Research Program on Research Security

Contact: Gordon Long — glong@mitre.org

JSR-22-08

March 2023

JASON
The MITRE Corporation
7515 Colshire Drive
McLean, Virginia 22102-7508
(703) 983-6997

Contents

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
March 2023	Technical	

4. TITLE AND SUBTITLE

Research Program on Research Security

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

5d. PROJECT NUMBER
100775.10.111.JAPM

5e. TASK NUMBER
IN0

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

The MITRE Corporation
JASON Program Office
7515 Colshire Drive
McLean, Virginia 22102

8. PERFORMING ORGANIZATION REPORT NUMBER

JSR-22-08

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

National Science Foundation
Research Security Strategy and Policy
2415 Eisenhower Avenue
Alexandria, Virginia 22314

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Distribution A. Approved for public release. Distribution is unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

NSF is considering creating a research program on research security. NSF asked JASON to consider what a research program on research security might entail, how it would be defined, and which areas of study are ripe for advances that might have the most immediate impact on the way NSF, and possibly more broadly, the federal government, considers research security.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	b. ABSTRACT	c. THIS PAGE			Rebecca Keiser, PhD
					19b. TELEPHONE NUMBER *(include area code)* 703-292-4901

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

1 EXECUTIVE SUMMARY

The National Science Foundation (NSF) is at the forefront of US government agencies supporting fundamental research. It has also been a center of activity on the security of federally-funded fundamental research, creating a new position of Chief of Research Security Strategy and Policy. Research security has become a much-used term over the past few years, and it has become apparent that research security is not a commonly understood concept in the fundamental research community. Indeed, many of the US and international attempts to define the nature of the problem do not clearly distinguish between research security and research integrity. Thus, NSF needs to understand the aspects of "research security" that are distinct from "research integrity" as well as how the concepts overlap and how they depend on scientific discipline. This understanding will assist NSF, its federal partners, and the research community to assess in an evidence-based manner which, if any, controls are needed to secure research from undue foreign influence. Also, there is a lack of data on the frequency of research security issues, and federal agencies continue to depend on references to individual cases or potentially biased measures.

In light of these needs, NSF is considering creating a research program on research security. NSF asked JASON to consider what a research program on research security might entail, how it would be defined, and which areas of study are ripe for advances that might have the most immediate impact on the way NSF, and possibly more broadly, the federal government, considers research security.

JASON was asked to address the following questions:

1. Based on current understanding, how can "research security" be distinguished from "research integrity"? What is required to sharpen this distinction?

2. How much does the definition of research security depend on discipline? For example, would the working definition differ in synthetic biology, quantum information science, and advanced wireless communication, and does that impact the approach to both protection and research?

3. What central research themes or questions should be addressed? Which themes or questions are most urgent, given the current security threats to the US research environment?

4. What are the critical research communities that must be engaged for research on research security to be successful?

5. What data will be required for research on research security? What privacy controls will be required?

In responding to these questions, JASON engaged with NSF leadership, law enforcement, members of the academic community, and professional societies. This report details the results from the ensuing inquiry and discussions.

The body of the report considers in depth the answer to each of the questions posed. Below is a summary of those responses.

1. JASON developed the following definitions of research security and research integrity, simplifying and sharpening the distinction relative to other efforts:
   Research Integrity is adherence to accepted values and principles — objectivity, honesty, openness, accountability, fairness, and stewardship — that guide the conduct of research and recognize the expectations of funding agencies, research institutions, and the research community.
   Research Security is protecting the means, know-how, and products of research until they are ready to be shared, by approval of the leader(s) of the research program and other stakeholders in their security.

2. Research security by the JASON definition does not vary across disciplines. However, the consequences of breaches in research security and the measures to be taken to prevent breaches will differ across disciplines. For example, by some measures, much of the basic operational technology of synthetic biology is already highly democratized, whereas the operational technology in quantum information science is less so and is more difficult to create. However, there are many complexities to these considerations, and these are considered more fully in the report.

3. JASON has provided a set of illustrative topical areas for a possible NSF program solicitation. These include working case studies of research security breaches, developing and accessing effective education and training strategies, conducting controlled experiments involving risk assessment, and performing a comparative analysis of policies of US research institutions and identifying best practices.

4. The social sciences will be important for a successful research program and JASON strongly encourages collaborative efforts of social scientists and researchers in the natural sciences. We suggest embedding social scientists as visitors within research laboratories to strengthen the understanding of the customs and operations of open science. STEM fields will also be important, including computer science and disciplinary experts in natural sciences and engineering. Additionally, professional societies will be important partners for researchers in this program, for disseminating findings and enacting recommendations.

5. Data from NSF and other funding agencies, law enforcement, universities, and private companies on the numbers of breaches of research security and their consequences will be essential. Some of this information is held as confidential. NSF should be prepared to support acquisition and anonymization of data for research projects pertaining to research security. This is particularly challenging for data held by universities, which often have human resources policies that protect such data. To protect the personal information of subjects in research projects, one must carefully anonymize collected data.

In addition to the specific responses to these questions, JASON offers the following findings and recommendations.

Findings

1. The issue of research security is real. The fruits of US STEM research and their benefits to US interests across many arenas have been challenged by inappropriate practices in the international arena.

2. US researchers often feel threatened, frightened, and/or burdened by past and current actions

to deal with problems of research security and integrity. Survey data indicate that these concerns are widespread and deep.

3. The consequences and appropriate actions related to breaches of research security differ among STEM fields.

4. The definition of research integrity differs across national interests and cultures.

5. The NSF internal project on the identification of potential breaches of research integrity and security through analysis of open-source data could lead to a useful product for dissemination to other federal, academic, and commercial organizations.

6. STEM Principal Investigators best understand the customs and practices of their discipline, and they can be important partners in a research program on research security. They should have the ability to decide when the products of research are ready for publication and public dissemination.

7. The success of an NSF program on research security will depend on NSF working with universities and private companies to make available their data on issues of research security in a protected manner that allows access to approved research programs on this topic and provides protection of the privacy of the sources.

Recommendations

1. The products of a research program on research security must not be used to disadvantage anyone based on their ethnic background or country of origin. Every effort should be taken to keep the US as the premier destination for top scholars around the world, working in an open science environment, and we must avoid creating a reputation of racial profiling or injustice.

2. In a research program on research security, NSF and proposers must consider the ability to access confidential data at universities and private companies. NSF should assist Principal Investigators with data access and in the use of methods for anonymization of data.

3. The NSF program should emphasize research on effective methods for informing and training Principal Investigators about potential risks in international collaborations by country and, where appropriate, by institution.

4. The NSF research program should encourage research projects in collaboration with international organizations that share our concerns for research security.

5. As part of the proposed research program, NSF should encourage collaborations between social scientists and other STEM researchers, for example, via cross-disciplinary workshops before and during research performance.

6. The NSF should work closely with US STEM professional societies to maximize access of research program awardees to STEM researchers and to disseminate educational and training materials.

7. NSF should work with other Federal agencies (e.g., NIH, DOE, NASA) that have a major stake in unclassified basic and applied research to create a protected database of matters of breaches of research security at universities, private companies, and government laboratories, which can be accessed by approved researchers in the NSF research program on research security while maintaining the privacy of the sources. The larger size of a database with information from other Federal agencies included will make statistical analysis more robust and can aid in the implementation of anonymization methods such as differential privacy.

JASON concludes that an NSF research program on research security would be useful in addressing many of the concerns about foreign influence and the security of the US fundamental research ecosystem. There are many topics that could be the subject of such a research program and most of these will benefit from strong engagement with social scientists, and collaboration of those social scientists with practicing natural scientists in the fields of interest. Access to data will be a serious challenge to the success of a research program, but one that likely can be mitigated by application of appropriate anonymization methods.

This Page Intentionally Left Blank

2 INTRODUCTION

The experience during WWII with the value of science, primarily in the arena of military technology, was summarized by Vannevar Bush (Bush July 1945) in a report to President Truman as the war was nearing its end. Bush outlined a broad value of science to the nation and anticipated a significant return on investment in natural science, technology, engineering, and mathematics (STEM) to the quality of life in the United States.

This document led to the establishment of the Office of Naval Research in 1946 and other Department of Defense agencies supporting both military and civilian-focused research. The National Science Foundation (NSF) was established by Congress in 1950 as fundamental research funding agency supporting programs in a growing number of public and private university-based basic and applied research programs. The National Institutes of Health, focused on fundamental and applied biomedical research, grew out of the Public Health Service.

Also following WWII, the work at the Los Alamos laboratory eventually grew into the US Department of Energy, with significant basic and applied research programs across STEM fields. Many other Federal departments established their own, typically mission-oriented, research programs complementing those of NSF both before and since WWII. The private sector created a parallel set of research laboratories, often in collaboration with the efforts of these Federal agencies.

The research ethic of unclassified research in these laboratories — academic, governmental, and private sector — was to support the open publication of results, transparent presentation of experimental data, broad discussion of theoretical work, and strong collaboration with international programs as they grew in parallel with US efforts. The latter included exchanges of university students at the undergraduate and graduate level, and exchanges of postdoctoral scholars and faculty in STEM and other fields of scholarship.

The success of this international cooperation rested on an agreed upon view of the integrity of the researchers, on the tenets of respect for research results, open publication of these results when those directing the research programs deemed appropriate, and mutual respect for cooperation and fair competition.

It became clear a decade or more ago that not all governments and cultures throughout the world adhered to this same view of the scientific enterprise. Much of the concern has focused on the actions of the Chinese government, which, through “talent programs,” “Confucius Institutes,” and unethical reporting requirements of international students supported via Chinese military and intelligence agencies, poses a growing challenge to the fundamental assumptions of the working mores of international scientific cooperation.

In 2019 NSF sponsored a JASON study (JSR-19-21 2019), “*Fundamental Research Security*.“ Since publication of that report and other contemporaneous reports, there has been substantial US government and international activity addressing “research security”; see, for example (G7 Common Values and Principles on Research Security and Research Integrity 2022).

At the highest level, in January, 2021, the US government issued National Security Presidential Memorandum (NSPM-33) (Presidential Memorandum on United States Government-Supported Research and Development National Security Policy January 14, 2021), the goal of which was to “strengthen protections of United States Government-supported R&D against foreign government interference and exploitation” while “maintaining an open environment to foster research discoveries and innovation that benefit our nation and the world.”

On August 21, 2021, the White House Office of Science and Technology Policy tasked the National Science and Technology Council (NSTC) with developing “clear and effective implementation guidance” for NSPM-33. This resulted in a document (Guidance for Implementing National Security Presidential Memorandum 33 (NSPM-33) on National Security Strategy for United States Government-Supported Research and Development, January 2022) meant to aid federal funding agencies in balancing their responses across agencies. It also notes that “the research community will be equally engaged in understanding and complying with the implementations of this guidance.”

The NSPM-33 guidance has many specifics for action. The first principle of general guidance in NSPM-33 states: “Agencies should continue to support open and transparent scientific inquiry.”

Among the other requirements in the NSPM-33 guidance document are these:

- "Research funding agencies shall require the disclosure of information related to potential conflicts of interest and commitment from participants in the Federally funded R&D enterprise."

- "Research Security Programs: Section 4(g) of NSPM-33 directs that by January 14, 2022, 'heads of funding agencies shall require that research institutions receiving Federal science and engineering support in excess of 50 million dollars per year certify to the funding agency that the institution has established and operates a research security program. Institutional research security programs should include elements of cyber security, foreign travel security, insider threat awareness and identification, and, as appropriate, export control training. Heads of funding agencies shall consider whether additional research security program requirements are appropriate for institutions receiving Federal funding for R&D in critical and emerging technology areas with implications for United States national and economic security.'"

The first of these is a common requirement for all faculty and key research personnel of many, if not all, US research institutions, while the second impacts about 130 US research organizations according to information provided for 2016 and 2017 to JASON by the NSF. This means that compliance via a "research security program" is required of a relatively small number of US research institutions receiving substantial federal STEM funding.

The response of federal research funding agencies has been similar to the example of DARPA in its June 15, 2022 Broad Agency Announcement in Section II B Fundamental Research (HR001122S0041 DSO OFFICE-WIDE BAA June 15, 2022), where it states "The University or non-profit research institution performer or recipient must establish and maintain an internal process or procedure to address foreign talent programs, conflicts of commitment, conflicts of interest, and research integrity." The BAA requires that such information "will be provided to the Government as part of the proposal response to the solicitation and will be reviewed and assessed prior to award. Generally, this information will be included in the Research and Related Senior/Key Personnel Profile (Expanded) form (SF-424) required as part of the proposer's submission through Grants.gov." SF-424 is essentially a conflict of interest and conflict of commitment form that can be found at Grants.gov.

At another scale of involvement in developing guidance for the implementation of NSPM-33, and consistent with its mission to support fundamental research, the NSF has proposed establishing a Research Program in Research Security to examine, through the work of those receiving grants through the program, a set of fundamental research questions in the area of research security. The products of these research efforts should be the evidential foundation for further implementation of the guidance suggestions for NSPM-33.

A cautionary note is that there are some in the US fundamental research community who view "research security" as a setting for a racist policy toward certain ethnic groups in US society. For example, the December 2021 membership poll conducted by the American Physical Society (APS 2021) revealed that there are strongly held views that the current focus on research security is without an evidential basis and has been a mechanism to pursue a racist policy against Chinese and Chinese-American scientists.

In JASON's assessment, there is a real issue of research security, expressed well in NSPM-33 and in several of the international documents promulgated since 2019 (G7 Common Values and Principles on Research Security and Research Integrity 2022). The proposed NSF research program on research security presents an opportunity to understand the risks quantitatively, establish an educational and training effort bringing this information to the US and world research communities, and serve the essential goals of an open international scientific collaboration atmosphere.

NSF has asked JASON to assist them in formulating a research program that delineates the scope of this problem and whose results are expected to provide insights into possible responses to these external challenges while maintaining open international cooperation in STEM fields.

Specifically, NSF asked JASON to address the following questions that would assist the Foundation in preparing an NSF Program Solicitation:

1. Based on current understanding, how can "research security" be distinguished from "research integrity?" What is required to sharpen this distinction?

2. How much does the definition of research security depend on discipline? For example, would the working definition differ in synthetic biology, quantum information science, and

3. advanced wireless communication, and does that impact the approach to both protection and research?

4. What central research themes or questions should be addressed? Which themes or questions are most urgent, given the current security threats to the US research environment?

5. What are the critical research communities that must be engaged for research on “research security” to be successful?

6. What data will be required for research on “research security?” What privacy controls will be required?

Addressing these questions individually forms the core of this report. JASON’s conclusions in the form of answers to these questions, along with other information, briefly condensed into a set of **Findings** and **Recommendations** can be found in both the Executive Summary of the report and at the end of the report.

This Page Left Blank Intentionally

3 DISTINCTION BETWEEN RESEARCH INTEGRITY AND RESEARCH SECURITY

JASON was asked by NSF: Based on current understanding, how can “research security” be distinguished from “research integrity?” What is required to sharpen this distinction?”

The concepts of research integrity and research security are intertwined, often in ways that obscure useful and important distinctions. Here we present two recent examples of other attempts at definitions being considered in the public arena and derive simplified definitions of these two concepts.

The first are definitions that are closely based on those in the NSTC (National Science and Technology Council) guide for implementation of NSPM-33. These were presented to JASON in a briefing slide in June 2022 by Dr. Rebecca S. Keiser of the NSF:

> Research integrity is adherence to professional values and principles — including objectivity, honesty, transparency, fairness, accountability, and stewardship — in proposing, performing, evaluating, and reporting research and development activities.
>
> Research security is safeguarding the research enterprise against behaviors aimed at misappropriating research and development to the detriment of national or economic security, related violations of research integrity, and foreign government interference.

Second, in the G7 document Working Group on Research Integrity and Security (G7 Common Values and Principles on Research Security and Research Integrity 2022) we find another definition for these two concepts:

> Research integrity is the adherence to the professional values, principles, and best practices that underpin our research communities. It forms the base on which to collaborate in a fair, innovative, open, and trusted research environment.
>
> Research security involves the actions that protect our research communities from actors and

> behaviors that pose economic, strategic, and/or national and international security risks. Particularly relevant are the risks of undue influence, interference, or misappropriation of research; the outright theft of ideas, research outcomes, and intellectual property by states, militaries, and their proxies, as well as by non-state actors and organized criminal activity.

The first of these is important to consider as it reflects the US government outlook in a document meant to guide federal agencies on how to consider both research integrity and research security. The second, from the G7 document, is significant as it reflects the views of the members of the G7 (Italy, Japan, Germany, UK, US, Canada and France) which have taken a leadership role in the international arena in thinking through how to respond to actions by several countries that they perceive to pose a threat to research security**.**

After considering these perspectives and others, JASON concluded that it would be useful to derive simpler definitions that more clearly distinguish the two concepts. Our proposal for these definitions is this:

> Research integrity is adherence to accepted values and principles — objectivity, honesty, openness, accountability, fairness, and stewardship — that guide the conduct of research and recognize the expectations of funding agencies, research institutions, and the research community.
>
> Research security is protecting the means, know-how, and products of research until they are ready to be shared, by approval of the leader(s) of the research program and other stakeholders in their security.

JASON's definition of research integrity emphasizes the values and principles that the US and other G7 countries have expressed. The six listed in the definition are from the 2017 report "Fostering Integrity in Research" by the National Academies of Sciences, Engineering, and Medicine (https://nap.nationalacademies.org/catalog/21896/fostering-integrity-in-research) and previous work that is cited in that report. The report summarizes these values as follows:

> "The first of the six values discussed in this report — objectivity — describes the attitude of impartiality with which researchers should strive to approach their work. The next four values — honesty, openness, accountability, and fairness — describe relationships among those involved in the research enterprise. The final value — stewardship — involves the relationship between members of the research enterprise, the enterprise as a whole, and the broader society within which the enterprise is situated. Although we discuss stewardship last, it is an essential value that perpetuates the other values."

These are broadly shared perspectives in many countries with which the US has longstanding international research collaborations. However, it has become clear, as identified in NSPM-33, that this shared concept is not universally agreed upon. Different countries and cultures may have different views on what are regarded as ethical standards in research, possibly leading to different views on "research integrity" and a different position on what constitutes a breach of research security.

It is also worth noting that the values listed under research integrity, as described in the 2017 report, are expressed with words that are quite general and open to interpretation. They do not explicitly mention some of the common values that have been brought to the forefront since 2017. For example, the value of ensuring that research is diverse, equitable, and inclusive, or the value of promoting public trust in the face of growing disinformation. These more specifically stated values are likely to resonate more with researchers than the general values of fairness and accountability, respectively.

In JASON's definition of research security the "leader(s) of the research program" are seen to be in control of the products of their research and have the primary role in determining what is to be released for publication and public dissemination in other media and when. This is often the principal investigator (PI) of the research project, an official designation within institutions that indicates a person responsible for the preparation, conduct, and administration of a research grant or other project.

While JASON identifies the PI as responsible for judgments on the release of research products, we recognize that there may be many stakeholders in the security of the research, and these stakeholders have shared responsibility for such decisions related to various parts of the work. This is particularly

evident in large science and technology projects sponsored by federal support at universities, which have offices of research administration and technology transfer. It is essential that there be effective education and training on research security among all of these stakeholders — some of whom are likely already well-versed in the matter — and with all of the working members of research teams. How best to formulate this education and training for collaborations, domestic and international, is one of the suggested research topics for the NSF research program on research security. It is of great importance that all members of the research units in collaborations remain well informed about the lines of responsibility associated with the PI, associated with the PI's designated key personnel, and associated with individuals at each level of the research project.

In the JASON definition of research security, we sought to make clear that the information relevant to research projects includes the means and know-how of research and not just the final products of research. In addition to traditional publications, the dissemination of this information might occur in webpages, social media postings, preprints on ArXiv, bioRxiv, or the equivalent, release to the popular press, or release to others outside the research group. This definition implicitly notes that the customs and framework for release of research information are known to the PI working in the discipline in which the work is done, accounting for differences among disciplines. Interdisciplinary work will inherently require closer attention to such differences.

4 DISCIPLINE-SPECIFIC CONSIDERATIONS

JASON was asked by NSF: How much does the definition of research security depend on discipline? For example, would the working definition differ in synthetic biology, quantum information science, and advanced wireless communication, and does that impact the approach to both protection and research?

Discipline-specific considerations are an important issue given the broad portfolio of research supported by NSF, the increased focus on research areas perceived as being relevant to economic and national security, and whether new access restrictions, such as controlled unclassified information (CUI) categories, should be invoked. We note that the JASON version of a definition of research security, in contrast to the others, purposely left out mention of economic security or national security in the interest of a discipline-agnostic definition that focuses on what should be secured and who is responsible for approving release of information.

Would the working definition of research security and approaches differ across fields? JASON was given synthetic biology, quantum information science, and advanced wireless communication as example fields to consider. These are all important areas of research that have been at the forefront of discussions about national and economic security. We concluded that the discipline-agnostic definition we have provided is applicable to all of these fields, but that the consequences of breaches in research security and the measures to be taken to prevent breaches, will differ across disciplines. As an example of how differences between fields can impact research security considerations, we consider two of these fields, synthetic biology and quantum information science, in more depth.

Synthetic biology

Synthetic biology is a field of research that seeks to address societal needs by engineering organisms or components of organisms to have new abilities. Genetic engineering is a foundational technology of synthetic biology, but the full set of tools applied come from many disciplines, including material science, chemical engineering, computer science, and evolutionary biology.

Although the goals and desired endpoints are often sophisticated, much of the enabling technology of synthetic biology is highly democratized and accessible. That is, the tools used to precisely manipulate DNA, insert that DNA into an organism, and to assess the change in phenotype that results from the manipulation are published in the open literature, available to laboratories with modest research budgets and personnel with limited training, and updated constantly in something of an open-source environment. Indeed, the international iGEM competition pits teams of high school and college students against each other in developing new synthetic biology outcomes from universal building blocks, with 3,600 teams and 70,000 participants this year (https://igem.org). Some of the technological landmarks in synthetic biology include constructing synthetic biological circuits, creation of a synthetic bacterial genome, the development of the bacterial CRISPR/Cas system for genome editing, and the creation of a range of biosensors.

Synthetic biology has tremendous economic potential, recognized in the September 2022 Executive Order on "Advancing Biotechnology and Biomanufacturing Innovation for a Sustainable, Safe, and Secure American Bioeconomy." (https://www.whitehouse.gov/briefing-room/presidential-actions/2022/09/12/executive-order-on-advancing-biotechnology-and-biomanufacturing-innovation-for-a-sustainable-safe-and-secure-american-bioeconomy/). The challenges in going from lab-scale efforts to significant components of the bioeconomy are often in integration of components and scaling up to relevant production scales. These efforts typically take place in industry settings rather than university labs. Given this, the fundamental research security risks in synthetic biology are centered more on biological data and intellectual property than on means and know-how.

Quantum information science

Quantum information science (QIS) is a field of research that aims to understand the analysis, processing, and transmission of information using the principles of quantum mechanics. Part of the appeal of QIS is the possibility that new types of computing and information processing based on quantum effects could overcome the physical constraints that limit the growth of computing power. As described by the Department of Energy Office of Science (https://www.energy.gov/science/initiatives/quantum-information-science), which is investing heavily in QIS, there are four areas that show the most promise:

1) Quantum computing. Has the potential to solve some problems much more effectively than classical computers, such as the factoring of large numbers and simulating physical quantum behavior of natural systems.

2) Quantum communication. Has the potential for more secure means of encryption.

3) Quantum sensing. Could lead to improved sensors, based on quantum effects, that would have much greater sensitivity for many applications in the natural sciences.

4) Quantum foundational science. Entails fundamental theoretical and experimental research to provide a framework for applications in computing, communication, and sensing.

In contrast to synthetic biology, the enabling technology of QIS is expensive and requires specialized training. Many experiments require ultracold temperatures — in the range of 10–20 millikelvin — to reduce noise and increase fidelity through control over errors. These conditions are achieved with dilution refrigerators, which cost ~$500,000 for academic lab-scale experiments, and can be scaled to larger sizes, at greater expense (see Project Goldeneye at IBM (https://research.ibm.com/blog/goldeneye-cryogenic-concept-system). The fundamental unit of quantum computing, the qubit, which can exist in intermediate states as opposed to the 0 or 1 of traditional bits, can have many possible physical implementations, including polarization of a photon, the spin state of an electron, or the energy level of an ion. Achieving the required entanglement of qubits for quantum computing is experimentally very challenging, requiring isolation from the environment while retaining the ability to be manipulated. Currently, even the largest quantum computers have very limited capability and commercial uses are only just beginning.

Clearly, these two areas of active research are very different, with synthetic biology using commonly accessible tools to create a diverse array of capabilities, limited by creativity, understanding of the system, and, if desired, the ability to scale up, whereas QIS is using expensive equipment and specialized know-how to progress toward common goals. Based on these differences, the consequences of breaches of research security differ. For example, an idea in synthetic biology, if released prior to execution could likely easily be reproduced elsewhere, because the know-how and capabilities are widespread, with the caveat that scale-up to achieve economic impact is difficult. This situation is also the basis for the extraordinarily rapid worldwide spread of new technologies,

such as CRISPR/Cas9, amongst researchers in the life sciences. In contrast, an idea in QIS is likely to be actionable by only a few university and industry groups as well as US government laboratories in the US or elsewhere because of the large investment required to implement it. Similarly, export controls, for example, on dilution refrigerators, would potentially slow progress of competitors in QIS, whereas they would have little effect on pre-scale-up synthetic biology because most of the hardware is already in common use in biomedical labs worldwide.

5 ILLUSTRATIVE RESEARCH TOPICS

JASON was asked by NSF: What central research themes or questions should be addressed in the research program on research security? Which themes or questions are most urgent, given the current security threats to the US research environment?”

We have organized our selection of illustrative research topics for an NSF research program on research security into four groups that could appear within the format for an NSF Program Solicitation. In such a solicitation, there is often a guide to potential proposers to give information on the scope of the solicitation. Potential proposers are asked to view the topics as not exclusive or imperative, but only illustrative, and the ideas of all proposers are welcomed.

Data Collection and Analysis. One of the key challenges in assessing research security risk has been the lack of relevant data. This was noted in our 2019 JASON report (JSR-19-21 2019) and remains an important problem to be addressed. Establishing the scale and scope of the research security problem should be an essential ingredient in an NSF program for research on research security. Given the roles of each of the key stakeholders of the relevant data, it is perhaps understandable that the research community has not been presented with a full picture of the scale and scope of the problem. FBI releases limited data on completed cases, and the information that is shared has often revealed a lack of understanding of the norms of conduct of fundamental research at universities. Universities usually keep data on breaches of research security tightly held because these data involve privacy and HR issues. In addition, the failures of several recent legal cases against academic researchers are likely to make university leadership even more guarded in releasing information relevant to investigations of their faculty.

Funding agencies, including NSF, have been the most active in sharing data on research security breaches, although there too the data are mostly limited to completed cases as part of case closeout memoranda from the Office of the Inspector General. The research topics listed below are critical to understanding the nature of the research security threats but can only be addressed if funded researchers have access to relevant data on such threats. NSF could, for example, create a controlled-access data pool of unclassified information for researchers working on this problem.

1. Case studies of research security breaches. Frequency of occurrence and resulting actions taken by academic research institutions, private companies, and governmental enforcement agencies. Analyze historical trends regarding the occurrence and consequences of breaches of research security.

2. Collection and analysis of on the frequency and potential severity of research security breaches. Analysis of security implications across research fields and types of research institutions. What fraction of these incidents are due to actions of trainees, research staff, administrators, or principal investigators?

3. Analysis of how unauthorized transmissions of research results have occurred. To which countries, institutions, universities, and private companies have research results been inappropriately disclosed?

4. Analysis of motivations for the premature or unauthorized transmission of research and how such actions are justified by the individuals involved.

5. Analysis of STEM fields that have been of greatest concern and the maturity level of the research when the results were inappropriately transmitted.

6. Comparative assessment of policies of US research institutions and analysis of best practices for research security.

Risk Assessment and Quantitative Approaches. An area of tension between academic researchers and government agencies is the nature of the risk associated with breaches of research security in fundamental research. Because the research is ultimately intended for publication in the open literature, it may seem that that there is little risk associated with failure to protect such research. However, this ignores damage to the academic enterprise that occurs from unapproved sharing of information from grant proposals under review or manuscripts being considered for publication. It is also sometimes the case that the researchers aim to apply for patent protection, usually through the university's office of technology licensing, which may be compromised by unapproved release of information. As discussed above, the consequences of loss of information are likely to be different in different fields, but in some extreme cases could be severe for economic and/or national security.

However, imposing controls that restrict access to research areas could slow progress in critical research areas. Thus, it would be helpful to have reliable models of the effects of different control regimes on the development of research fields.

Assessment of risk associated with the know-how and methods for acquiring and analyzing new data, as well as building new theoretical frameworks based on those data is also essential.

1. Risk assessment via objective functions to provide quantitative measures of the risks and costs of various research security infractions and prevention methodologies. Risk assessment should be carried out for individual scientific fields.

2. Controlled experiments (red team, blue team) involving risk assessment of research security incidents.

3. Game theoretic risk assessment of research security breaches for various scientific fields.

4. Analysis of which types of breaches of research security pose actual economic or national security threats.

5. Algorithms and tools for detection of breaches of research security.

Education and Training. Breaches of research security and the involvement of foreign governments in such breaches are emerging threats. Education and training will be required to help the research community understand the nature of the threat and to adopt measures to mitigate it. The cultural differences between academics engaged in fundamental research and those who are well-versed in security risks will pose a significant challenge to success. Many academics have regular interactions with foreign faculty, graduate students, and postdocs, and consider these to be critical to their research programs. Law enforcement and intelligence community agencies often lack an understanding of how academic research labs operate with respect to the relationships among faculty members and the researchers they supervise, and how those interactions differ across scientific disciplines. This problem is exacerbated by the inability to share confidential or classified information with the research community that might help them to understand the risks associated with breaches of research security. On a hopeful note, there are already mandated Responsible Conduct of Research training programs, and these could be modified to better cover topics of research security.

The NSF recently made awards for four research security training modules. Assessment of the value of these modules after implementation would be useful in guiding further Education and Training. Noting what worked in the present efforts, and equally what did not work, will provide an informed path to future efforts. For this, see https://beta.nsf.gov/news/nsf-2022-research-security-training-united-states

1. Development and assessment of effective education and training strategies for academic, commercial, and other research personnel on issues of research security. Online and in-person approaches, including, where possible, the cooperative presence of law enforcement agencies.

2. Evaluation of existing mandated training and education of Responsible Conduct of Research programs and strategies for incorporating research security issues.

3. Proactive efforts to reduce research security risk in the fundamental research community based on lessons learned from prior cases.

International Cooperation and Reduction of Threats to Research Security. A major factor in the rise of the US in science and technology has been the nation's ability to attract and retain talented researchers from around the world. Foreign researchers contribute at every level of the research ecosystem and in many cases choose to stay in the US after their training. This includes some of our most prominent international scientists. Many in the academic research community believe that the recent actions taken in the interest of research security have unfairly targeted Asian Americans, and that such actions may cause more damage to our competitiveness than breaches of research security. There are also growing concerns about reciprocity and transparency in international science collaborations, which must be balanced with the reality that, in some disciplines, progress can only be made by continuing to engage in such collaborations.

1. Assessment of international differences in the views of scientific research integrity and implications for research security.

2. Analysis of potential costs and benefits to US research security from actively recruiting and retaining students and faculty from a broader range of countries. Extension of this analysis to underserved regions of the US.

3. Considerations in balancing US interests with global interests and how to mitigate risk when global engagement is essential.

4. Analysis of possible threat reduction strategies and preservation of productive international open science ecosystems.

We stress that these illustrative topics for an NSF research program on research security should not be considered to be fully inclusive because the research needs will evolve as more information is gathered and global events unfold. Particularly urgent now are topic areas that deal with current issues associated with Chinese government activities that are at odds with our expectations for research security, and those that deal with collaborations and foreign engagements, focused on maintaining our ability to attract and retain the best talent while making clear our research-related values. Clearly, adaptability is a virtue in this domain, and would ideally be a theme that runs through the research program.

This Page Intentionally Left Blank

6 RESEARCH COMMUNITIES TO BE ENGAGED

JASON was asked by NSF: What are the critical research communities that must be engaged for a research program on research security to be successful?

NSF is considering creating a research program on research security that would provide grants to researchers addressing critical topics. In section 5 of this report we provided illustrative research topics in four areas: data collection and analysis, risk assessment and quantitative approaches, education and training, and international cooperation and reduction of threats to national security. Although most of the concern about research security is focused on the natural sciences and engineering, it is apparent from these topic areas that the research program will require strong engagement with the social sciences, humanities, and the growing field of data science. Because elements of the culture of different fields are integral both to understanding research security issues and proposing workable solutions to them, it will also be necessary to facilitate engagement between grant recipients and the research communities they are studying. Here we consider these needs in the context of the topic areas and the broader research program.

Data collection and analysis. The social sciences are undergoing a transformation driven in large part by the availability of large datasets and new methods to analyze them. As an example, the History Lab (http://history-lab.org/about) is a multi-institutional organization of academic social scientists aiming to use data science to “recover and repair the fabric of the past.” They aggregate documents declassified by the US government and use machine learning tools to probe them. Another example is Opportunity Insights (https://opportunityinsights.org),
a multi-institutional group based at Harvard University using data to identify barriers to economic opportunity in the US and to develop policy solutions. The data needed to address research security issues in the context of the NSF research program are likely to include information from FBI and the intelligence community, senior university administrators for research, technology transfer and information security and data pertaining to international collaborations and exchanges.

It will be important to engage the growing data science community in this effort. Many universities are starting data science programs, either as separate degree-granting units or in conjunction with statistics, computer science, and social sciences. Indeed, NSF has been driving some of this with

"Harnessing the Data Revolution" as one of ten "Big Ideas" that have been highlighted for increased support (https://www.nsf.gov/news/special_reports/big_ideas/index.jsp). The Data Science Collaboratory at Stanford University (https://datascience.stanford.edu/programs/data-science-collaboratory) is an example of a university effort funded through this NSF program, and brings together faculty from statistics, biology, computer science, communication, biomedical data science, and electrical engineering. Ideally, members of such interdisciplinary groups would be engaged, drawn by the economic and societal importance and by availability of data sets.

Risk Assessment and Quantitative Approaches. Because of the lack of agreement on the risks associated with breaches of research security, and the field-dependent differences in those risks, it will be essential to have robust engagement with economists and others in the risk analysis research community. The US government engages in open risk assessment across many topics, with USDA being a good example. USDA has a Chief Economist, and an Office of Risk Assessment and Cost-Benefit Analysis (ORACBA), which sponsors a Science, Policy and Risk Forum. These government efforts are similar to private sector efforts focused on decision making with respect to economic risks, which are often regulatory in nature. Fundamental research presents different challenges, with the benefits often playing out over many years, and the risks less defined. It will be essential to engage economists and academics studying decision science and operations research in this problem.

This is a topic that will also have benefit outside of research security, to help government officials and the public understand the value of fundamental research to the nation. Similar efforts have been very successful in highlighting the economic benefit of natural resources, or the "natural capital" of a nation, and arguing for their conservation (Costanza 1997). Mathematical simulation models, particularly Bayesian network models, are an important part of these analyses, and have been used extensively in health policy decision making and many other fields. There are conferences devoted to this topic sponsored by the American Statistical Association and other organizations that can serve as points of dissemination of information about the NSF research program.

Education and Training. Policies, practices, and programs on research security are only as effective as the extent to which the stakeholders in research security know about them and adhere to them. Universities have over the last two decades adopted new ways of training faculty, students and staff on important topics, often to meet the requirements of funding agencies, accreditors and state and federal law. In some cases, they rely on third-party providers focused on the academic market, such

as The Collaborative Institutional Training Initiative (CITI Program). The topics covered by these programs include ethics and compliance and sexual harassment training. The needs for research security education and training are analogous to these, allowing some leverage of existing programs, but also different due to the reliance on classified or confidential information as part of the basis of the topic, and with greater opportunity for proactive measures to be taken. Faculty in graduate schools of education are likely to be interested in addressing these problems. There are also important issues of organizational change with respect to how the research community sees issues of research security, and faculty specializing in management and organizational change and renewal, typically at graduate schools of business, would also be useful partners.

International Cooperation and Reduction of Threats to Research Security. The US fundamental research ecosystem benefits from openness and international engagement, but few analyses have been carried out to assess the balance between these benefits and their potential costs to research security. Like risk assessment, this is, in part, an issue of economics and understanding the consequences of restrictions on innovation and productivity. It will be important to engage with academic economics communities, particularly those that have embraced interdisciplinary approaches to analysis. Prominent examples include the Becker Friedman Institute for Economics at the University of Chicago and the Institute for Economic Policy Research at Stanford University. These institutes, and others like them, bring together faculty from across the research university to address important issues of economics and how to translate results to policy. It will also be critical to learn from previous examples, accessing the expertise of historians and political scientists working in science and technology.

Many of the international issues confronting research security are connected deeply with cultures and customs of science in different countries. For example, the mounting of various “talent programs” by the Chinese government, engaging scientists and engineers in the US with little regard for conflicts of interest or commitment, reflects a different view than is widely accepted as appropriate and normal in the US. This situation argues for engagement with academic communities that study these differences, including history and ethics. We anticipate that the results of this direction of a research program into research security will provide an evidence-based understanding of the relevant mores of the societies where research collaboration takes place.

Scientists and their research programs exist within a framework of discipline-specific cultural norms established over many years. For example, the order of authors on a publication in the biosciences has implied meaning with respect to contributions of those authors (Tscharntke 2007). This meaning is apparent to a practitioner in that discipline but opaque to a researcher from a different discipline that, for example, simply lists authors alphabetically. Because elements of the culture of different fields are integral both to understanding research security issues and proposing workable solutions to them, it will also be necessary to facilitate engagement between grant recipients and the research communities they are studying. In accord with this need, JASON recommends that social scientists pursuing research on research security actively engage with natural scientists as part of their work and that NSF structure the program to incentivize that engagement. Three ways we suggest to promote such engagement are: (1) encourage cooperative proposals from teams of social scientists and natural scientists; (2) note opportunities (and allow use of grant funding) to embed social science awardees in natural sciences laboratories, following on the idea attributed to Bronislaw Malinowski that anthropologists must “come down off the veranda” and experience the everyday life of their subjects to truly understand them; and (3) sponsor multidisciplinary workshops and symposia with participation of both natural scientists and social scientists on topics chosen to stimulate interaction between them.

Professional societies that serve the scientific community are an important point of intersection between the practicing scientists that are their members, and funding agencies and government policy makers that are their sponsors. As part of their role in representing their constituent members, professional societies have the pulse of discipline-specific attitudes of members towards current policy topics, including research security. JASON spoke at length with one professional research society, the American Physical Society (APS), and we analyzed the public statements of two others: the American Geophysical Union and the American Chemical Society.

According to a survey of APS members in December 2021 (APS 2021) there was deep skepticism among the members of the APS that there is any evidence-based threat to fundamental research security. Those responding APS members also felt that US government actions had singled out Chinese and Chinese-American scientists as targets for law enforcement actions. The possible missteps of US law enforcement efforts with respect to individuals charged with research security violations have likely strengthened the conviction that there is no substantive issue. Presumably these views are influenced by a combination of lack of information about the threat, general distrust of

government interventions in the conduct of research – particularly when it comes with increased regulatory burden – and genuine disagreement about what constitutes a threat to fundamental research.

For those pursuing research on research security in the context of an NSF program, it will be important to understand the dynamic of such professional societies and their relationship to member attitudes, as well as enlisting them to aid in that research by sharing information. Ultimately, professional societies could be allies in addressing threats to research security, if the research products of the proposed NSF program are able to surmount the attitude issues evident in the APS membership survey. Societies have many members (APS has approximately 50,000) and these members often have a strong affinity for their society, for events such as the annual meeting, and for journals published by the society.

Professional societies are thus important conduits for information about research security, with messages from the leadership of the societies received by members without a sense of legal threat or government interference.

Clearly, an NSF research program on research security would benefit from representation of the relevant professional societies, building on the relationships that NSF already has with them. The societies can be partners in research projects supported by the program, and participants — even organizers — of the recommended multidisciplinary workshops that would precede grant-making. Reaching out to these societies as partners, where appropriate, will contribute to the practical success of the proposed NSF program by helping to develop and disseminate the results of educational and training programs emerging from research on research security to principal investigators and other senior personnel in the research ecosystem.

The NSF may wish to consider a number of large awards, at the level of a Center, to assure that all of the, sometimes disparate, important disciplines will be working together effectively. This would balance the smaller individual awards that will also form part of a research program in research security.

This Page Intentionally Left Blank

7 DATA AND PRIVACY CONSIDERATIONS

JASON was asked by NSF: What data will be required for research on research security? What privacy controls will be required?

Acquisition and analysis of data on the numbers and nature of breaches of research security and their consequences will be essential for the success of this research program. NSF and other funding agencies, law enforcement, universities, and private companies all hold relevant and important data. Restrictions that the relevant data might be under include the following:

Classified information by the US government or the government of other countries, which is only accessible to those with appropriate security clearances and a need to know. This includes information from the intelligence community and FBI at the TS/SCI (Top Secret / Sensitive Compartmented Information**)** level that few academics are cleared to access. These data might, for example, include information about talent recruitment programs organized by other countries, the details of which would reveal specifics of the method of collection of that information, or pertain to cases that law enforcement is currently prosecuting.

Confidential unclassified information (CUI), which is subject to a range of restrictions, and generally is information held by the US government that requires safeguarding of some form. Such data includes personally identifiable information, law enforcement information, controlled technical information, export control, and many other categories (see National Archives for current listing: https://www.archives.gov/cui/registry/category-list). An example relevant to research security would be the names of US researchers who have been identified by federal agencies as potentially having unresolved conflicts of commitment.

University and business confidential and proprietary information. Both academic and private sector institutions hold some information as confidential, including human resources records, internal communications, and strategy documents. These institutions also hold proprietary information that might include research results, internal grants, trade secrets, client and supplier lists, security practices, etc.

JASON assesses that researcher access to relevant data will be one of the most significant challenges faced by the proposed research program. In the face of these issues of privacy and confidentiality, NSF should be prepared to support acquisition and anonymization of data for use by researchers and to establish this support prior to awarding grants. We note that NSF already has an internal program for gathering and analyzing open access data, which could circumvent some of these issues (Paul Morris, NSF briefing to JASON, June 2022).

Anonymization techniques and privacy controls on individual records in databases such as will be needed for research on research security have been explored for at least two decades (Sweeney 2002) (Wood 2020) (Cohen 2022). An example of current best practices in this area is the use of differential privacy methods, which make it possible to release some aggregate statistical information about collected confidential data while maintaining meaningful privacy guarantees. These methods add noise to the output of a computation, with the amount of noise necessary to maintain privacy depending on the sensitivity of the output (how much it can change with a small change in the input) and the desired inference bound (privacy guarantee). When the amount of data is small and sensitivity is high, the amount of noise needed to provide a useful privacy guarantee may be too much to preserve the reliable use of the data. This is likely to be the situation with the current data of relevance to research security, highlighting the importance of making the research security database as large as possible, for example by including information on breaches from other, non-NSF research organizations such as NIH and DOE Office of Science. A useful review of the methods of differential privacy may be found in (Wood 2020).

The largest real-world example of the application of differential privacy is the 2020 US census. The census contains multiple pieces of information on each of the 330,000,000 people in the US, and the Census Bureau publishes billions of summary statistics, which are counts of individuals with given properties. Publishing completely accurate values of these counts would enable computational reconstruction and deanonymization for an unacceptable fraction of individual records, violating the confidentiality requirements of federal law. Therefore, these counts cannot be revealed both completely and accurately. Thus, the Census Bureau chose to adopt differential privacy as a way of adding noise that maintains confidentiality while preserving the usefulness of the data (Cole 2021) (Wood 2020)).

Differential privacy is a property of the questions asked of the data and of the analysis of the data. That is, if one is committed to using differential privacy to protect privacy, the set of questions must be limited. Data cannot be collected and then used in arbitrary ways. Other privacy protections are possible, such as usage agreements and analysis in protected enclaves. Their utility for the purposes of the NSF research program would have to be evaluated based on the damage that might result from disclosures compared to the value of the proposed analysis.

Consideration must be given to how researchers will access these data and how to retain privacy and anonymity as the researchers perform their own analyses and reach their own conclusions. For statistics on top-level descriptors (e.g., number of breaches by discipline, broad categories of what and how much was breached) it may not be necessary to have secure protocols for the computing environments used by researchers at their home institutions. However, for research topics involving details of how specific sub-classes of incidents occurred or that analyze “case study” examples, researchers will likely need to use protected computing enclaves (sometimes called “trusted research environments” or “data safe havens”) at their home institutions. These enclaves are being actively developed and refined, particularly in the field of health care (see for example (Gao 2022, Burton 2015).

This Page Left Blank Intentionally

8 SUMMARY

JASON concludes that an NSF research program on research security would be useful in addressing many of the concerns about foreign influence and the security of the US fundamental research ecosystem. There are many topics that could be the subject of such a research program and most of these will benefit from strong engagement with social scientists, and collaboration of those social scientists with practicing natural scientists in the fields of interest. Access to data will be a serious challenge to the success of a research program, but one that likely can be mitigated by application of appropriate anonymization methods.

In addition to the specific responses to the questions presented in the body of this report, JASON offers the following findings and recommendations (also in Executive Summary):

Findings

1. The issue of research security is real. The fruits of US STEM research and their benefits to US interests across many arenas have been challenged by inappropriate practices in the international arena.

2. US researchers often feel threatened, frightened, and/or burdened by past and current actions to deal with problems of research security and integrity. Survey data indicate that these concerns are widespread and deep.

3. The consequences and appropriate actions related to breaches of research security differ among STEM fields.

4. The definition of research integrity differs across national interests and cultures.

5. The NSF internal project on the identification of potential breaches of research integrity and security through analysis of open-source data could lead to a useful product for dissemination to other federal, academic, and commercial organizations.

6. STEM Principal Investigators best understand the customs and practices of their discipline, and they can be important partners in a research program on research security. They should have the ability to decide when the products of research are ready for publication and public dissemination.

7. The success of an NSF program on research security will depend on NSF working with universities and private companies to make available their data on issues of research security in a protected manner that allows access to approved research programs on this topic and provides protection of the privacy of the sources.

Recommendations

1. The products of a research program on research security must not be used to disadvantage anyone based on their ethnic background or country of origin. Every effort should be taken to keep the US as the premier destination for top scholars around the world, working in an open science environment, and we must avoid creating a reputation of racial profiling or injustice.2. In a research program on research security, NSF and proposers must consider the ability to access confidential data at universities and private companies. NSF should assist Principal Investigators with data access and in the use of methods for anonymization of data.

3. The NSF program should emphasize research on effective methods for informing and training Principal Investigators about potential risks in international collaborations by country and, where appropriate, by institution.

4. The NSF research program should encourage research projects in collaboration with international organizations that share our concerns for research security.

5. As part of the proposed research program, NSF should encourage collaborations between social scientists and other STEM researchers, for example, via cross-disciplinary workshops before and during research performance.

6. The NSF should work closely with US STEM professional societies to maximize access of research program awardees to STEM researchers and to disseminate educational and training materials.

7. NSF should work with other Federal agencies (e.g., NIH, DOE, NASA) that have a major stake in unclassified basic and applied research to create a protected database of matters of breaches of research security at universities, private companies, and government laboratories, which can be accessed by approved researchers in the NSF research program on research security while maintaining the privacy of the sources. The larger size of a database with information from other Federal agencies included will make statistical analysis more robust and can aid in the implementation of anonymization methods such as differential privacy.

This Page Intentionally Left Blank

Bibliography

APS. 2021. *Impact of US Research Security Policies US Security and the Benefits of Open Science and International Collaborations.* American Physical Society. https://www.aps.org/newsroom/pressreleases/upload/APS-Impact-of-Research-Security-Report.pdf.

Burton, P. R. et al. 2015. "Data Safe Havens in Health Research and Healthcare." *Bioinformatics* 31: 3241–3248.

Bush, Vannevar. July 1945. *Science the Endless Frontier.* Washington, D. C.: A Report to the President by Vannevar Bush, Director of the Office of Scientific Research and Development, July 1945. https://www.nsf.gov/od/lpa/nsf50/vbush1945.htm.

Cohen, Aloni. 2022. "Attacks on Deindetification's Defenses." *31st USENIX Security Symposium.* Boston, MA. https://www.usenix.org/conference/usenixsecurity22/presentation/cohen.

Cole, Shawn and Dhaliwal, Iqbal and Sautmann, Anja and Vilhuber, Lars. 2021. "Handbook on Using Administrative Data for Research and Evidence-based Policy." https://admindatahandbook.mit.edu/.

Costanza, et al. 1997. "The value of the world's ecosystem services and natural capital." *Nature* 387: 253-260.

2022. "G7 Common Values and Principles on Research Security and Research Integrity." https://sciencebusiness.net/news/g7-science-ministers-urge-democracies-unite-research-efforts.

Gao, C. et al. 2022. "A National Network of Safe Havens: Scottish Perspective." *Journal of Medical Internet Research* 24.

January 2022. "Guidance for Implementing National Security Presidential Memorandum 33 (NSPM-33) on National Security Strategy for United States Government-Supported Research and Development." https://www.whitehouse.gov/wp-content/uploads/2022/01/010422-NSPM-33-Implementation-Guidance.pdf.

June 15, 2022. "HR001122S0041 DSO OFFICE-WIDE BAA." DSO. https://govtribe.com/opportunity/federal-contract-opportunity/defense-sciences-office-dso-office-wide-baa-hr001122s0041.

JSR-19-21, JASON. 2019. "Fundamental Research Security." https://www.nsf.gov/news/special_reports/jasonsecurity/JSR-19-2IFundamentalResearchSecurity_12062019FINAL.pdf.

Keith W. Crane, Thomas J. Colvin, Abby R. Goldman, Emily R. Grumbling, and Andrew B. Ware. 2021. *Economic Benefits and Losses from Foreign STEM Talent in the United States.* Washington, D. C.: IDA SCIENCE & TECHNOLOGY POLICY INSTITUTE; IDA Document D-31855. https://www.ida.org/research-and-publications/publications/all/e/ec/economic-benefits-and-losses-from-foreign-stem-talent-in-the-united-states.

Malinowski, Bronislaw. 1964. *The Revolution in Anthropology.* https://en.wikipedia.org/wiki/Off_the_verandah.

January 14, 2021. "Presidential Memorandum on United States Government-Supported Research and Development National Security Policy." https://trumpwhitehouse.archives.gov/presidential-actions/presidential-memorandum-united-states-government-supported-research-development-national-security-policy/.

Sweeney, Latanya. 2002. "k-anonymity: a model for protecting privacy." *International Journal on Uncertainty, Fuzziness and Knowledge-based Systems* 10: 557-570.

Tscharntke, et al. 2007. "Author Sequence and Credit for Contributions in Multiauthored Publications." *PLOS Biology* 5: 0013-0014. doi:10.1371/journal.pbio.0050018.

Wood, Alexandra and Altman, Micah and Nissim, Kobbi and Vadhan, Salil. 2020. *"Designing Access with Differential Privacy," Chapter 6, Handbook on Using Administrative Data for Research and Evidence-based Policy.* Edited by Dhaliwal, Sautmann, and Vilhuber Cole. https://admindatahandbook.mit.edu/book/v1.0/diffpriv.html.