comparison of observations that are closely above and below the threshold value to estimate the impact of the policy. Despite the absence of an experimental design, an RDD allows a comparison of participants near the threshold value. The assumption is that participants' threshold values are similar to each other and that comparing the outcome of the policy (treatment group) to the counterfactual outcome on the nonrecipient (control group) will provide the treatment effect or the impact of the policy.

Example: For an example, consider the NSPM-33, which is intended to strengthen protections of the U.S. government-supported research and development against foreign government interference and misappropriation. The NSPM-33 directs federal funding agencies to require research institutions receiving $50 million or more in federal funding to establish and operate a research security program that includes elements of cyber security, foreign travel security, insider threat awareness and identification, and, as appropriate, export control training. The eligibility score in our example is the amount of funding received by a research institution, and the cutoff is $50 million.

NSMP-33 dictates that research institutions receiving above $50 million in federal funding establish and operate a research security program, while research institutions with less than $50 million in federal funding are not required to do so. For research institutions with less than $50 million in federal funds, we might expect that these institutions would have fewer documented research security concerns compared to those receiving more than $50 million in federal funds, particularly that pertaining to foreign influence, as shown in Figure 2, which plots research security concerns and amount of federal funding received by an institution. The RDD calculates impact as the difference in outcomes, such as the number of research security concerns, between the units on both sides of the eligibility cutoff, which in our example is research institutions receiving $50 million or more in federal research funds. Using an RDD, a researcher can generate unbiased estimates of a research security program's impact by calculating the change between the factual observed vs the counterfactual.

Figure 2 — Number of Research Security Incidents, Smaller Research Institutions Versus Larger Research Institutions



Source: Created by authors.

The next sections address the three key challenges for the research security field:

- Obtaining relevant data on research security.
- Building a research security community of practice.
- Developing a theory of research security.

4.2.3 The Need for Relevant Data on Research Security

A key challenge for the research security field is access to relevant research security data; indeed, this was a frequent discussion point among workshop participants and appeared to be one of the main barriers facing the field of research security. This was not surprising given that the lack of relevant data was also noted in the 2019 JASON report (JSR-19-21 2019) and the 2022 JASON report (JSR-22-08) as a key challenge to the development of a successful research security program. For some of the workshop participants, access to relevant research security data is essential, and a better system needs to be put in place to allow researchers access to such data.

Three unique but overlapping entities can play an instrumental role in collecting research security data and for sharing relevant research security data for the purpose of scientific inquiries. Funding agencies and universities will have access to data on research security breaches. Both entities are responsible for protecting federally funded research from misappropriation. Federal law enforcement agencies, including the FBI, have access to unclassified and classified data on research security breaches. The FBI, in many instances, will be directly or indirectly involved with university investigations or inquiries related to research security breaches, given their role in identifying and mitigating foreign influence on federally funded research.

Many researchers are suspicious of the government (Asian Americans Advancing Justice, 2021). The access to data on research security breaches will allow researchers to conduct their own studies to validate or invalidate current research security policies. Thus, a research security digital enclave needs to be developed that can support the creation, storage, use, and retrieval of research security incidents across all three entities. The key will be striking a balance between protecting personal sensitive information while retaining the utility of the data for research purposes. One potential solution is to incorporate artificial intelligence and machine learning technologies to enhance techniques already employed, such as data masking and data anonymization, which are commonly used in the healthcare industry. This process can be modified to incorporate research security variables of interest and be carried out as a part of data cleansing and preparation before the datasets are shared with the broader research security community.

4.2.4 Building a Research Security Community of Practice

A second notable challenge to the research security field involves creating and maintaining a robust research community of practice. Our workshop was a step in the right direction and brought together key stakeholders in research security, including national and international experts from diverse scientific disciplines, public and private organizations, government agencies, intelligence communities, federal funding agencies, and university administrators to raise awareness and understanding of research security issues. However, it became evident that a much broader community of practice is necessary to generate a significant impact on the field. The discussions from the workshop were insightful, but due to time constraints, these discussions did not advance toward the deeper level of conversations that are needed given the complex and elusive concept of research security. Therefore, the organizing committee felt it was necessary to arrange additional meetings with workshop participants and other subject matter experts connected through the workshop participants to develop insights into research methods and designs that were mentioned in the workshop.

In follow-up meetings, it became apparent that many experts in the social sciences (e.g., political science, economics, sociology, and psychology) were unaware of the research security landscape. While many of those we interviewed were vaguely familiar with research security since it has been discussed at their respective institutions, they appeared to have the perspective that the topic does not really pertain much to them since their research does not involve classified or sensitive data or technology. A common view of those in the social sciences was that research security applies mostly to those working on sensitive or classified data or technology, that research security does not apply to those working on research intended for publication or dissemination and can lead to unfair treatment of those coming from countries like China. This perspective might be exacerbated by the notion that law enforcement agencies such as the FBI and other government agencies such as the Department of Defense and the Defense Counterintelligence and Security Agency focus their counterintelligence outreach program and training on STEM disciplines when addressing research security concerns.

For the social scientists at the workshop and those we interviewed after the workshop, only after a thorough discussion on research security did participants feel comfortable offering their expertise in research methods and designs. Despite this, some remained apprehensive about applying their expertise to the research security field due to its negative connotations in recent years. Some expressed the fear of engaging in research that may lead to racial profiling or exacerbating the geopolitical tension between the U.S. and countries such as China, Russia, or Iran. Others were reluctant to shift their research focus to research security simply because they do not feel passionate about the field, although their subject matter expertise in various research methods would be beneficial to the research security field.

A plausible approach to addressing this issue is to train those already involved in research security on the research methods and designs mentioned in this report. Instead of focusing primarily on generating interest from other disciplines, an equal amount of time should be dedicated to helping those passionate about research security learn the necessary research methods to conduct studies to advance the field. Additionally, research security support networks should be developed and promoted. Similar to this workshop, these proposed networking activities would occur regularly and should center on specific themes such as those identified in this workshop to foster communication and new collaborations among social scientists, engineers, technology, computer scientists, and educators who share a common interest in developing and advancing the new field of research security. A robust research security community of practice will take time to develop and will require a thoughtful and purposeful design and implementation plan that includes appropriate mentoring and promotion to achieve the desired result.

4.2.5 Developing a Theory of Research Security

The third challenge facing the field is the clear need for a well-developed theory on research security that encompasses research security concepts and definitions, and that highlights the complex relationships, both anticipated and unanticipated, between the research security variables of interest. A well-developed theory on research security will help guide research questions and offer new hypotheses for future research. The immediate issue involves the question of what should come first, collecting and analyzing the research security data to generate a theory on research security, or relying on the current literature to develop a sound theoretical framework on research security that can be used to explain the current foreign influence landscape.

Our interactions with those at the workshop and through our own experiences suggest that a “both/and” rather than an “either/or” approach would be beneficial to the field. Put simply, the building blocks that are essential for research security theory development are available and can be ascertained by examining espionage or foreign influence case studies, many of which are unclassified, documented and presented at various law enforcement conferences. These case studies contain essential elements for theory development, including information on assessing an individual’s personality, as well as on available university and government resources to assist with foreign influence risk assessment. Simultaneously, comparative analyses and observational studies using surveys and interviews — as mentioned previously — can be used to collect quantitative data and used in turn to create or modify research security theory based on anecdotal data obtained primarily through case studies on foreign influence or espionage.

As stated earlier in this report, the research on the research security field lacks data on the prevalence or base rates of various research security incidents, making it challenging to determine the scale and scope of foreign influence at the individual and organizational level. For theory development, it would be ideal to have quantitative data to generate theory to explain why individuals engage in behaviors that constitute conflicts of interests or conflicts of commitment. However, the field is in such a nascent phase that it might be more beneficial to start involving individuals who have subject matter expertise to help with theory development on research security. Based on workshop discussions, this might be difficult since those who have subject matter expertise in research security investigations (e.g., law enforcement backgrounds) do not have the necessary expertise on theory development, and those from academia with expertise in theory development might not have enough research security knowledge to formulate the components that lead to research security incidents.

5 Summary and Recommendations

5.1 Findings

This workshop generated four broad research clusters to guide the NSF RoRS program: national security, policy and governance, research enterprise, and domestic and international collaboration. Each theme spurred the development of numerous research questions and challenges, as well as possible methods for exploring these questions and approaches for addressing identified challenges.

METHODS AND APPROACHES FOR RESEARCH ON RESEARCH SECURITY

1. There is a need for RoRS to adopt social science methods, particularly from the disciplines of psychology, political science, sociology, and economics, to help understand the complex relationships between human behavior and research security policies, and how these constructs impact the research ecosystem and national security interests.

2. An interdisciplinary research toolkit is essential to answer the most fundamental and important questions in the field of research security. This toolkit should include research methods that will help address key issues, such as determining the pervasiveness of research security issues, developing and testing theoretical research security models, and assessing the impact of research security policies.

3. Comparative analyses, observational studies using surveys and interviews, and control group studies are commonly used in the social sciences. However, these methods face significant limitations when addressing sensitive topics, such as foreign influence, economic espionage, and research security. Indirect questioning techniques combined with experimental designs, such as the unmatched count technique (UCT), can provide anonymity while establishing base rates on sensitive research security topics.

4. Research methods and approaches from the social sciences, such as path analysis (e.g., structural equation modeling) and quasi-experimental regression designs (e.g., regression discontinuity design) can be used to evaluate causal models between the variables of interests and to assess the impact of research security policies that offer a balanced approach to the gold standard randomized controlled prospective study design.

CHALLENGES AND HURDLES TO RESEARCH ON RESEARCH SECURITY

1. Access to relevant research security data was a frequent discussion point among workshop participants and appeared to be one of the main barriers facing the field of research security. To overcome this challenge, a research security enclave needs to be developed that can support the creation, storage, use, and retrieval of research security incidents across government, industry, and academia.

2. Artificial intelligence and machine learning technologies can enhance existing techniques, such as data masking and data anonymization. These tasks can be carried out as a part of data cleansing and preparation before the datasets are shared with the broader research security community.

3. There were genuine concerns from workshop participants as to whether research security policies and mandates are consistently implemented and effectively creating the desired outcomes.

4. Creating and maintaining a robust research community of practice that encompasses more diverse disciplines (e.g., economics, political science, instructional design, etc.) who have the research and technical expertise to enhance the field of research security is essential.

5. There is an evident need for well-developed theories on research security that encompass research security concepts and definitions, and that highlights the complex relationships that are anticipated and unanticipated between the research security variables of interest.

5.2 Recommendations

The RoRS program should fund novel, interdisciplinary research that addresses the questions generated and challenges identified during the workshop. The workshop offers the following recommendations:

1. The RoRS program should build on this workshop to promote research security support networks. These proposed networking activities should occur regularly and should center on specific clusters — such as those identified during the workshop — to foster communication and new collaborations among social, natural, and medical scientists, engineers, computer scientists, and educators who share a common interest in developing and advancing the new field of research on research security.

2. In line with NSF's review criteria, the RoRS program should fund research that both advances the nascent field of research on research security and addresses broader societal concerns. In particular, funded proposals should produce policy-relevant data, analysis, theory, and tools that inform current and future decision-making on U.S. research security.

3. The RoRS program should align with the core mission of NSF's Directorate for Social, Behavioral, and Economic Sciences (SBE) — to understand human and social behavior — to attract scholars from related disciplines and address researcher motivations. Drawing on this expertise, RoRS-sponsored should support and inform the activities and funding of all of NSF's directorates.

4. Although the RoRS program was developed in response to current geopolitical concerns related to China, China should not be the sole focus of funded proposals. Indeed, the program should establish a longer-term vision for addressing future research challenges beyond the immediate policy risk landscape.

5. The RoRS program should serve as a resource for information sharing through the Safeguarding the Entire Community of the U.S. Research Ecosystem (SECURE) Center, the NSF-sponsored clearinghouse for information and training on research security.

6. The RoRS program should explore pathways for stimulating international collaboration on research on research security. This effort should build on the strong participation of both NSF and international partner organizations at the workshop, such as the Commonwealth Scientific and Industrial Research Organization (CSIRO), Japan Science and Technology Agency (JST), Natural Sciences and Engineering Research Council of Canada (NSERC), and UK Research and Innovation (UKRI).

Image by Teera Konakan via Getty Images.

6 Addendum A

Qualitative RoRS

The focus of any workshop is determined by those who attend. The focus of those who attended the RoRS workshop was predominantly — although not exclusively — quantitative. The majority of discussion centered around data: how to get it, how to analyze it, and how to develop theories for making a larger sense of it. This is a critical perspective, and future RoRS research must carry this quantitative work far forward.

There was also valuable discussion of qualitative topics, such as forming and catalyzing the RoRS research community and the importance of understanding the research security ecosystem. While the significance of these topics was recognized, not many attendees represented these critical fields of relevant expertise: sociologists, ethnographers, designers, change management experts, and specialists in socio-technical systems. These are just some of the vibrant fields that will push forward the qualitative side of RoRS. And, working closely with their more quantitative colleagues, these researchers will help lead the integration of all RoRS research, quantitative and qualitative, into a complete, coherent, nationally vital field. NSF already values and funds this qualitative side of research, both in the SBE Directorate and through interdisciplinary programs such as the Research Coordination Network (RCN) funding mechanism. RCNs, in particular, are relevant to the formation of new research communities like RoRS. In addition, some universities house interdisciplinary centers like the University of Washington's Collaborative Systems for Security, Safety, and Resilience (CoSSaR) that take qualitative and engineering approaches to RoRS issues. Much of the needed expertise and knowledge is already out there, though it needs to be retrofitted to research security. As RoRS evolves into an exciting and dynamic field of research with critical world impact, it will become easier to attract established experts to contribute to the burgeoning field.

In addition, as changes stemming from new requirements for research security cascade across a range of kinds of institutions, and within their administrative operations, research will be needed to understand these changes in terms of formal structures and informal cultures. This will include understanding the practical work of administrators and researchers, their intersections and their frictions. Questions and issues to be addressed will include:

- How will research security needs differ at small and large research universities, at health-focused research institutes, at HBCUs, or at other minority-serving institutions?
- What metrics can we institute to track organizational transformations to research security and identify trouble spots? What new data and information are needed?
- In addition to quantitative data and statistical approaches, understanding the practices and cultures of administration and research will demand the development of, for instance, case studies, user scenarios, organizational mapping, communities of practice, and sociocultural evaluations.
- International-comparative research and historical-comparative research will be able to learn from how others have sought to approach research security, including by characterizing success and failure cases. Canada and the EU are also ramping up research on research security. Are there synergies between them and the U.S. that
- we could explore?

Experts who focus on these topics and approaches can be drawn from fields such as privacy, management and information systems (MIS), organizational science, science and technology studies (STS), practice studies, and service science.

Finally, in addition to understanding people and their interactions (such as researchers and administrators), we must also understand the technical systems that support them, adopting a "sociotechnical approach." What kinds of new support systems will be needed? What can we learn from other fields who have accomplished similar organizational transformations? These are largely research questions for the fields of design and IT, and experts who focus on these topics and approaches can be drawn from fields such as privacy and security design, MIS, human-computer interaction (HCI), computer-supported cooperative work (CSCW), and design research more widely.

This addendum is a reminder that while the first RoRS workshop took exciting steps toward articulating the challenges and goals of this new and exciting field, there is much more to look forward to, especially in the realm of qualitative RoRS.

7 Addendum B

Finding an Appropriate Balance Between Research Security and Openness Is a Priority

International collaboration is an important indicator of research excellence and quality. Not only is international collaboration necessary to maintain or strengthen competitiveness on individual, organizational, and aggregated national levels, but it is also necessary to find solutions to global challenges and increase understanding between different countries and cultures.

Fortunately, we see increased academic interaction between a more diverse palette of countries today. Still, the global research system is still highly divided and science of the highest quality is usually conducted in North America, Europe, and China, with the latter rising from relative science obscurity to a leading science nation in just three decades. Not surprisingly, the most frequent international collaborations, especially those with high citation impact, occur generally between three regions: Europe, North America, and China (Wagner and Cai 2022). Jointly, the collaborations of these regions make up the lion's share of international collaborations that are highly cited and impactful, particularly in the STEM field.

On the global stage, the geopolitics of recent years have affected the era of open research collaboration. With the emergence of a multipolar world, governments have increasingly been concerned about the academic and research sectors as vectors for the transfer of technologies and foreign interference, which can adversely impact national competitiveness. Today, more attention is aimed at national interests than ever before. Research security plays a vital role in systematically integrating national interests in the research enterprise.

However, it is also important to articulate the goals and the processes through which they can be achieved and critically analyze the impact and proportionality of the research security measures. Goals in liberal democracies with advanced science capabilities associated with protecting a national research system include:

- **Ensuring national security.** This goal can relate to safeguarding through export controls, research, and technologies that can be used for dual items so they do not end up in the hands of adversarial states. National security measures can also be about protecting critical national research infrastructure from espionage.
- **Maintaining competitiveness on an aggregated national level** and ensuring that nationally funded research contributes to economic value creation and research strength. The ability to utilize research to strengthen the economy translates into increased possibilities for societal stability and utilizing soft power on the multilateral stage.
- **Protecting liberal democratic values.** In a multipolar world, the friction between liberal democracies and authoritarian states is apparent. The relative strengthening of authoritarian states and authoritarianism (also seen within liberal democracies) in the world poses threats to the values espoused in liberal democracies, including the rule of law, an open society, and individual rights. Research collaborations have, over time, accumulatively strengthened the power of various authoritarian states. Western governments have argued that some authoritarian states have been able to systematically use the open, collaborative system to their advantage.

Based on these three goal domains, research security has become a term acknowledging the need for action and recognizing that the world is currently facing considerable uncertainties in the geopolitical sphere. In Western countries with advanced scientific and technological capabilities, government actors have also intensified the securitization of national S&T systems, i.e., constructing scientific matters as a security problem. However, research security has no shared definition across organizations and countries. There is a plethora of different activities, definitions, and vague uses of the term by various actors from the governmental level down to the individual. This makes it difficult to evaluate whether research security measures have an effect. Against this background, an important question is whether present research security measures are sound. Given that there is no unified definition or view of research security and its goals, it is a challenge to evaluate intended outcomes and effectiveness. It is, however, possible to trace specific activities that are conducted under the banner of research security and investigate some of these in relation to the three goal domains mentioned above.

Here, the soundness of research security measures and practices relates to whether they can:

- Reduce vulnerabilities and meaningfully address identified security threats.
- Maintain competitiveness and openness to a high degree.
- Not erode democratic institutions.

Some inferences can be drawn from some existing practices concerning how effective they are in addressing objectives in the three goal domains. These examples can also provide directions for further work and identify areas that need significant reconsideration.

Reducing vulnerabilities: A specific measure that has been adopted to reduce identified vulnerabilities, such as illicit or unwitting technology transfers, has been the introduction of stricter disclosure requirements regarding professional associations and funding sources through NSPM-33. The increased level of disclosure and transparency reduces double dipping and the risk of unwitting technology transfer. Nonetheless, unwitting technology transfer also requires the identification of what is a matter of national security and what is not. An example that has not been successful in that aspect is the China Initiative. A recent study shows that the China Initiative has been far less successful than stated by the U.S. Department of Justice (Guo, Aloe, and Hao 2021). The China Initiative led to few convictions that were actually related to national security, although more than 160 indictments were made. In its latter stages, the China Initiative focused more on targeting issues related to research integrity, which suggests that the problem description — i.e., what is this a problem of? — requires much more granularity and a more detailed data/evidence base. However, perhaps the most damaging effects of the China Initiative have been the erosion of trust between security actors and the academic sector and the failure to protect fundamental civil rights.

Maintaining competitiveness: Disclosure requirements for federal funding have likely successfully addressed double-dipping problems. Generally, though, the increased focus on research security tends to have a chilling effect on international research collaboration and mobility (Jia et al. 2024). The chilling effect will likely negatively impact competitiveness in the long term, as it is highly dependent on working in an international arena.

Not eroding democratic institutions: Securitization is always a challenge for democratic institutions due to often untransparent processes. National security threats are not commonly discussed in detail. The use of information asymmetry is a form of reflexive control where authorities are requesting or seeking action (de Goeij 2023). However, the motives of the sender and the accuracy of the information are unclear to the actors being asked to change their behaviors. Over time, the strategic use of information asymmetry will erode principles such as institutional autonomy and academic freedom. Hence, securitization cannot be a blanket approach, but a more granular and transparent approach will be needed. Increasing transparency might require legislative or behavioral changes so that security agencies can release more information or new ways of working between security agencies and academia to identify and proactively deal with the truly problematic case patterns.

Nonetheless, it is essential to note that success is not about meeting objectives in just one of the three goal domains. The main overarching goal should integrate reducing vulnerabilities, maintaining openness, and not eroding democratic institutions.

RECOMMENDATIONS

- Focus on the fact that an essential goal of research security is to enable international collaboration and that securitization cannot be an end by itself.
- Define research security in a more precise way with international partners.
- Develop a more granular understanding of what research security should not be doing (avoiding blanket securitization).
- Identify research security practices and trace their impact and consequences.
- Integrate goals related to national security, competitiveness, and protection of democratic institutions.
- Based on the above, develop a national and international agenda for research security.

8 References

Asian Americans Advancing Justice. 2021. "AAJC Submits Comment to the White House Office of Science and Technology Policy Raising Concerns of Profiling and Criminalization of Asian Americans and Asian Immigrants." https://www.advancingjustice-aajc.org/press-release/asian-americans-advancing-justice-aajc-submits-comment-white-house-office-science-and.

Atsusaka, Yuki, and Randolph T. Stevenson. 2023. "A Bias-Corrected Estimator for the Crosswise Model with Inattentive Respondents." Political Analysis 31, no. 1 (January): 134–48. https://doi.org/10.1017/pan.2021.43.

Carnegie Classification of Institutions of Higher Education. "2025 Research Designations." Accessed August 16, 2024. https://carnegieclassifications.acenet.edu/carnegie-classification/research-designations/

Collins, Francis. 2018. "Statement on Protecting the Integrity of U.S. Biomedical Research." Department of Health and Human Services, National Institutes of Health, August 23, 2018. https://www.nih.gov/about-nih/who-we-are/nih-director/statements/statement-protecting-integrity-us-biomedical-research.

Dalton, Dan R., James C. Wimbush, and Catherine M. Daily. 1994. "Using the Unmatched Count Technique (UCT) to Estimate Base Rates for Sensitive Behavior." Personnel Psychology 47, no. 4 (December): 817–29. https://doi.org/10.1111/j.1744-6570.1994.tb01578.x.

de Goeij, Maria W. R. 2023. "Reflexive Control: Influencing Strategic Behavior." The US Army War College Quarterly: Parameters 53, no. 4 (Winter 2023): art. 14. https://press.armywarcollege.edu/parameters/vol53/iss4/14/.

Droitcour, Judith A., Eric M. Larson, and Fritz J. Scheuren. 2001. "The Three Card Method: Estimating Sensitive Survey Items — With Permanent Anonymity of Response." Proceedings of the Annual Meeting of the American Statistical Association, August 5–9, 2001. http://www.asasrms.org/Proceedings/y2001/Proceed/00582.pdf.

Government Accountability Office. 1999. "Survey Methodology: An Innovative Technique for Estimating Sensitive Survey Items." Washington, DC: Government Printing Office. https://www.gao.gov/assets/ggd-00-30.pdf.

Guo, Eileen, Jess Aloe, and Karen Hao. 2021. "The US Crackdown on Chinese Economic Espionage Is a Mess. We Have the Data to Show It." MIT Technology Review. December 2. https://www.technologyreview.com/2021/12/02/1040656/china-initative-us-justice-department/.

Jia, Ruixue, Margaret E. Roberts, Ye Wang, and Eddie Yang. 2024. "The Impact of US-China Tensions on US Science: Evidence from the NIH Investigations." PNAS 121, no. 19 (April 30): e2301436121. https://doi.org/10.1073/pnas.2301436121.

Lauer, Michael. 2019. "Responding to Undue Foreign Influence and Security Concerns: Perspectives of the National Institutes of Health." Briefing on JASON Summer Study 2019, National Institutes of Health, July 10, 2019, La Jolla, CA.

Neal, Zachary. 2024. "Large Sampling Errors When Using the Unmatched Count Technique to Estimate Prevalence: A Simulation Study." Survey Practice 17 (February). https://doi.org/10.29115/SP-2024-0002.

Portman, Rob. 2019. "Threats to the U.S. Research Enterprise: China's Talent Recruitment Plans." Staff Report, Committee on Homeland Security and Governmental Affairs, Permanent Subcommittee on Investigations, United States Senate. https://www.hsgac.senate.gov/wp-content/uploads/imo/media/doc/2019-11-18%20PSI%20Staff%20Report%20-%20China's%20Talent%20Recruitment%20Plans%20Updated2.pdf.

Prabhakar, Arati. 2024. "Guidelines for Research Security Programs at Covered Institutions." Memorandum for the Heads of Federal Research Agencies, Executive Office of the President, Office of Science and Technology Policy, Washington, DC. https://www.whitehouse.gov/wp-content/uploads/2024/07/OSTP-RSP-Guidelines-Memo.pdf.

Schnell, Rainer, and Kathrin Thomas. 2023. "A Meta-Analysis of Studies on the Performance of the Crosswise Model." Sociological Methods & Research 52, no. 3: 1493–518. https://doi.org/10.1177/0049124121995520.

Subcommittee on Research Security Joint Committee on Research Environment, National Science and Technology Committee. 2022. "Guidance for Implementing National Security Presidential Memorandum 33 (NSPM-33) on National Security Strategy for United States Government-Supported Research and Development." Washington, DC: United States Government. https://www.whitehouse.gov/wp-content/uploads/2022/01/010422-NSPM-33-Implementation-Guidance.pdf.

The Mitre Corporation. 2019. "JSR-19-21 Fundamental Research Security." Washington, DC. https://www.nsf.gov/news/special_reports/jasonsecurity/JSR-19-2IFundamentalResearchSecurity_12062019FINAL.pdf.

The Mitre Corporation. 2022. "Research Program on Research Security (JSR-22-08)." Washington, DC. https://nsf-gov-resources.nsf.gov/2023-03/JSR-22-08 NSF Research Program on Research Security_03152023_FINAL_1.pdf?VersionId=IwtxqUjbqGNmbtJ7E66IqQBbt9gzCV8A.

Wagner, Caroline S., and Xiaojing Cai. 2022. "Changes in Co-publication Patterns among China, the European Union (28) and the United States of America, 2016–2021." arxiv.org. February 11, 2022. https://doi.org/10.48550/arXiv.2202.00453.

Appendix A: Workshop Organization

Virtual: May 2, 2024

In-Person: May 23–24, 2024, at Rice University's Baker Institute for Public Policy, Houston, Texas.

Organizing Committee

Kenneth M. Evans and Tam K. Dao
Rice University

Chris Bronk and Claudia Neuhauser
University of Houston

Evan Roberts
Society of Research Administrators International

Michael D. Shannon
IPTalons, Inc.

Workshop Chairs and Co-Chairs

Tommy Shih
Lund University

Mickey Stevenson
Rice University

Diane Cutler
U.S. Department of Health and Human Services, Office of Inspector General (Former Affiliation)

Terry Oroszi
Wright University

Appendix B: In-Person Workshop Agenda

May 23, 2024

7:15 am **Check-In and Breakfast**
Rice University's Baker Institute for Public Policy

7:45 am **Introduction, Workshop Objectives, and Housekeeping Matters**
Tam K. Dao, Rice University

8:00 am **Welcome Remarks**
Ramamoorthy Ramesh, Executive Vice President for Research, Rice University
Professor for Materials Science and Nanoengineering; Professor of Physics and Astronomy

8:30 am **Keynote Speech**
Rebecca Keiser, Chief Research Security Strategy and Policy, National Science Foundation

9:15 am **Break**

9:20 am **JASON Study on Fundamental Research — Zoom Presentation**
Peter H. Fisher, Thomas A. Frank Professor of Physics, Massachusetts Institute of Technology

9:50 am **NSF Landscape Data — Zoom Presentation**
John M. Finamore, Chief Statistician, National Center for Science and Engineering Statistics, National Science Foundation

10:20 am **Break**

10:30 am **Framing and Integrating Research on Responsible Internationalization and Research Security**
Tommy Shih, Associate Professor of Business Administration, Lund University; Senior Advisor at the Swedish Foundation for International Cooperation in Research and Higher Education (STINT)

11:30 am **Impact of U.S.-China tensions on U.S. Science — Zoom Presentation**
Ruixue Jia, Associate Professor, University of California San Diego

Noon **Lunch**

1:00 pm **Breakout Session Objectives and Room Assignments**
Christopher Bronk, Associate Professor, Hobby School of Public Affairs, University of Houston

1:15 pm **Transition to Breakout Session**

1:30 pm **First Breakout Session (Structured)***

National Security	Policy & Governance	Research Enterprise	Int. Collaboration
Rm 114	*Rm 271*	*Rm 283*	*Rm 330*
Kenny	Chris	Terry	Tommy
Diane	Mike	Mickey	Evan
Jordan	John	Neethu	Manna
Group 4	*Group 1*	*Group 2*	*Group 3*

4:20 pm **Break**

4:30 pm **Wrap-Up Discussion and Closing Thoughts**
Evan Roberts, Executive Director, Society of Research Administrators International
Tam K. Dao

5:00 pm **Reception:** Hors d'oeuvres and light refreshments

6:00 pm **Chair and Co-Chair Closed Discussion**

*** Breakout session teams:**
Kenneth M. Evans, Diane Cutler, Jordan Traylor, Christopher Bronk, Michael D. Shannon, John Marsh, Terry Orozi, Mickey Stevenson, Neethu Pottackal, Tommy Shih, Evan Roberts, Manna Treviño.

May 24, 2024

7:15 am **Check-In and Breakfast**

8:00 am **Keynote Speech**
Christopher Raia, Deputy Assistant Director, Federal Bureau of Investigation

8:20 am **JASON Study on Research on Research Security Program**
Paul Zukas, Director of Research Security, Rice University
Michael D. Shannon, IPTalons, Inc.

8:50 am **Break and Transition to Breakout Session**

9:00 am **Third Breakout Session (Structured)**

National Security	Policy & Governance	Research Enterprise	Int. Collaboration
Rm 114	*Rm 271*	*Rm 283*	*Rm 330*
Kenny	Chris	Terry	Tommy
Diane	Mike	Mickey	Evan
Jordan	John	Neethu	Manna
Group 3	*Group 4*	*Group 1*	*Group 2*

10:20 am **Break**

10:30 am **Fourth Breakout Session (Structured)**

National Security	Policy & Governance	Research Enterprise	Int. Collaboration
Rm 114	*Rm 271*	*Rm 283*	*Rm 330*
Kenny	Chris	Terry	Tommy
Diane	Mike	Mickey	Evan
Jordan	John	Neethu	Manna
Group 2	*Group 3*	*Group 4*	*Group 1*

11:50 am **Lunch** (Chairs will have working lunch)

12:50 pm **Mini-Presentation from Chairs**
Information collected during Structured Breakout Sessions will be shared with participants.

1:20 pm **Overview of Unstructured Breakout Session**
Christopher Bronk, Associate Professor, Hobby School of Public Affairs, University of Houston

1:30 pm **Break and Transition to Unstructured Breakout Session**

1:40 pm **Unstructured Breakout Session**

National Security	Policy & Governance	Research Enterprise	Int. Collaboration
Rm 114	*Rm 271*	*Rm 283*	*Rm 330*

Participants will pick and choose which sessions they would like to attend and contribute to. The unstructured breakout session allows participants to move freely around to connect, share their knowledge, and interact with individuals they have not yet engaged with at the workshop.

3:00 pm **Wrap Up Discussion and Closing Thoughts**
Kenneth M. Evans | Claudia Neuhauser | Tam K. Dao | Evan Roberts
Christopher Bronk | Michael D. Shannon

3:30 pm **Chair and Co-Chair Meeting Closed Discussion**

Appendix C: Virtual and In-Person Workshop Participants

Last Name	First Name	Affiliation
Amal	Rabti	The National Institute for Research and Physico-Chemical Analysis (INRAP)
Atchley	Trey	The University of Texas System
Bante	Holly	University of Cincinnati
Baumer	Alexa	U.S. National Science Foundation (NSF)
Beitle	Bob	University of Arkansas
Bernard	Florent	EU Delegation to the USA
Bickenbach	Jared	Baylor University
Bonenkamp	Berry	Dutch Research Council (NWO)
Boone	Jen	University of Maryland
Carpenter	Joshua	CRDF Global
Cartledge	Erica	National Security and Resilience, Commonwealth Scientific and Industrial Research Organisation (CSIRO)
Carwile	Zach	Texas A&M University
Chambliss	Kevin	Baylor University
Chen	Jing	Rice University
Chottiner	Cameron	Office of Rep. Dan Crenshaw
Collins	Gabriel	Rice University's Baker Institute for Public Policy
Cothren	Jack	University of Arkansas
Cox	Jim	Rice University
Czarnezki	Ian	University of Arkansas
d'Hooghe	Ingrid	Clingendael China Centre
Desai	Anand	Clarivate
Droegemeier	Kelvin	NSF
Durant	Charles	Oak Ridge National Laboratory
Dworak	Jennifer	Southern Methodist University
Eads	LJ	Parallax Advanced Research Corporation
Farnell	Chris	University of Arkansas
Finamore	John	NSF
Fisher	Peter	Massachusetts Institute of Technology
Forsberg	Jeremy	University of Texas at Arlington
Fuhrmann	Matt	Texas A&M University
Gamache	Kevin	Texas A&M University
Greening	Lisa	University of Texas at Arlington
Haselkorn	Mark	Collaborative Systems for Safety, Security and Regional Resilience (CoSSaR), University of Washington
Heemskerk	Renske	Netherlands Embassy in the U.S.
Hu	Ben	Rice University
Islam	ABM Rezbaul	Sam Houston State University

Jaros	Stephanie	Applied Research Laboratory for Intelligence and Security (ARLIS), University of Maryland
Jia	Ruixue	University of California, San Diego
Kakadiaris	Ionnis	University of Houston
Keiser	Rebecca	NSF
Kidd	Ally	Naval Criminal Investigative Service
Koshy	Chetna	Rice University
Lampe	Steve	University of Kansas
Lewis	Margaret	Seton Hall University
Lewis	Steven	Rice University's Baker Institute for Public Policy
Lin	Ann	University of Michigan
Littlewood	Jacqueline	University of Alberta
Liu	Zhandong	Baylor College of Medicine
McGuirk	Shawn	Natural Sciences and Engineering Research Council of Canada (NSERC/CRSNG)
McMahon	Heather	ARLIS
McNeil	Robert	Texas Heart Institute
Moffatt	Gregory	Massachusetts Institute of Technology
Murdoch	Matthew	Office of Sen. Bryan Hughes
Natelson	Douglas	Rice University
Nichols	Lisa	University of Michigan
O'Shea	Patrick	University of Maryland
Peck	Karina	CSIRO
Pei	Steven	University of Houston
Pena	Jomyra	University of Texas at San Antonio
Phelps	Allen	IPTalons
Puglisi	Anna	Puglisi Ventures
Rajashekara	Kaushik	University of Houston
Ribes	David	University of Washington
Sa	Creso	University of Toronto
Salt	Karen	UK Research and Innovation
Sanders	Ashley	National Institutes of Health (NIH)
Schellhammer	Michael	Artemist Advisory Group
Sharman	Ben	UK Research and Innovation (UKRI)
Stalker-Lehoux	Sarah	NSF
Steele	Michael	NSF
Talerico	John	Virginia Tech
Thompson	Susan	Office of the Director of National Intelligence
Tiffert	Glenn	Hoover Institution, Stanford University
Toups	Krystal	Council on Government Relations
Trinh	Anh-Khoi	NSERC/CRSNG
Usami	Takeshi	National Research and Development, Japan Science and Technology Agency

van der Wende	Marijk	Utrecht University
Vandible	Pretta	Houston Community College
Vazquez	Tania	University of Texas at San Antonio
Vincenzo	Daniel	University of Texas at Arlington
Wagner	Caroline	The Ohio State University
Wang	Jingguo	University of Texas at Arlington
Woodruff	Kim	Rice University
Youngbull	Cody	Office of the Under Secretary of Defense for Intelligence & Security

Some participants who attended the workshops preferred not to have their names disclosed.

Appendix D: Detailed Breakdown of Research Clusters Across Different Perspectives

Institutional Leader

National Security

Research administration in the context of national security plays a critical role in balancing scientific advancement with protecting national interests. Visa and immigration policies significantly impact this balance by restricting the flow of international researchers, potentially hindering recruitment, collaboration, and innovation. The tension between national and economic security increases competition, creating an environment susceptible to improper influence and information exfiltration. Overly stringent measures can stifle economic growth by limiting the talent pool and slowing technological progress. Countries often attempt to influence and exfiltrate information from critical and strategic areas such as technology, military capabilities, and higher education, as evidenced in publications and citations.

While publications and citations are common metrics for measuring productivity and innovation, they may not fully capture the practical impact or commercialization of research. Alternative measures such as patent filings, R&D expenditure, and the successful application of technologies in industry may provide a more accurate reflection of true innovation and productivity. Therefore, research administration must continuously adapt to effectively support scientific progress while safeguarding national security interests.

Policy and Governance

Research administration within the context of policy and governance must navigate a complex landscape where restrictive policies, resource allocation, and policy enforcement significantly impact research efficacy. Excessive or overly complex regulations, while ensuring oversight, can also become barriers to entry, pushing researchers to seek funding from less stringent sources, potentially overseas. Tools such as streamlined compliance systems, clear communication channels, and supportive administrative frameworks can enhance policy effectiveness.

Policy effectiveness often hinges on balancing threat and persuasion — a lack of oversight, as well as overly punitive measures, can lead to resistance and non-compliance. Conversely, persuasive, incentivized policies can foster a more collaborative and productive environment. Policy must also consider institutional culture, addressing philosophical differences, such as the "It's not my job to comply; it's your job to enforce" mentality, by integrating compliance as a shared responsibility.

Effective policy management requires continuous updates and revisions to stay relevant and reduce the administrative burden that can deter emerging research institutes. Managing the movement of offenders between organizations and ensuring compliance across institutions further complicates this landscape, highlighting the need for robust, adaptable, and inclusive policy frameworks in research administration. This is essential for maintaining the U.S.' competitive edge in research and innovation.

Research Enterprise

Research administration in the U.S. research enterprise faces numerous challenges related to burden, cost-benefit measures, and compliance. The burden of compliance includes both direct financial costs and the opportunity costs associated with diverted resources and time. Loss and risk are calculated by assessing potential financial, reputational, and operational impacts, while opportunity costs are evaluated based on missed research opportunities and innovations due to regulatory constraints. Risk tolerance is determined by institutional policies and funding agency priorities, balancing potential gains against the risks of non-compliance.

The high cost of compliance and administrative burden can hinder research productivity and innovation. Ensuring a comprehensive understanding of compliance requirements and applying internal controls from an overarching research compliance perspective may be more practical than addressing every global threat individually. Balancing research security initiatives with collaborative activities requires a sophisticated blend of interests between innovative collaborations and stewardship emphasis.

Technological tools, such as automated compliance tracking systems, data management software, and verification mechanisms for reported information, can help reduce administrative burdens. The structure and design of research security must balance internal self-regulation with external oversight to be effective, ensuring accountability while fostering an environment conducive to research collaborations and innovation.

Domestic and International Collaboration

Research administration in the context of domestic and international collaboration must ensure that collaborations are transparent and reciprocal, promoting scientific advancement while managing associated risks. A successful collaboration is characterized by clear communication, shared goals, equitable contributions, and mutual respect for requirements. Key risk factors include intellectual property theft, data security breaches, and geopolitical tensions.

Co-publication rates are an important measure of collaboration success; however, concerns over national, economic, and research security have led to a noticeable decline in collaborations with China, Russia, and Iran. This decline may be attributed to factors such as malign talent program countermeasures, stringent regulations, potential accusations of espionage, and increased scrutiny, contributing to the perception of cultural profiling. These perceptions, along with compliance requirements that impact a researcher's sense of autonomy, can make it more challenging to attract and retain top talent.

Research funding and talent are increasingly flowing toward institutions and countries perceived as having a stable and supportive environment for research. Effective research administration must navigate these dynamics, fostering a balance between open scientific collaboration and the need for public trust and stewardship. This ensures that collaborations enhance innovation while mitigating risks.

Government Official

National Security

Funding agencies as part of the U.S. executive branch have the responsibility to ensure proper oversight to balance the benefits of open collaboration and protecting national and economic security that contributes to U.S. research and innovation. Countries such as the U.S., China, EU nations, and other global powers all balance both collaboration and competition. The cost of reactive versus proactive initiatives in this balance is a significant consideration: Proactive measures may be costly upfront but can prevent larger issues, whereas reactive responses often lead to hurried, sometimes overreaching policies that can stifle innovation and international cooperation. This balancing act is seen as a bipartisan issue in the U.S., with both political perspectives recognizing the need for security while also fostering economic growth. Scrutinizing company ownership regarding foreign and Chinese investments in U.S. and EU firms helps to ensure critical industries and technologies are secure. Policies must avoid overreaction, which can lead to unnecessary barriers and underreaction, which can leave vulnerabilities.

Policy and Governance

Evaluating funding against project risk levels requires the careful application of policy and governance. The politicization of policy recommendations can undermine objectivity, effective governance, and equity in regulatory responses to non-compliance. Research funding organizations expect compliance with requirements, while researchers and funded organizations should rely on consistently applied and fair consequences based on established standards, ensuring due process. Adequate funding for compliance efforts is essential to promote adherence and avoid disproportionately burdening smaller institutions. Overly stringent research security policies may hinder innovation and competitiveness if they are too restrictive in the long term.

Understanding different compliance attitudes in policy development can foster a sense of shared responsibility. Well-defined policies prevent confusion, such as the apparent contradiction between requiring information protection and mandating public access. States may exhibit varying policy applications and attitudes, reflecting broader political divides. Oversight failures often result from inadequate policy or enforcement rather than intentional actions. The level of detail in defining rules should be a collaborative effort between agencies and the funded community, ensuring practicality and relevance. Comparing agency policies and enforcement mechanisms reveals the need to harmonize rather than merely standardize actions, promoting fair and consistent application. Agencies must make requirement decisions transparently and equitably. Compliance should align with the Administrative Procedure Act (APA) and include clearly understood definitions to ensure fairness and clarity. For example, "case" typically involves a specific instance of non-compliance or misconduct, while an "investigation" is the process of examining such instances to determine facts and appropriate actions.

Research Enterprise

Deciding on how and at what level to apply compliance requirements, agencies often focus on award value rather than the critical and sensitive nature of the projects. Training should aim to enhance understanding of compliance and security issues without being politicized, emphasizing practical knowledge and best practices. Comparing requirements internationally can reveal best practices and assess their effectiveness. Measuring the level of bureaucratic burdens can provide valuable lessons. Effective training should be ongoing, targeted at different levels of research personnel, and emphasize the importance of security and compliance in a non-political manner. The research enterprise should highlight the shared responsibility of safeguarding research integrity. The cost-benefit analysis of new requirements must weigh the additional administrative load against the protection of intellectual property, resources, and reputation. Ensuring the security of the peer review process is crucial, with measures in place to protect submissions through confidentiality agreements and secure handling protocols, thereby ensuring researchers' work is not compromised.

Domestic and International Collaboration

Balancing the restriction and enabling of domestic and international collaborations is crucial for maintaining a productive research portfolio. Such collaborations can drive significant advancements, often yielding benefits that outweigh associated risks. Funding agencies and research organizations must assess these collaborations carefully, funding them when the potential for innovation and scientific progress justifies the cost and effort of protective measures. If the government strictly enforces regulations without collaboration with the funded community, researchers may face more significant challenges, leading to shifts in funding sources. For instance, stringent security concerns in the U.S. might push faculty toward noncompliance or seeking funding from less restrictive international sources. Robust compliance accountability, risk assessment, and mitigation strategies can enable beneficial collaborations without compromising security. Monitoring how funding patterns shift in response to these policies can inform better governance, ensuring that the U.S. research enterprise remains competitive and secure.

Research Administrator

National Security

Research security prioritizes the protection of critical infrastructure, defense technologies, advanced materials, biotechnologies, and pre-applied fundamental research topics. Collaborations involving sensitive information and assets should be carefully monitored to mitigate risks. Examining high-risk cases that successfully avoided information leaks can provide crucial insights into effective security practices.

The data life cycle necessitates protection protocols to identify precise points of vulnerability and determine appropriate durations for safeguarding sensitive information. A key research security question is, "When does information become 'sensitive' and require protection"? Artificial intelligence (AI) plays a dual role in research security: enhancing capabilities for threat detection and data protection while also presenting new challenges and vulnerabilities.

The assertion that the U.S. has experienced significant intellectual property (IP) theft, particularly by Chinese actors, prompts a critical examination of this issue. It is important to assess whether this reflects reality and to measure the size and scope of the problem. Additionally, it is essential to determine if such theft represents failures in U.S. policy or the success of sophisticated exfiltration efforts by adversaries.

Ensuring the security and protection of U.S. patents requires robust legal and technological measures. Collaborative research on patent policy, comparing practices across countries, can yield valuable insights. The private sector, often at the forefront of innovation in security protocols, offers lessons and comparative models that can enhance public sector strategies.

Policy and Governance

Universities and research institutions must adopt effective practices that safeguard sensitive data and technologies while facilitating collaboration and knowledge sharing. Comparisons with the corporate and private sectors highlight differing approaches to security, offering valuable lessons on what works and what doesn't. Current challenges in research security include gaps in effectively implementing existing laws and insufficient measures to protect data and information from unauthorized access or theft.

Effective protection measures include encryption, access controls, secure data storage, and regular audits to ensure compliance with security protocols. However, there is a concern that overly stringent measures may slow down the application for and management of awards, impeding legitimate research activities rather than solely targeting malicious actors.

The process for reporting security breaches or concerns, including self-reporting and whistleblower mechanisms like qui tam — where individuals who assist with prosecutions are compensated with recovered damages —aims to encourage transparency and accountability. The effectiveness of treble damages under whistleblower rules incentivizes reporting but can be challenging to enforce without clear evidence of effectiveness. Balancing robust security measures with the need for efficient research administration is crucial to maintaining a productive and secure research environment.

Research Enterprise

Enhancing research security in the research enterprise involves continuous improvement and evaluation through internal reviews and robust methodologies — what gets checked gets done. AI holds promise for integrating into risk remediation by enabling rapid analysis of data to detect potential threats. However, addressing false positives, where normal activities are incorrectly identified as suspicious, is crucial to prevent distrust, unnecessary disruptions, and inefficient resource allocation.

Understanding the frequency and scale of IP or data losses and identifying perpetrators requires a thorough assessment of the scope and impact. Historically, universities have faced challenges with limited control over employee actions, and improved deterrence measures need to be measured for effectiveness. Evaluating the effectiveness of recent versus older case examples can provide insights into past security incidents and inform future strategies. Ensuring that research members possess adequate knowledge of information security concepts may promote common best practices. Additionally, addressing concerns and measuring racial components in enforcement is critical to ensure fair and equitable treatment within the research community.

Domestic and International Collaboration

Research security must address risks associated with "adversary" nations, particularly those perceived as potential threats to intellectual property and national security. Promoting domestic and international collaborations is essential to successful research portfolios. A secure collaboration involves rigorous frameworks for evaluating partners, ensuring shared values, transparency, and adherence to legal and ethical standards. The scope and scale of security risks, often dominated by concerns about China, vary across different sectors and research domains. While collaboration on global challenges such as climate change and food security is encouraged, sensitive areas involving high technology often require cautious approaches and safeguards to protect innovations and data. Balancing cooperation and security involve safeguarding national interests without compromising the benefits of international collaboration. Effective research security strategies involve proactive risk assessments, clear communication of expectations, and robust enforcement mechanisms to maintain trust and integrity in collaborative research efforts.

Researcher

National Security

STEM, behavioral, and social science research intersect with national security concerns between foreign countries and collaborators. The impact of restrictions on foreign collaborations varies significantly across disciplines, with STEM fields often facing more stringent scrutiny due to their direct implications for technological advancement and defense capabilities. Historical actions in response to foreign concerns, such as espionage allegations or intellectual property theft, have often failed to consider behavioral or psychosocial perspectives. This sometimes leads to accusations of disloyalty or asset theft, which can provoke intense scrutiny and affect organizational trust and research collaborations, particularly in sensitive areas or when strategic knowledge is involved.

Policy and Governance

Policy and governance should incorporate toolsets ensuring reciprocity and transparency. These tools include robust data management systems, clear communication channels, and agreements that facilitate equitable collaboration while safeguarding organizational and national interests. Researchers often do not view themselves as solely responsible for U.S. economic and innovation prominence, highlighting the divergent perspectives between academic pursuits and governmental policy objectives. Government policy decisions in research are driven by national, economic, and research security concerns over economic competitiveness and societal impact. Divergent perspectives influence funding agency policies crafted through legislative processes and enforced through regulatory frameworks and should be subject to appeal mechanisms.

Different perspectives are essential for evaluating the effectiveness of governance and policy, particularly regarding information sensitivity, classification, and the introduction of controls in traditionally open research areas. The shift toward more controlled research environments raises questions about the future of open collaborations and necessitates clear classification schemes to manage data access and dissemination appropriately.

Examining these issues through actuarial science could provide quantitative insights into risk management and policy effectiveness across scientific disciplines, offering benefits such as data-driven decision-making but also potentially constricting creativity and collaboration depending on risk appetite.

Research Enterprise

The U.S. research enterprise reveals a complex interplay of factors influencing compliance and collaboration across STEM, behavioral, and social science disciplines. Stringent security measures can create a chilling effect, deterring the cross-disciplinary collaborations essential for innovation. Researchers may face concerns about their career trajectories, as heightened compliance requirements can stifle creativity and slow progress. The psycho-social impact of these policies includes increased stress and decreased job satisfaction, particularly if compliance is perceived as a punitive "gotcha" mechanism rather than a reasoned necessity. Empirical assessments of past grants and research can identify patterns and issues in compliance, informing better practices. Cultural variations play a significant role in compliance attitudes; Western approaches may emphasize individual responsibility, while Eastern cultures might stress collective compliance, and other cultures may present unique blends of these attitudes. Researchers' motivations for compliance may oscillate between fear of punishment, rationalizing necessity, and the desire to be respected team members. Effective policy measures should align incentives and ensure organizational justice and fairness in grant applications and awards. Assessing campus climate before and after policy implementation provides valuable insights into trust levels and job satisfaction, which are critical indicators of a healthy research environment.

Domestic and International Collaboration

Assessing STEM, behavioral, and social science research within the context of domestic and international collaborations reveals significant benefits and inherent risks. Domestic and international collaborations facilitate the exchange of knowledge, enhance innovation, and address global challenges more effectively. However, these collaborations also may pose risks, including the potential exfiltration of sensitive information, which some argue is an unavoidable cost of international cooperation. Despite this, the long-term benefits of collaborations, such as fostering mutual understanding and global benefits from discoveries, often outweigh these risks. The balance between collectivist and individualist mentalities is crucial; collectivist approaches may promote stronger collaborative ties and shared goals, while individualist perspectives can drive personal accountability and innovation. Historical lessons, such as those from Japan's post-war recovery, provide historical examples for avoiding past mistakes and managing reactions to "foreign" threats on a conduct rather than a cultural basis. There are many incentives for participating in foreign affiliations that may pose a risk to accountable collaborations, including family pressures, elicitation efforts, and talent program prestige monetary benefits. Understanding talent growth and importation patterns is essential for sustaining a vibrant research community. Regularly gauging whether researchers feel safe in their collaborations can inform policies that enhance security while maintaining the openness necessary for scientific progress.

RICE UNIVERSITY'S
Baker Institute
for Public Policy