Safeguarding the Research Enterprise

Contact: Gordon Long—glong@mitre.org

JSR-23-12

March 21, 2024

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

Contents

‘

This Page Intentionally Left Blank

1 EXECUTIVE SUMMARY

The National Science Foundation (NSF) is the premier government organization supporting fundamental scientific and engineering research in the United States. In 2019, NSF asked JASON to comment on how NSF might respond to growing concerns that the openness of the U.S. academic research system was being taken advantage of by other countries. The resulting JASON report, *Fundamental Research Security*, discussed the issues of both research integrity and research security, and identified four major themes:

- The value of, and need for, foreign scientific talent in the United States;
- The significant negative impacts of placing new restrictions on access to the results of fundamental research;
- The need to extend our notion of research integrity to include disclosures of commitments and potential conflicts of interest; and
- The need for a common understanding between academia and U.S. Government agencies about how to best protect U.S. interests in fundamental research while maintaining openness and successfully competing in the global marketplace for science talent.

In the 4 years since the 2019 report, the discussion of how best to address issues of research security has evolved. Legislation, such as the CHIPS and Science Act of August 2022, has further defined NSF's obligations to identify and protect certain types of research—in particular, those involving Controlled Unclassified Information (CUI). In addition, other U.S. government agencies, such as the Department of Energy (DOE) and the Department of Defense (DOD), have developed approaches to identify and mitigate risks to national security from research funded by their organizations. Given the evolving landscape for research security, NSF asked JASON to comment further on specific steps it might take to identify sensitive areas of research and describe processes NSF might use to address security in those research areas of concern.

JASON was asked:

1. What are the general principles that NSF might use in developing lists of research/technology areas of concern?
2. What existing structure and guidance for federal Controlled Unclassified Information (CUI) might be applicable to identifying NSF-funded research/technology areas of concern?
3. What processes might NSF establish for annually reviewing its list of research/technology areas of concern?
4. Using one or more specific research/technology areas, as examples, what detailed evaluation criteria might NSF use for identifying research/technology areas of concern?
5. What are some of the potential impacts on the research community should some NSF-funded research areas be designated as areas of concern?
6. What processes and restrictions might be implemented to carry out research that falls within the NSF-designated CUI category?

In addressing these questions, JASON had frequent discussions with NSF leadership and heard a wide spectrum of ideas from individuals from various government agencies, university administrators, and experts on issues of research security. We came to understand that the subject of *research security* is much broader than the narrower issue of *research controls*, and that there is a need to go beyond research controls toward a broader strategy for enhancing research security for NSF.

Our study endorses the major themes of the 2019 JASON report, and considers the following additional themes.

- Fundamental research is a critical component of U.S. scientific and technical leadership, promoting national security in both defense and economic domains.
- Recipients of federal funding have a responsibility to protect U.S. interests, and the U.S. research community should be actively engaged in protecting those interests.
- Transfers of sensitive technologies to foreign countries can create national security risks.

- Research controls, such as CUI, are only one component of a broader strategy of risk mitigation and management to ensure that U.S. research contributes significantly and positively to the national interest.

Our principal findings and recommendations address and build on these themes, and suggest approaches NSF might use to identify research areas of concern, as well as processes for mitigating the risks to national security in those areas. This report focuses on security for research that has potential military or defense applications, rather than on research with potential economic implications.

JASON presents the following Key Findings and Recommendations.

1.1 Key Findings

1. Openness and transparency in fundamental research promote scientific discovery, which improves national security.

2. International collaborations with those who share the ideals of openness and transparency benefit all participants. However, recent efforts of the People's Republic of China (PRC) to preferentially direct fundamental research toward military needs, and its decision to restrict the flow of information out of the country, may severely limit the benefits of collaborations with research organizations within the PRC.

3. Differentiation between sensitive and non-sensitive research is most natural at the project level, not at the sub-field level. Projects in the same sub-field can have very different levels of risk.

4. Risk mitigation must consider the spectrum of risk and be adaptable to changing trends in research. Resources should be concentrated on areas of maximum risk to ensure that benefits outweigh the costs.

5. Formal controls on research, such as a CUI designation, will have unintended consequences, including: increasing the cost of doing research, diverting resources better applied to expanding U.S. research efforts in critical fields, inhibiting rigorous and competitive development of new technologies, and discouraging some individuals and research organizations from engaging in U.S. research.

6. The NSF proposal and reporting cycle provides the most natural means for identifying sensitive projects—i.e., those projects for which the release of information about research execution or outcomes could have a significant, direct, and predictable impact on national security.

7. Research institutions and NSF have key roles to play in the process of risk identification and management. Dialogue between NSF and research institutions such as universities is critical.

8. Awareness of research security issues among university researchers is lower than warranted at present, but approaches are available to raise the awareness level, and such steps are mandated under the CHIPS and Science Act.

1.2 Key Recommendations

1. NSF should adopt a dynamic approach for identifying potentially sensitive research topics as they arise, instead of attempting to maintain a comprehensive list of sensitive research areas. NSF's process of identifying sensitive research projects should:

   - Differentiate research projects based on the sensitivity of their potential applications,
   - Include the maturity of the development path (Technology Readiness Level—TRL) for potential applications in the assessment of risk, and
   - Include an assessment of the direct and predictable national security impact of the applications of each research proposal, if successful.

2. NSF should proceed with caution before adding access or dissemination controls to grants or contracts. In considering whether to apply formal controls to a sensitive research project, NSF should weigh the balance between the positive protective benefits and the unintended negative consequences of such controls. Controls can protect U.S. national security by preventing malign use of research results, but they can also hinder the beneficial free flow of research results in a way that negatively impacts broader U.S. economic and national security interests.

3. The identification of sensitive projects proposed to NSF occurs most naturally before peer or panel review. We recommend that the principal investigator (PI) and the NSF program officer, with guidance from the NSF Division Office, determine if a proposal constitutes a sensitive project. NSF may wish to implement a pilot program within some division of NSF to gain experience with the process. NSF should consult with other federal research funding agencies such

as the Department of Energy (DOE), the National Institutes of Health (NIH), and the Department of Defense (DOD) to help identify sensitive research.

4. Specific mitigation strategies for sensitive research projects should be negotiated and agreed upon by the principal investigator (PI), NSF, and the sponsored projects office of the institution accepting responsibility for execution of the research. Specific mitigation steps should be proportionate to the assessed risk, relative to the associated costs.

5. NSF should foster a culture of research security awareness by providing substantive information to researchers about real risks, making resources available for researchers to voluntarily seek guidance, and continuously engaging with researchers and their institutions about the efficacy of research risk mitigation and control efforts.

6. NSF should engage in dialogue with international partners who have like-minded approaches to research security and integrity, and who are facing similar research security problems.

1.3 Conclusions

This report recommends specific steps that NSF can take to enhance awareness of research security, both within NSF and in the research community. It also suggests mechanisms for NSF to address research projects that are identified as sensitive because of their possible impact on national security. The processes we describe are compatible with the existing NSF structure and its emphasis on funding of research proposals from individual researchers and research organizations. The processes are flexible and adaptable so that they can respond to changing conditions and thinking about research security. While our recommendations focus on academic research security, many are relevant to NSF-funded R&D at organizations other than institutions of higher learning.

This Page Intentionally Left Blank

2 INTRODUCTION AND CONTEXT

2.1 Historical Retrospective: We Have Been Here Before

We are in a period of debate about how to ensure U.S. research security in a manner that does not undermine the great benefits that research in science and technology (S&T) brings to our Nation. In the past few years, policymakers across the U.S. Government have expressed increasing concern that foreign nations, principally the People's Republic of China (PRC), seek to exploit the fruits of U.S. scientific and technological research for purposes that are harmful to U.S. interests.

However, this is not the first time that a national debate has been raised on the issue of research security. In the 1980s, there was concern about Soviet technology acquisition, and it was apparent that the Soviets were making a concerted worldwide effort to secure military technology and know-how.[1] The security concerns extended to new technology early in the R&D cycle by universities and research centers. To help address these concerns, Richard DeLauer, Under Secretary of Defense for Research and Engineering, established a DOD-university forum. DeLauer worked with Frank Press, President of the National Academy of Sciences (NAS), to set up a panel of the NAS, chaired by Dale Corson of Cornell, that included representatives from government, industry, and academia. The panel's mission was to discuss the relationship of scientific research to national security. In September 1982, the Corson panel[2] found that:

> Scientific communication is traditionally open and international in character. Scientific advance depends on worldwide access to all the prior findings in a field—and, often, in seemingly unrelated fields—and on systematic critical review of findings by the world scientific community.

and further found that:

> Controls on scientific communications can be considered in the light of several national objectives. Controls can be seen to strengthen national

[1] Mario Daniels and John Krige, *Knowledge Regulation and National Security in Postwar America*, Chicago, IL: University of Chicago Press, 2022. [1]

[2] National Academies of Sciences, Engineering, and Medicine, Committee on Science, Engineering, and Public Policy, "Scientific Communication and National Security," Washington, DC: National Academies Press, 1982, accessed December 18, 2023, https://doi.org/10.17226/253. [2]

> security by preventing the use of American results to advance Soviet military strength. But they can also be seen to weaken both military and economic capacities by restricting the mutually beneficial interaction of scientific investigators, inhibiting the flow of research results into military and civilian technology, and lessening the capacity of universities to train advanced researchers. Finally, the imposition of such controls may well erode important educational and cultural values.

Finally, in underlined text, the Corson panel concluded that:

> in comparison with other channels of technology transfer, open scientific communication involving the research community does not present a material danger from near-term military implications.

As an interesting nuance, the report stated:

> The Panel found it possible to define three categories of university research. The first, and by far the largest share, are those activities in which the benefits of total openness overshadow their possible near-term military benefits to the Soviet Union. There are also those areas of research for which classification is clearly indicated. Between the two lies a small "gray area" of research activities for which limited restrictions short of classification are appropriate.

Forty years later, we are again discussing possible controls on a "gray area" of research for which limited restrictions short of classification might be appropriate. Our report considers this "gray area" in the current context of the U.S. research enterprise, and specifically how NSF might identify sensitive research projects; and what NSF can do, working with universities and other funded research organizations, to mitigate risks to research security.

The Corson Report was followed in September 1985 by President Ronald Reagan's National Security Decision Directive (NSDD)-189, National Policy on the Transfer of Scientific, Technical and Engineering Information, which referred to the Corson Report and defined fundamental research as follows:

> "Fundamental Research" means basic and applied research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community.

NSDD-189 continues:

> It is the policy of this Administration that, to the maximum extent possible, the products of fundamental research remain unrestricted. It is also the policy of this Administration that, where national security requires control, that the mechanism for control of information generated during federally-funded fundamental research at colleges, universities and laboratories is classification.

The document concluded:

> No restrictions may be placed upon the conduct or reporting of federally-funded fundamental research that has not received national security classification, except as provided in applicable U.S. Statutes.

The important question for U.S. research security today is: *Has the situation changed significantly enough that the principles underlying unrestricted fundamental research need to be re-examined?* In this report, we judge that those principles remain valid, but the evolving context of the U.S. research enterprise requires new approaches to ensure research security in cases of substantive perceived risk. Recognizing that restrictions and controls are not the only, or even the most effective, approach to ensure research security, this report explores how best to identify sensitive areas of research and discusses the broad spectrum of responses available to address issues of research security.

2.2 What Has Changed?

Some of the changes affecting security in the U.S. research enterprise include:

- The perception that national defense is increasingly connected to technology innovation in the civilian commercial sector. Examples include large constellations of commercial satellites and the development of artificial intelligence (AI) and large language models by the commercial sector. Supply chain issues are another aspect of this linkage. While a strong economy has long been recognized as essential to a strong national defense, in the past, technologies have often flowed from the military to the civilian sector (e.g., the internet and GPS.) We now see growth in the flow in the opposite direction.

- The increasing connection and decreasing distance between areas of academic research and their application and commercial development. The new NSF Directorate for Technology, Innovation, and Partnerships (TIP), authorized by the CHIPS and Science Act,[3]. is a recognition of this linkage.
- The increasing globalization of the research enterprise, driven in part by the broad dissemination of knowledge via the internet.
- The continuing rise of the PRC as a peer competitor to the United States, together with concerns about the PRC's policies of military–civil fusion.
- The evolving regulatory and legislative landscape in the United States with respect to research security.

As context for this report, we now discuss recent changes in the regulatory and legislative landscape, and the changing situation with respect to the PRC.

2.3 Recent Directives and Legislation

Since the Corson Report in 1982, and NSDD-189 in 1985, additional orders, regulations, and legislation have implications for research security in the United States.

Executive Order 13556: Controlled Unclassified Information (CUI). A 2010 executive order from President Barack Obama[4] stated:

> This order establishes an open and uniform program for managing information that requires safeguarding or dissemination controls... At present, executive departments and agencies (agencies) employ ad hoc, agency-specific policies, procedures, and markings to safeguard and control this information, such as information that involves privacy, security, proprietary business interests, and law enforcement investigations. This inefficient, confusing patchwork has resulted in inconsistent marking and safeguarding of documents, led to unclear or unnecessarily restrictive dissemination policies, and created impediments to authorized information

[3]U.S. Congress, *CHIPS and Science Act*, 117th Congress (2021–2022), Public Law No. 117-167, 2022, accessed December 18, 2023, https://www.congress.gov/117/plaws/publ167/PLAW-117publ167.pdf

[4]Office of the President of the United States, *Controlled Unclassified Information, Executive Order 13556 of November 4, 2010*, accessed December 18, 2023, https://www.govinfo.gov/content/pkg/FR-2010-11-09/pdf/2010-28360.pdf.

> sharing... To address these problems, this order establishes a program for managing this information, hereinafter described as Controlled Unclassified Information.

Executive Order 13556 established the concept of CUI and declared the National Archives as being the responsible organization for implementation and oversight of the actions of federal agencies regarding CUI. The implementing regulation for CUI was stated later, in 2016, in the Code of Federal Regulations (CFR).[5] While Executive Order 13556 makes no mention of research security itself, CUI is part of the implementation guidelines for both National Security Presidential Memorandum (NSPM)-33 and the CHIPS and Science Act, described next.

National Security Presidential Memorandum (NSPM-33). In January 2021, the broader issues of security for government-supported R&D were addressed in NSPM-33[6] at the end of the Trump Administration. In January 2022, the National Science and Technology Council (NSTC) issued guidance for implementing NSPM-33,[7] which provided further details on how federal agencies should implement the provisions of NSPM-33. Together, these two documents describe the executive branch guidelines for funding agencies and funded organizations regarding research security. Additionally, a "Draft Research Security Programs Standard Requirement"[8] was circulated for public comment by the NSTC in February 2023. This document discussed draft guidelines for universities and other research organizations in several areas, including training, travel, and disclosures.

[5]"Controlled Unclassified Information (CUI)," *Code of Federal Regulations*, title 32 (2018): 497–517, accessed December 18, 2023, https://www.govinfo.gov/content/pkg/CFR-2018-title32-vol6/pdf/CFR-2018-title32-vol6-part2002.pdf.

[6]Office of the President of the United States, *Presidential Memorandum on United States Government-Supported Research and Development National Security Policy*, (January 14, 2021), accessed December 18, 2023, https://trumpwhitehouse.archives.gov/presidential-actions/presidential-memorandum-united-states-government-supported-research-development-national-security-policy/.

[7]NSTC, Subcommittee on Research Security, Joint Committee on the Research Environment, *Guidance for Implementing National Security Presidential Memorandum 33 (NSPM-33) on National Security Strategy for United States Government-Supported Research and Development*, 2022, accessed December 18, 2023, https://www.whitehouse.gov/wp-content/uploads/2022/01/010422-NSPM-33-Implementation-Guidance.pdf. [3]

[8]NSTC, Office of Science and Technology Policy, Subcommittee on Research Security, *Draft Research Security Programs Standard Requirement*, 2023, https://www.whitehouse.gov/wp-content/uploads/2023/02/RS_Programs_Guidance_public_comment.pdf [4], accessed December 18, 2023.

CHIPS and Science Act. August 2022 saw passage of the landmark CHIPS and Science Act,[9] which describes the detailed provisions for individual federal agencies regarding research security, including the Department of Energy (DOE) and NSF. In particular, Title III, Subtitle D of the CHIPS and Science Act is named "NSF Research Security," and a few selected sections include: establishment of an Office of Research Security and Policy within the NSF Director's Office, NSF development of online resources describing NSF research security policies and best practices for mitigating security risks, training for academic researchers in research security, establishment of a research security and integrity information sharing analysis organization (RSI-ISAO), and ensuring proper protections for CUI. The CHIPS and Science Act also calls for establishment of the NSF TIP Directorate. In addition to agency-specific guidance on research security, the law mandates research security training for federal research award personnel. A useful summary of research security provisions of the CHIPS and Science Act has been provided by the American Association of Universities (AAU).[10]

Taken together, Executive Order 13556, NSPM-33, and the CHIPS and Science Act form the basis of federal guidance with respect to research security.

2.4 The Changing Situation vis-à-vis the PRC

Much of the current discussion on research security has been prompted by the rise of the PRC as a peer competitor to the United States in S&T. Competition between nations is not new, and can even be constructive; what is of concern is the PRC's widespread acquisition of U.S. technology through duplicitous or illegal means.[5] As of the writing of this report, the Biden Administration has adopted a "small yard, high fence" approach,[11] enacting targeted trade restrictions on selected critical technology

[9] U.S. Congress, *CHIPS and Science Act*, 117th Congress (2021-2022), Public Law No. 117-167, 2022, accessed December 18, 2023, https://www.congress.gov/117/plaws/publ167/PLAW-117publ167.pdf.

[10] AAU, *The CHIPS and Science Act of 2022 (H.R. 4346) Research Security Provisions*, August 8, 2022, accessed December 18, 2023, https://www.aau.edu/sites/default/files/AAU-Files/Key-Issues/Science-Security/CHIPSandScienceFinalResearchSecurityProvisions.pdf.

[11] The White House, "Remarks by National Security Advisor Jake Sullivan on the Biden-Harris Administration's National Security Policy," October 12, 2022, accessed December 18, 2023, https://www.whitehouse.gov/briefing-room/speeches-remarks/2022/10/13/remarks-by-national-security-advisor-jake-sullivan-on-the-biden-harris-administrations-national-security-strategy. [6]

areas.[12] This JASON report does not focus on economic and trade issues, but rather on the issue of research security in key areas of S&T with implications for national defense.

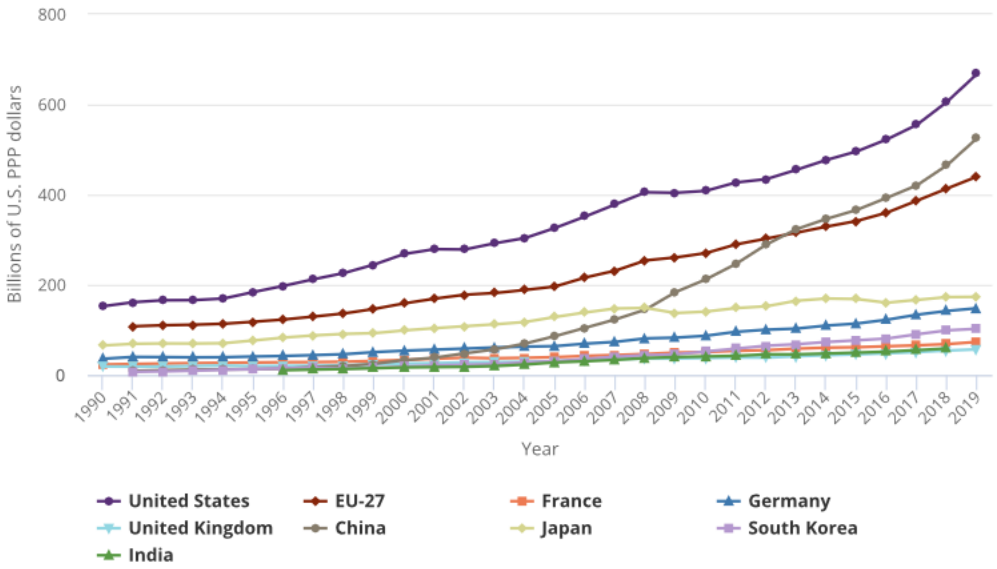

Figure 1: Gross domestic expenditures on R&D, by selected region, country, or economy: 1990–2019. The expenditures are adjusted for purchasing power parity (PPP).

The PRC as a Peer Competitor in R&D.
Figure 1 shows the R&D expenditures for the United States, the PRC, the European Union (EU), and several other countries between 1990 and 2019.[13] The figure clearly shows a sharp increase in R&D investment by the PRC relative to the United States. It also shows that the combined U.S. and EU investment is more than twice that of the PRC, as of 2019 (note that 2019 was prior to the Covid-19 pandemic).

The PRC's government funding for higher education more than doubled over the last decade. When adjusted for purchasing power parity (PPP), Ministry of Education

[12]The White House, "President Biden Signs Executive Order on Addressing United States Investments In Certain National Security Technologies And Products In Countries Of Concern," (August 09, 2023), accessed December 18, 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/08/09/president-biden-signs-executive-order-on-addressing-united-states-investments-in-certain-national-security-technologies-and-products-in-countries-of-concern. [7]

[13]NSF, National Science Board (NSB), *Science and Engineering Indicators*, 2022, *Research and Development: U.S. Trends and International Comparisons, NSB 2022-5*, (April 28, 2022), accessed December 18, 2023, https://ncses.nsf.gov/pubs/nsb20225. [8]

(MOE) spending on higher education now exceeds $179 billion.[14] Perhaps as a result of these efforts, the PRC has surpassed the United States in publishing the largest number of scholarly papers annually.[15]

The PRC's global position in research is clearly a major priority, and the PRC is investing in targeted areas identified as critical emerging technologies.

Another key statistic with significant long-term implications for R&D leadership is the total number of STEM (science, technology, engineering, and mathematics) PhDs educated in the United States compared to the PRC; and further, the number of domestic PhDs educated in the United States, shown in Figure 2.

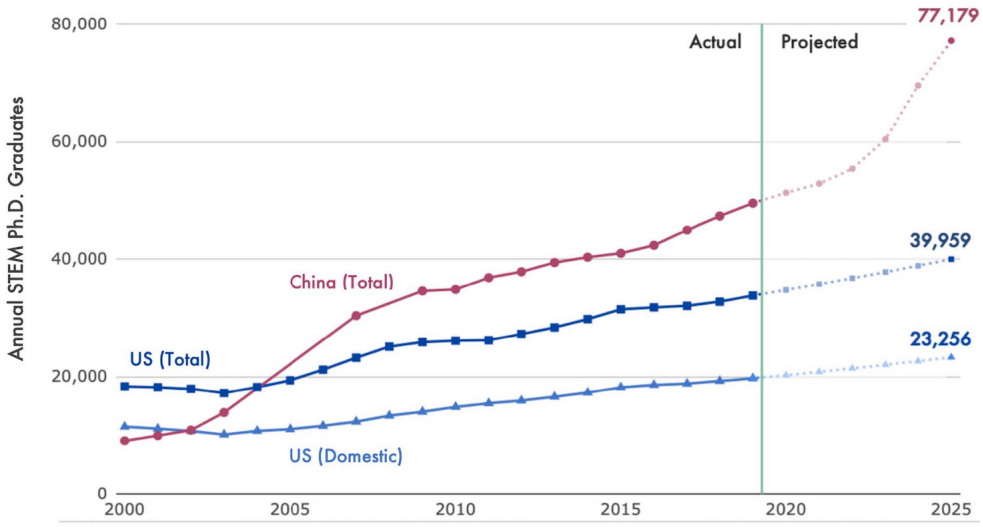

Figure 2: The number of STEM PhD graduates in the PRC has rapidly outpaced the United States in the last 20 years. Regarding the projections, the authors of the report in which the figure appears explain: "The Chinese Ministry of Education publishes data on the number of students who enter PhD programs each year. In recent years, for every 100 students who enter a Chinese STEM PhD program, an average of 93 students obtains a PhD six years later... The rapid growth in projected graduates after 2022 is due to rapid growth in PhD entrants after 2016."[16]

[14]Ryan Fedasiuk et al., "A Competitive Era for China's Universities: How Increased Funding Is Paving the Way," *Center for Security and Emerging Technology (CSET)*, (2022), accessed December 18, 2023, https://cset.georgetown.edu/wp-content/uploads/CSET-A-Competitive-Era-for-Chinas-Universities.pdf. [9]

[15]NSF, NSB, *Science and Engineering Indicators 2022, Publications Output: U.S. Trends and International Comparisons, NSB-2021-4*, October 28, 2021, accessed December 18, 2023, https://ncses.nsf.gov/pubs/nsb20214/international-collaboration-and-citations. [10]

Figures 1 and 2 together indicate that the PRC is domestically producing significantly more STEM PhDs than the United States, and significantly more STEM PhDs per dollar invested in domestic R&D than the United States. While a significant fraction of the U.S. R&D effort is carried out by individuals with degrees other than a PhD, the trends are consistent with the view that the United States has challenges in building a large STEM labor force[17] and that the size of the skilled U.S. STEM labor force may hamper its R&D growth in the future.

Finally, Figure 3 indicates a falloff in the number of students from the PRC studying in the United States. This may be due to several factors, including a perception that the United States is not entirely welcoming to Chinese students, or the difficulty PRC students face acquiring visas for study in the United States. While the pandemic likely also has been a factor, Figure 3 indicates that the total number of international students in the United States has rebounded from its post-Covid minimum, in contrast to the number of students from the PRC, which remains below pre-pandemic numbers. This may be a further indication that the PRC is shifting its incentives and priorities more toward domestic training of graduate students and away from training at institutions outside the PRC.

To maintain leadership in critical technology areas, the United States will need to invest significantly in its own targeted R&D efforts and in the development of its broad STEM workforce. While it is expected that the PRC will continue to attempt to exploit the results of U.S. R&D for its economic and military benefit, it should be clear that *protection of U.S. research from such exploitation will be insufficient by itself to ensure U.S. leadership in critical technologies*. As the PRC increases its competitiveness with the United States in R&D, the PRC's own internal domestic R&D will increasingly power its economic and military development.

The PRC's Military–Civil Fusion (MCF).
The PRC's MCF is a government-led program meant to leverage all state, academic, and commercial developments to strengthen the PRC military. Specifically, it aims

[16]Remco Zwetsloot et al., "China is Fast Outpacing U.S. STEM PhD Growth," *Center for Security and Emerging Technology (CSET)*, (2021), accessed December 18, 2023, https://doi.org/10.51593/20210018. [11]

[17]NSF, NSB, *Science and Engineering Indicators 2022, The State of U.S. Science and Engineering 2022, NSB-2022-1, Conclusion*, accessed December 18, 2023, https://ncses.nsf.gov/pubs/nsb20221/conclusion. [12]

[18]The Open Doors Report on International Educational Exchange is a comprehensive information resource on international students in the United States and U.S. students studying abroad. It is sponsored by the U.S. Department of State, with funding provided by the U.S. Government, and is published by the Institute of International Education. See https://opendoorsdata.org/data/international-students/leading-places-of-origin/ (accessed December 18, 2023).

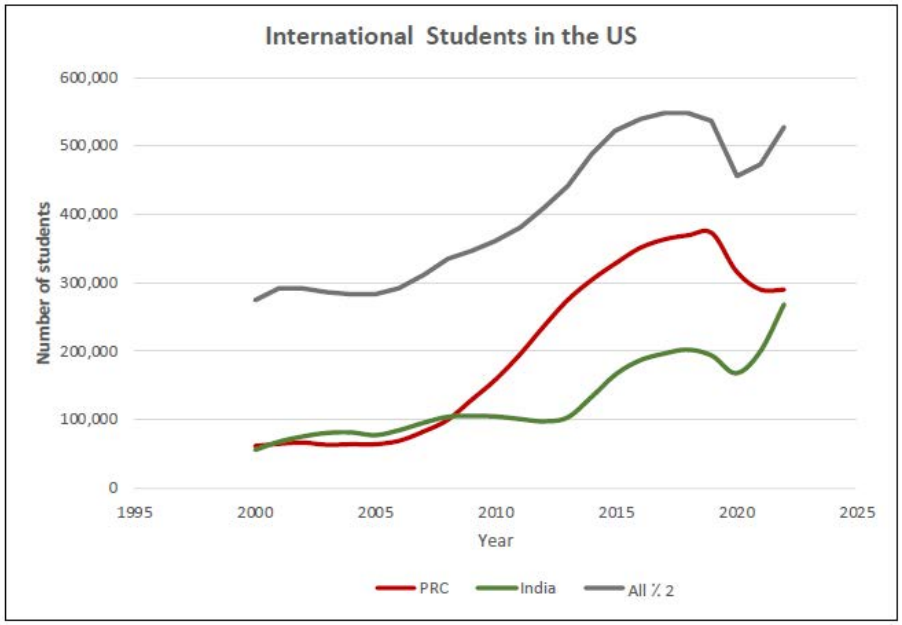

Figure 3: U.S. Department of State data suggest that the number of students from the PRC studying in the United States leveled off prior to the 2020 start of the Covid-19 pandemic, then dropped precipitously, and has not returned to pre-pandemic levels. This is in contrast to the total number of international students in the United States, which has rebounded to pre-pandemic levels, as well as the number of students from India, which is growing dramatically and now exceeds pre-pandemic levels. The PRC and India are the countries with the largest numbers of students in the United States. Note that the curve for the number of students from all countries has been reduced by a factor of two for presentation purposes.[18]

to "Establish a complete policy and institutional system for S&T military–civil fusion. Basically build a policy and institutional system for military–civil fusion with complete systems, linked support, and effective incentives, issue a series of supporting policies to promote S&T military–civil fusion in terms of fiscal spending, prices, investment, financing, and S&T awards, promote the further optimization of the policy and institutional environment for military–civil fusion, and facilitate the flow of innovative elements for S&T military–civil fusion."[19]

The PRC's MCF is significantly different from Civil–Military Integration (CMI) in the United States (see, e.g., [14]). Both have the goal of ensuring that innovations in the civilian sector are utilized effectively by the military. However, while the government

[19]PRC Ministry of Science and Technology (MOST), The "13th Five-Year Special Plan for S&T Military–Civil Fusion Development," June 24, 2020, accessed December 18, 2023, https://cset.georgetown.edu/publication/the-13th-five-year-special-plan-for-st-military-civil-fusion-development/. [13]

of the PRC plays the central role in MCF, mandating and directing fusion activities in the civilian sector, the U.S. approach is decentralized and depends on voluntary cooperation between the U.S. civilian and military sectors, using mechanisms such as research grants and technology-sharing agreements.

The PRC is systematically reorganizing both Chinese academic and industrial enterprises to maximize simultaneous economic and military development. MCF focuses on emerging technologies, specifically "Artificial Intelligence, bio-tech, advanced electronics, quantum, advanced energy, advanced manufacturing, future networks, [and] new materials," in order "to capture commanding heights of international competition."[20] While the PRC term for MCF is not used explicitly in the 14th Five-Year Plan, the plan describes deepening of military–civilian S&T collaboration and adds maritime, aerospace, cyberspace, biotech, and AI to the list of areas for military–civilian development activities.[21]

The ability of the PRC to direct research toward specific targeted areas, and its willingness to close off the external flow of basic scientific information,[22] represents an extreme asymmetry with the global trend to support a broad base of scientific R&D together with open access to scientific data. Further, the PRC's MCF plans allow the ability to direct a vast set of resources (in terms of both civil R&D workforce and capital) toward targeted areas, so as to dwarf U.S. investments that are more broadly based and more open. The U.S. approach to open collaboration and open, broad dissemination of not just results, but also raw data, has contributed to accelerated innovation within the United States and to the efficient leveraging of the results of fundamental research. Further, the potential for fundamental research to result in impactful innovation has been vital in creating the U.S. technology base. As a result, it is hard to predict the long-term implications of the PRC's "closed and directed" MCF policy.

After considerable research and deliberations, JASON arrived at the following finding.

[20]Richard A. Bitzinger, "China's Shift from Civil-Military Integration to Military-Civil Fusion." *Asia Policy* 16, no. 1 (2021): 5-24, https://doi.org/10.1353/asp.2021.0001 (accessed December 18, 2023). [15]

[21]PRC, Outline of the People's Republic of China 14th Five-Year Plan for National Economic and Social Development and Long-Range Objectives for 2035[中华人民共和国国民经济和社会发展第十四个五年规划和 2035 [年远景目标纲要], Xinhua News Agency [(新华社)], March 12, 2021. Chinese source text: https://perma.cc/73AK-BUW2, translation: https://cset.georgetown.edu/wp-content/uploads/t0284_14th_Five_Year_Plan_EN.pdf (accessed December 18, 2023). [16]

[22]Beginning in Fall 2022, the Cyberspace Administration of China began implementing regulations that require the review of major exports of data; and in April 2023, the China National Knowledge Infrastructure platform cut 1,600 institutional users outside mainland China from access to some of its database of statistical and academic publications. See https://www.scmp.com/news/china/article/3214808/portal-china-closing-least-temporarily-and-researchers-are-nervous (accessed December 18, 2023).

> **Finding:** International collaborations with those who share the ideals of openness and transparency benefit all participants. However, recent efforts of the People's Republic of China (PRC) to preferentially direct fundamental research toward military needs, and its decision to restrict the flow of information out of the country, may severely limit the benefits of collaborations with research organizations within the PRC.

While research security to protect against the potential that a foreign actor may misappropriate U.S. R&D efforts is of significant concern, future technological threats may arise from the asymmetrical strategies for the development of critical and emerging technologies in the PRC versus the United States. This future threat is likely best addressed by maintaining or establishing U.S. scientific leadership in critical emerging areas, particularly those that are fundamental, with potential for long-term impact.

2.5 Prior JASON Guidance on Research Security

The 2019 JASON report, *Fundamental Research Security*,[23] provides important context for the current report. We therefore summarize the most relevant findings and recommendations of the 2019 report here and provide its Executive Summary in full in Appendix B.

The 2019 JASON report found that foreign-born scientists and engineers training and working in the United States have made essential contributions to our country's preeminence in science, engineering, and technology; and maintaining that leading position will require that the United States continues to attract and retain the best science talent from around the world. Furthermore, NSDD-189, National Policy on the Transfer of Scientific, Technical and Engineering Information, remains a cornerstone to the fundamental research enterprise that protects the free exchange of ideas.

The 2019 report found that concern over actions of the government and institutions of the PRC that are not in accord with U.S. values of scientific ethics is justified. There are credible problems with respect to research transparency, lack of reciprocity in collaborations and consortia, and reporting of commitments and potential conflicts of interest related to these actions. Exacerbating the issue, U.S. academic leadership, faculty, and front-line government agencies lack a common understanding of undue foreign influence in U.S. fundamental research, the possible risks it poses, and the

[23] Gordon Long, "JSR-19-2I Fundamental Research Security," MITRE Corporation (2019), accessed December 18, 2023, https://www.nsf.gov/news/special_reports/jasonsecurity/JSR-19-2IFundamentalResearchSecurity_12062019FINAL.pdf. [17]

potential detrimental effects that might result from restrictions on such research. Universities and research funding agencies have policies and guidelines regarding some of these responsibilities, but these are often insufficient for individuals to assess risk and take appropriate actions.

JASON recommendations to address the concerns were based on principles of openness, communication, and engagement with stakeholders. The 2019 report recommended that NSF support reaffirmation of the principles of NSDD-189, which make clear that fundamental research should remain unrestricted to the fullest extent possible. It recommended that NSF take lead in working with NSF-funded universities and other entities, as well as professional societies and publishers, to ensure that the responsibilities of all stakeholders in maintaining research integrity are clearly stated, acknowledged, and adopted. JASON furthermore recommended that NSF engage with intelligence agencies and law enforcement to communicate to academic leadership and faculty the scale and scope of risks posed by foreign influence in fundamental research, while also communicating to other government agencies the critical importance of foreign researchers and collaborations to U.S. fundamental research. An additional recommendation was that NSF further engage with the community of foreign researchers in the United States to enlist them in the effort to foster openness and transparency in fundamental research, nationally and globally, as well as to benefit from their connections to identify, recruit, and retain the best scientific talent.

Regarding CUI, the 2019 report found that while the designation in existing categories (HIPAA, FERPA, export control, and Title XIII) is suitable in the relevant circumstances, it is ill-suited to the protection of fundamental research areas. JASON specifically discouraged the designation of new CUI definitions as a mechanism to erect intermediate-level boundaries around fundamental research areas. Based on evolving circumstances, described in Section 2.2, the current report revisits in detail this topic.

Another JASON report, from 2022, *Research Program on Research Security* (JSR 22-08), advised NSF on development of an NSF-funded program on research security. The 2022 report reaffirmed the need to keep the United States a premier destination for international scholars, as well as the necessity for communication and coordination among government agency and academic stakeholders.

2.6 Guiding Themes for the Current JASON Report

The current report endorses the major findings of the 2019 and 2022 JASON reports, and highlights the following themes, which helped guide the deliberations described in the remainder of this report.

- Fundamental research is a critical component of U.S. scientific and technical leadership, promoting national security in both defense and economic domains.
- Openness and transparency, with appropriate controls, are essential in fundamental research, both to validate results and to promote discovery.
- Recipients of federal funding have a responsibility to protect U.S. interests, and the U.S. research community should be actively engaged in protecting those interests.
- Transfers of sensitive technologies to foreign countries can create U.S. national security risks.
- Research controls are only one component of a broader strategy of risk mitigation and management to ensure that U.S. research contributes significantly and positively to the national interest.

3 DEFINITIONS

In writing this report, we became aware of the need to formulate definitions of important words and phrases, as terms like "research" have different meanings depending on the specific context in which they appear. For clarity, throughout this report, we use the working definitions provided in this section.

We first define the related concepts of *national security* and *research security*. We then define various types of research and the important concept of the *fundamental research exclusion* (FRE). We conclude by providing working definitions of *mitigations* and various categories of *controls*.

National Security
Broadly defined, *national security* implies the protection of the United States, its citizens, and its interests, at home and abroad, from threats. In this report, we specifically deal with threats resulting from the misappropriation of the results of U.S. R&D.

Research Security
We use the definition from the National Science and Technology Council (NSTC) *Guidance for Implementing National Security Presidential Memorandum (NSPM-33)*,[24] "Research security is safeguarding the research enterprise against behaviors aimed at misappropriating R&D to the detriment of national or economic security, related violations of research integrity, and foreign government interference."

Research and Development (R&D)
As defined in the guidance for implementing NSPM-33,

> R&D includes basic research, applied research, and experimental development. *Basic research* is experimental or theoretical work undertaken primarily to acquire new knowledge of the underlying foundations of phenomena and observable facts. *Applied research* is original investigation undertaken in order to acquire new knowledge, and directed primarily towards a specific practical aim or objective. *Experimental development* is creative and systematic work, drawing on knowledge gained from research

[24] NSTC, Subcommittee on Research Security, Joint Committee on the Research Environment, *Guidance for Implementing National Security Presidential Memorandum 33 (NSPM-33) On National Security Strategy for United States Government-Supported Research and Development*, 2022, accessed December 18, 2023, https://www.whitehouse.gov/wp-content/uploads/2022/01/010422-NSPM-33-Implementation-Guidance.pdf. [3]

> and practical experience, which is directed at producing new products or processes or improving existing products or processes.

For conciseness, we define *research* as encompassing all NSF-funded R&D.

Fundamental Research
As defined by National Security Decision Directive (NSDD)-189, *fundamental research* is basic and applied research in science and engineering, the results of which are ordinarily published and shared broadly within the scientific community. Federally funded development work is not formally considered fundamental research as defined by NSDD-189.

Fundamental Research Exclusion (FRE)
The FRE provides that research for which no publication, dissemination, or access restrictions have been accepted is excluded from export control regulations. The exclusion is voided if publication approval is required by the sponsor or the government, or if citizenship-based restrictions have been accepted. The relevant export regulations include Export Administration Regulations (EAR), 15 Code of Federal Regulations (CFR) 734.8(c), and International Traffic in Arms Regulations (ITAR), 22 CFR 120.34(a)(8).

Sensitive and Highly Sensitive Research
A research project is considered *sensitive* if the evolution of the research could feasibly lead to a direct and predictable impact on national security in the future. Research is defined as *highly sensitive* when the release of information about the performance or outcomes can currently be shown to have a significant, direct, and predictable impact on national security. The dividing line between *sensitive* and *highly sensitive* is the difference between the *possibility* of a future impact on national security and the *certainty* of a direct and predictable impact on national security. This is a critical distinction, and it underlies much of the discussion in later sections of this report.

Mitigations
In the context of this report, *mitigations* are any actions taken in the conduct of sensitive research to reduce possible risk to national security. We often use the term *mitigations* to describe actions that do not involve explicit *controls* (see definition for controls).

Controls
In this report, we define *controls* to mean any restrictions on the dissemination of information about performance or outcomes of highly sensitive research. This includes both Controlled Unclassified Information (CUI) and classification, but it can include

restrictions that fall into neither of these categories. Research that requires controls no longer falls within the fundamental research category protected by the FRE (see Section 3.1).

Controlled Unclassified Information (CUI)
The federal directive on implementing CUI (32 CFR 2002) defines CUI as including all unclassified information throughout the executive branch that requires any safeguarding or dissemination control by law, regulation, or government-wide policy.[25] CUI is discussed in detail in Appendix D.

Classification
The system for classification of national security information and for handling of classified information is prescribed in Executive Order 13526. Classification is the most stringent form of control.

3.1 Interrelationships among Definitions

The previous section provided definitions in a form that can be consulted when reading other sections of this report. However, several of the defined terms are interrelated. In this section, we discuss some of those interrelationships.

Sensitive Research and Highly Sensitive Research. *Sensitive research* is research that could likely evolve to have a direct and predictable impact on national security, *but it is not yet sufficiently advanced to know what level of impact it might have in the future*. For this type of research, some degree of risk mitigation is appropriate, but not necessarily formal controls. This research would retain the FRE (see discussion of the FRE later in this section). In contrast, *highly sensitive research* is research that can already be shown to have a direct and predictable impact on national security. For this type of research, formal controls are appropriate. CUI is one type of control, but there are others that may be better suited (see Section 5.1). These formal controls, sometimes referred to as restrictions, void the FRE, with important consequences for researchers.

[25]Note that some categories of information designated as CUI are not sensitive, according to our narrow working definition of sensitivity, which is based on national security impact. However, information in such categories is not relevant to the subject of this report.

Fundamental Research and the Fundamental Research Exclusion. The FRE protects researchers from unintentional export-control violations, allowing researchers to interact and collaborate with, participate in seminars involving, and engage in casual discussions with foreign persons. Critically, these protections allow researchers to publish without obtaining an export license. However, the protections are fragile, and are lost if restrictions are placed on research.

Specifically, the FRE is codified by 22 CFR 120.34(a)(8) and 15 CFR 734.8(c).

The first of these pertains to ITAR restrictions administered by the Department of State, which specify:

> Fundamental research is defined to mean basic and applied research in science and engineering where the resulting information is ordinarily published and shared broadly within the scientific community, as distinguished from research the results of which are restricted for proprietary reasons or specific U.S. Government access and dissemination controls. University research will not be considered fundamental research if:
>
> (i) The University or its researchers accept other restrictions on publication of scientific and technical information resulting from the project or activity; or
>
> (ii) The research is funded by the U.S. Government and specific access and dissemination controls protecting information resulting from the research are applicable.

The second of these pertains to EAR restrictions administered by the Department of Commerce. These state:

> Fundamental research means research in science, engineering, or mathematics, the results of which ordinarily are published and shared broadly within the research community, and for which the researchers have not accepted restrictions[26] for proprietary or national security reasons.

[26]Per this section of the code, pre-publication reviews done to ensure the protection of patent rights or to prevent inadvertent disclosure of proprietary information do not constitute a restriction.

In the United States, the communication of protected technology or software to a foreign national in the United States is deemed to be an export[27] and is a crime under the ITAR and EAR. Here, *technology* is very broadly defined as information[28] necessary for the development, production, or even simply the use of a protected product. Because university researchers routinely interact with foreign nationals in laboratories, classrooms, seminars, and conferences, the risk of an inadvertent export is high. In addition, the loss of the FRE would shut down the free exchange of ideas that is an essential component of the training of scientists. Given these serious consequences, actions that would eliminate the FRE should only be used in cases where the research is deemed *highly sensitive*.

National Security and Economic Security. The NSTC definition of *research security* given above refers to the misappropriation of R&D "to the detriment of national or economic security." In this JASON report, we have addressed the *national defense* aspects of research security, where we have taken national defense to include, for example, research areas identified as important by those federal agencies[29] that address military, intelligence, counterterrorism, space, critical infrastructure, or other aspects of national defense. Our guidance in this report on when and how to apply security-related mitigations and controls to research is limited to national defense and does not necessarily extend to the assessment of economic security.

Clearly, NSF-funded R&D can also be of economic importance. While we did not address economic security per se, a significant fraction of our discussion in Section 4 is relevant to economic assessments, including the life cycle of technology development and the assessment of Technology Readiness Level (TRL).

[27]The term "deemed export" is defined in 15 CFR 734.13 as "Releasing or otherwise transferring *Technology* or source code (but not object code) to a foreign person in the United States." For ITAR, 22 CFR 120.50(a)(2) defines an export to include "Releasing or otherwise transferring technical data to a foreign person in the United States," including, by §120.56(a), "(1) Visual or other inspection by foreign persons of a defense article that reveals technical data to a foreign person; (2) Oral or written exchanges with foreign persons of technical data in the United States or abroad; (3) The use of access information to cause or enable a foreign person, including yourself, to access, view, or possess unencrypted technical data; or (4) The use of access information to cause technical data outside of the United States to be in unencrypted form."

[28]The legal definition expressly includes plans, diagrams, models, formulae, tables, specifications, manuals, instructions, skill training, working knowledge, consulting services, etc.

[29]See the NSF Statement of Work (SOW) in Appendix A, which refers to congressional guidance asking "NSF to collaborate with the Secretary of Defense and the Director of National Intelligence to compile and maintain a list of all NSF-funded open source research capabilities that are known or suspected to have an impact on foreign military operations."

This Page Intentionally Left Blank

4 IDENTIFICATION OF SENSITIVE RESEARCH

JASON defines *sensitive research* to mean research for which the release of information about the performance or outcomes could lead to a significant, direct, and predictable impact on national security (see Section 3 for the precise definition). NSF asked JASON to provide guidance on how to identify sensitive research, including specifically whether the existing guidelines for Controlled Unclassified Information (CUI) provide any useful direction. JASON also reviewed a similar identification effort currently underway at the Department of Energy (DOE). Here, we review these existing programs and then share observations about how basic and applied research eventually generate sensitive technology. From this we lay out guidelines for how NSF might identify sensitive technologies at the right stage in their development so as not to unduly harm U.S. technical competitiveness and national security.

4.1 Existing CUI Categories as a Basis for Identifying Sensitive Technologies

The federal regulations regarding CUI are stated in 32 Code of Federal Regulations (CFR) 2002.[30] As a general matter, these regulations dictate data protections but do not identify types of information that need protection. We considered whether any CUI categories defined elsewhere in law or regulation might themselves bring insight. The National Archives' *CUI Registry* gives the complete list of information categories protectable as CUI. JASON reviewed these but did not identify any existing categories that would give NSF useful guidance. For instance, the category of Specified Controlled Technical Information (CUI//SP-CTI)[31] indicates that it includes "research, studies, and analyses with military or space application," but the registry itself does not provide guidance on how to identify which research might be of concern. We note that the SP-CTI category is not limited to the DOD and could apply to research funded by other agencies, such as NSF. However, documents[32] that attempt to describe SP-CTI within the DOD context do not provide relevant guidance to NSF on what might fall under SP-CTI. More detail about CUI and its utility to NSF can be found in Appendix D. Our finding below responds to Question 2 in the Statement of Work (SOW)—see Appendix A.

[30] 32 CFR Part 2002 - Controlled Unclassified Information (CUI), accessed December 20, 2023, https://www.ecfr.gov/current/title-32/subtitle-B/chapter-XX/part-2002.

[31] National Archives, "CUI Category: Controlled Technical Information," Archives.gov, accessed December 20, 2023, https://www.archives.gov/cui/registry/category-detail/controlled-technical-info.html.

[32] 48 CFR 252.204–7012, DOD Instruction 3200.12, and DOD Manual 5200.001 Version 4.

Finding: The existing categories of Controlled Unclassified Information (CUI) do not provide useful guidance for identifying sensitive research that might be funded by NSF. The CUI guidelines themselves are silent as to what kinds of information need protecting.

4.2 Insights from the Department of Energy

During its study, JASON heard from both the DOD and the DOE concerning their approaches to research security for unclassified research. The DOD policy for risk-based security reviews emphasizes identifying any association of individual principal investigators (PIs) with foreign entities of concern, while the DOE approach emphasizes the identification of critical research areas. We discuss both approaches in Appendix C. Here, we summarize DOE's process for identifying critical technology areas.

Since December 2018, the DOE has been maintaining a matrix of critical technologies associated with economic competitiveness, national security, and scientific leadership. The DOE approach was developed to protect research carried out within the national laboratory system.

Because the national laboratories are already equipped with an extensive security apparatus, the relative cost of implementing additional protections will be lower than for other research institutions. Nevertheless, the DOE's Science and Technology Risk Matrix effort has proven to be a significant undertaking. After being briefed by the DOE on its effort, we concluded that the task of building and maintaining a predetermined list of sensitive technologies in the DOE fashion is possible mainly because each of the national laboratories has a strong DOE-funded research security organization. The workforce needed to create protection guides in broad areas of unclassified science, and to maintain those guides on a regular basis, appears to be similar to the effort needed to define and maintain classification guides. The DOE has such infrastructure as part of its national laboratories. NSF does not.

A consequence of using broad, list-based categories is that the guidance will remain, by necessity, at least somewhat ambiguous. Small changes to the way a research project is presented can influence how it is categorized. For example, some areas of inquiry can be framed as either robotics research or AI research. In one framing, the project is subject to additional controls under the DOE guidelines; and in the other, it is not. Furthermore, the research in broad categories such as "robotics" and "AI" are likely to include large numbers of projects that present no research security risk. This demonstrates the inherent challenge of attempting to pre-organize large swaths

of science and engineering into a neat tree of knowledge, which is a problem that could be avoided by evaluating technologies as they are being developed, instead of depending on predetermined lists. More detail about the DOE program is available in Appendix C.

> **Finding:** The Department of Energy (DOE) approach involves identifying specific critical areas of emerging technologies and utilizing subject matter experts in evaluating the sensitivity of the research. Regular updating and implementation of this scheme is labor intensive.

4.3 How Are Technologies Created?

For all eventually realized technologies—sensitive and otherwise—there is first an incubation period in which insights and knowledge rooted in basic research grow. This is followed by one or more takeoff periods in which early expectations are tested and, if promising, developed into *application concepts*. If the application concepts are promising, this is followed by a maturation period during which it takes significantly more work to render each application concept into a practical technology.

This sequence can be presented as an "S-curve"[33] (see Figure 4). In the fundamental research stages, open conversation is of significant value. First, the design and testing of each proposed application crucially depends on a community effort to scrutinize the idea's potential, identify shortcomings, and recognize deal-breakers that would ultimately limit the concept's viability. As a result, there are innumerable nascent technologies that were initially hoped to be on a fast trajectory to maturation but for which development efforts pivoted away following open discussion. Second, open research catalyzes other innovations that may ultimately have significant impact of their own. Such innovations can cause seemingly unrelated and mature technologies to be reinvented long after the original concept was considered to have reached maturity. For example, the invention of multi-touch technologies inspired the reinvention of the telephone into the smartphone. Initially, new technologies often underperform, compared to incumbent technologies, but ultimately chart their own independent curve that overtakes the incumbent technology due to improved functionality. This web of innovation depends critically on the free sharing of ideas.

As a result of this disruptive process, a basic-science effort (as is routinely funded by NSF) may spawn many unforeseen application concepts. Equally, real-world chal-

[33] Richard N. Foster, "Working The S-Curve: Assessing Technological Threats," *Research Management* 29, no. 4, (1986): 17-20, DOI: 10.1080/00345334.1986.11756976. [18]

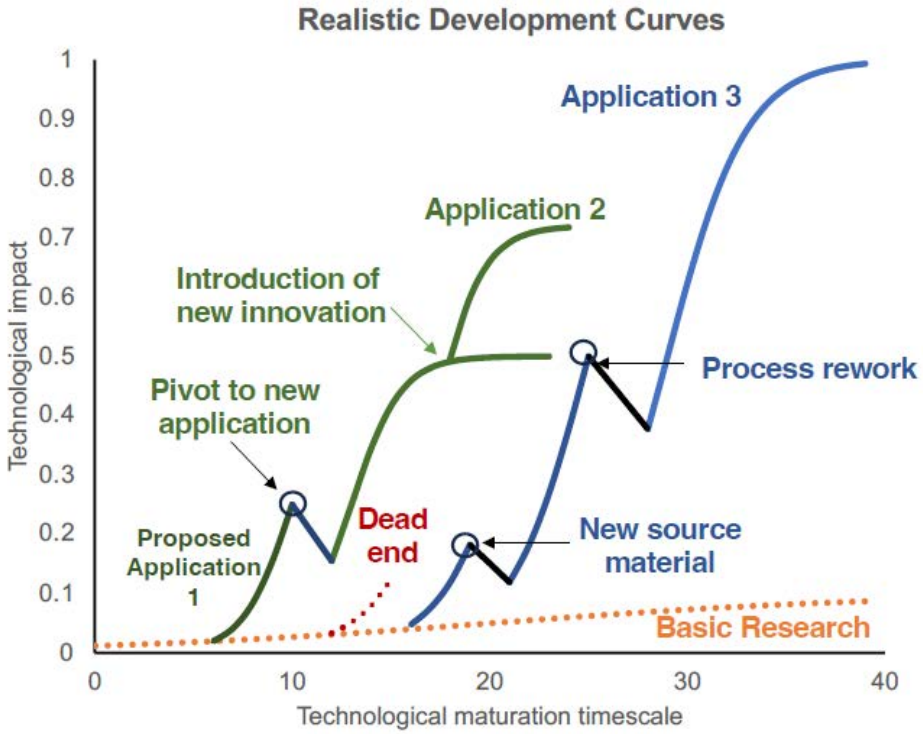

Figure 4: Basic science programs are likely to incubate and then support the takeoff of a number of applications of varying unpredictable growth curves and impact areas, typically illustrated as S-curves. Realistic technological impact curves are discontinuous and illustrate the importance of techno-economic factors on the translation of research concepts into applications. Early-stage exploration will spawn many application concepts, with variable potential impacts. Each concept will in turn be tested for technical success, as well as practical factors such as market scale, cost, supply chain, scale-up, and production feasibility. As concepts evolve, most will fail or pivot to a new application at some stage of development. These curves are rarely continuous, as impediments must be faced and overcome (black lines). Occasionally, new insights catalyze acceleration (or deceleration, as illustrated by varying takeoff points).

lenges can force pivots and reinventions away from the originally envisaged concept. These are notionally illustrated in Figure 4 as S-curves of different colors taking off from a single basic research trajectory. Many concepts fail (represented by a curve that ends abruptly), frequently subsequent to open discussion in the scientific community. Other concepts pause, backtrack, or pivot to a new or modified application at some stage of development, as hurdles are faced and overcome (represented by discontinuities in each of the curves). The timeline for overcoming such hurdles is unpredictable and may take weeks or decades.

For a real-world example in a research area that includes national security–sensitive

technologies, consider the basic science associated with directing the propagation of electromagnetic energy through materials (akin to the orange line in Figure 4). This fundamental research area has spawned many application concepts, such as electromagnetic bandgap structures in split-ring resonators for RF/microwave application, and optical-fiber waveguides. Some were readily successful, such as fiber-optic telecommunications (akin to the green curve). However, other early concepts ran into scaling and manufacturing concerns. The use of metastructured materials for invisibility cloaks[34] is one such example. Had it worked, it would have had obvious national security applications. While macroscopic invisibility cloaks proved unfeasible, such research nevertheless contributed to the foundation (orange line) on which still other technologies of great significance were ultimately realized[35]: the computational packages and patterning schemes needed to form negative-refractive-index materials for invisibility cloaks helped propel the development of metastructured antennae that allowed for effective phase compensation in 5G cellphone radios. The essential insight here is that the premature sequestering of research into a closed setting can significantly slow the development of valuable technologies while also permitting nonviable concepts to persist and consume economic resources longer than they should—both effects that have a negative impact on national security. In relation to Question 5 of the SOW (see Appendix A), this last insight provides a compelling example of the potential negative consequences of unwise decisions regarding research controls.

As technologies become more refined, the work done in support of those refinements becomes increasingly application specific. For many national security–sensitive technologies, a point eventually comes where the balance shifts in favor of protecting those developments because their less-fundamental nature means fewer opportunities to spawn new application concepts in unrelated spaces. Identification of research occurring in these late stages can be facilitated using the well-established framework of Technology Readiness Levels (TRLs).

> **Finding:** At early stages of research, the potential applications' outcomes are notional. Most commonly, highly ambitious potential applications postulated for early-stage research are later replaced with different potential applications, addressing a range of societal, commercial, and national security needs as the research area progresses in technical maturity.

[34] Tolga Ergin et al., "Three-Dimensional Invisibility Cloak at Optical Wavelengths," *Science* 328, no. 5976, (2018): 337-339, accessed December 20, 2023, https://www.science.org/doi/10.1126/science.1186351. [19]

[35] Josh Jacobs, "'Invisibility Cloak' Metamaterials Make Their Way Into Products," *Financial Times*, (2018), accessed December 21, 2023, https://www.ft.com/content/c6864c76-de7d-11e7-a0d4-0944c5f49e46. [20]

4.4 The Utility of Technology Readiness Levels

Technology maturity can be quantified using the framework of TRLs, which can be helpful for guiding NSF in identifying when a concept has reached a state of maturity such that the balance of considerations suggests that national security might be better served by imposing extra mitigations and controls than by maintaining openness. For NSF's purposes, a broad, domain-neutral scheme is needed. For illustrative purposes, we adopted the scheme shown in Table 1.[36]

Technology Development Stage	TRL	Definition
Fundamental Research	1	Basic principles observed and reported
	2	Technology and/or application concept formulated
Research and Development	3	Experimental proof of concept
	4	Validation of component(s) in a laboratory environment
	5	Validation of semi-integrated component(s) in a simulated environment
Pilot and Demonstration	6	System and/or process prototype demonstrated in a simulated environment
	7	Prototype system ready (form, fit and function) demonstrated in an appropriate operational environment
	8	Actual technology completed and qualified through tests and demonstrations
Early Adoption	9	Actual technology proven through successful deployment in an operational environment
Commercially Available		Technology development is complete

Table 1: TRLs suitable for broad research areas such as those at NSF. See footnote 36.

The earliest stage of research, TRL 1, is exploratory. Possible applications are often hypothesized at this stage, sometime generating a large amount of interest (e.g., high-temperature superconductors in the late 1980s) that is later tempered by further basic and applied research. The types of exploration are defined by the nature of the field and subfield. From TRL 1 work, which postulates and tests the fundamental principles of the field, will spring—at different times—pathways to different potential applications that are explored in TRL 2 and tested for basic feasibility in TRLs 3 and

[36]Government of Canada, "Technology Readiness Level (TRL) Assessment Tool," 2021, https://ised-isde.canada.ca/site/clean-growth-hub/en/technology-readiness-level-trl-assessment-tool. This is nearly identical to that used by the DOD, "Technology Readiness Levels in the Department of Defense (DoD)" in *Defense Acquisition Guidebook*, 2010, accessed December 21, 2023, https://api.army.mil/e2/c/downloads/404585.pdf.

4. As the emerging technologies move into validation stages at TRLs 4 and 5, practical issues such as the cost of the notional technology, the feasibility of manufacturing the technology reliably and at scale, and integration of the technology with other systems or environments, begin to impose substantial changes on the technical approach.

Generally, significant resources must be invested to move technologies from the R&D phase into the pilot and demonstration phase. Any organization that has assessed the outcomes of early-stage research will still need to make considerable investments to bring the work to a high TRL stage. This creates a natural barrier between the concept phase and the practical technology phase, where technologies begin to have demonstrable economic or national security significance. The key insight here is that while national security–sensitive concepts may seem apparent as early as TRLs 1 and 2, those concepts are subject to changes in approach and direction, and will likely require significant investments to mature before they transition to TRLs 5 and 6, where the actual national security significance can be demonstrated.

> **Finding:** The concept of Technology Readiness Level (TRL) is an essential component of the review to determine whether research is sensitive from a national security perspective.

4.5 Evaluating National Security Significance

In a national security evaluation, the designation of broad fields or sub-fields as sensitive or highly sensitive is problematic. Each field organizes itself in a different way, depending on history, funding, and culture. For example, quantum information science encompasses a range of work, such as materials science, device physics, and theoretical physics. Each sub-field has many different thrusts. Just choosing quantum sensors will still capture a spectrum of devices—gravitometers, plasmonic sensors, high-precision clocks, and so on—and each of those sub-sub-fields will have theory and multiple technical approaches at different TRLs, and with potentially entirely different national security impacts. Specific *projects* may need control, rather than their parent sub-fields.

> **Finding:** Differentiation between sensitive and non-sensitive research is most natural at the project level, not at the sub-field level. Projects in the same sub-field can have very different levels of risk.

A high TRL is not by itself a necessary or sufficient basis for deciding whether a research program merits additional mitigations or controls. The technology under

development must have national security significance, and the international state of R&D must be such that the applied protections would benefit U.S. national security. There might also be rare instances where fundamental research at low TRLs should be protected because of exceptional national security significance.

In deciding whether a technology has significant national security impact, NSF should consider the national security application goals, as well as any applications other than national security. If the development is aimed at an application outside national security, then NSF needs to consider whether the national security aspects are of such import that the need for protection overrides the social benefit of the non-national-security application. For example, a novel seismic monitoring system might improve the ability to characterize a country's explosive weapons testing, but NSF should ask whether the national security benefit of applying research controls to this research outweighs the benefit of developing capabilities that help mitigate earthquake hazards.

When reviewing these considerations, NSF should ask whether the technology is *sufficient and unique* for the national security use case in mind. It does not make sense to control emerging technologies, even at high TRLs, if they are not particularly suited to a national security use case. For example, precision clocks have national security applications, but precision is not by itself sufficient to constitute a national security concern; other factors such as low energy requirements and low physical volume must also be met before the clock becomes national security–sensitive.

Finally, before imposing any mitigations or controls, NSF needs to consider whether doing so would confer a meaningful advantage to the United States. In some domains of research, the United States might not be the leader, in which case international cooperation has the potential to elevate U.S. capabilities. In other cases, competition between the United States and a foreign country might be "neck and neck," in which case NSF should consider whether imposing the burden of security restrictions on U.S. researchers might slow the pace of U.S. innovation relative to foreign competitors. Mitigations and controls make the most sense when the United States has a definitive advantage and so can endure the burden of these protections without negatively impacting the country's relative position.

Overall, the discussion in this section sets the basis, further developed in Sections 5.1 and 6, of our response to Question 1 of the SOW (see Appendix A).

> **Finding:** Risk mitigation must consider the spectrum of risk and be adaptable to changing trends in research. Resources should be concentrated on areas of maximum risk to ensure that benefits outweigh the costs.

Recommendation: NSF should adopt a dynamic approach for identifying potentially sensitive research topics as they arise, instead of attempting to maintain a comprehensive list of sensitive research areas. NSF's process of identifying sensitive research projects should:

- Differentiate research projects based on the sensitivity of their potential applications,
- Include the maturity of the development path (Technology Readiness Level—TRL) for potential applications in the assessment of risk, and
- Include an assessment of the direct and predictable national security impact of the applications of each research proposal, if successful.

This Page Intentionally Left Blank

5 RISK MITIGATION STRATEGIES FOR NSF

5.1 Mitigations and Controls

Figure 5 visualizes the range in mitigations and controls, depending on research sensitivity: no mitigation for most basic research; mitigations for *sensitive* research; controls for *highly sensitive* research—those areas for which the fundamental research exclusion (FRE) should no longer apply; Controlled Unclassified Information (CUI) controls as a subset of controls; and, finally, classification.

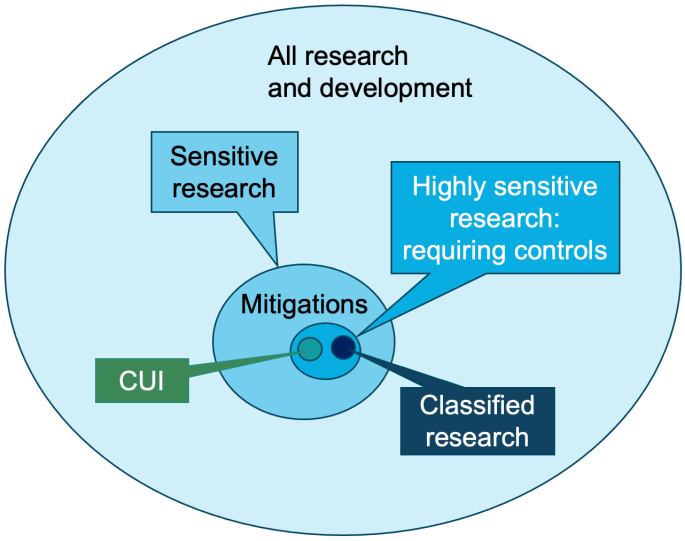

Figure 5: Categorization of NSF-funded research in terms of actions required to address sensitivity. *Sensitive* research generally requires mitigation measures—actions taken to protect sensitive research. *Highly sensitive* research generally requires controls; and for this category of research, the FRE does not apply. CUI and classified research are subcategories of controlled information. The areas of the research types depicted in the figure are not intended to be to scale. The fraction of NSF-funded academic research expected to be sensitive is small, and the fraction that is highly sensitive, even smaller.

A menu of possible mitigations and controls that provide a spectrum of protections, depending on the sensitivity of the research, follows. We recommend that NSF evaluate which of these mitigations or controls is appropriate on a project-by-project basis (see Section 6.1.1).

Mitigations Appropriate for Sensitive Research (FRE applies)

Possible mitigations include:

- Changes to the scope of a research grant,
- Training (or enhanced training) of the principal investigator (PI) on research security risk and protections,
- Enhanced training regarding publication of potentially sensitive results,
- Enhanced training on identifying individuals of concern who might be considered as possible participants or collaborators,
- Increased frequency or scope of reporting,
- Physical security standards for laboratories or computational facilities, and
- Cybersecurity standards for laboratory control systems or computing systems.

Controls for Highly Sensitive Research (FRE no longer applies)

Any of the above mitigations *plus* one or more of the following:

- Restrictions on participation for individuals of concern,
- Mandatory pre-approval for conferences or publication,
- Mandatory pre-approval before posting open-source data or software,
- CUI-like protections (see Appendix D and Section 5.2), and/or
- Funding contingent on accepting classification under Executive Order 13526.

Mitigations. In the case of *mitigations* for sensitive research, changes to the scope of a research grant are an easy way to limit potential accidental connections to sensitive topics. Training in research security awareness can be effective in helping reduce intellectual theft and ensuring that the benefits of research convey appropriately to U.S. entities. Such training will already be required per §10634 of the CHIPS and Science Act; but, in some cases, enhanced training focused on specific sensitivities

or extant compliance requirements may be valuable. Increased frequency or scope of reporting provides the opportunity for an NSF program officer to discuss aspects of sensitivity with the PI, as well as to get an update from the PI regarding evolution of the research toward possible applications. Finally, standards on physical security and cybersecurity are meant to prevent theft of valuable research results while not impeding the access of the researchers involved.

Controls. Any controls placed on research by NSF must be formally written as provisions in the grant or contract language accompanying the funding of the research. This is because controls and restrictions can place additional legal obligations on researchers that may require legal assistance and special training. In particular, acceptance of controls or restrictions voids the FRE, as explained in the definition of the FRE provided in Section 3 and discussed further in Section 5.3. Such controls should be reserved for highly sensitive research projects and include restrictions on participation of individuals and mandatory pre-approval of information dissemination. CUI is a type of control, but we judge its effectiveness to be limited (see Section 5.2 and Section D.5).

An alternative to imposition of controls by NSF is for NSF to simply not fund the research, or to refer the research to a more relevant funding agency—for example, the DOD. In some cases, this might be the most prudent action for NSF.

5.2 CUI as a Category of Research Control

NSF asked JASON, "What processes and restrictions might be implemented to carry out research that falls within the NSF-designated CUI category?" While CUI controls may be appropriate for some research areas of particularly high sensitivity and risk, CUI is generally a rather blunt and ineffective tool for addressing the broad issue of U.S. research security. CUI should not be used as a one-size-fits-all a pproach to mitigating research risk.

As explained in Section 4.1, adequate protection of national security–sensitive information using CUI might require the definition of a new CUI-specified category defined by law, regulation, or government-wide policy. Regardless, all au-thorized holders of any type of CUI must:

- Establish controlled environments;
- Prevent unauthorized individuals from overhearing or observing CUI;

- Require direct control or physical barriers to CUI;
- Use only printers, copiers, and scanners that do not retain data;
- Delete electronic data in a method that makes the data irrecoverable; and
- Store, transmit, and process data only on information systems meeting the National Institute of Standards and Technology (NIST) SP 800-171 standard, which outlines 110 computer security provisions that must be satisfied.

The supporting apparatus for CUI-style access controls would impose significant cost on the conduct of research and reduce research funding efficiency.

In addition, we note that any access control is directly in conflict with the formal provisions of equal access to research that are in place at many universities. Such controls would disadvantage students involved with a controlled project by denying them the opportunity to engage in the free exchange of ideas, peer review, and practice at science communication. These activities are central to a student's education as scientist or engineer. As such, these controls compromise the educational mission of universities and NSF, and their necessity should be weighed against this cost.

Such controls would additionally impede creativity and innovation in the protected sectors. President Reagan's National Security Decision Directive (NSDD)-189 states that "an environment [with] the free exchange of ideas is a vital component" of academic research, and that such openness is therefore "an essential element in our physical and national security."[37] Slowing research in areas of national interest would impose a national security cost. Such negatives must be weighed against the benefit of preventing the controlled information from potentially leaking to foreign nations, realizing that if an adversarial peer country is determined to acquire the protected information, the controls are unlikely to stop them.

> **Finding:** Access controls create hindrances for education, the progress of science, and national security. These must be weighed against hypothesized gains in preventing information transfer, especially in the context of a sophisticated and determined adversary.

> **Finding:** CUI-required security controls could lead to increased cost of doing research, with a resulting loss in research efficiency.

[37] Office of the President of the United States, *National Policy on Transfer of Scientific, Technical and Engineering Information*. National Security Decision Directive 189. September 21, 1985, accessed December 21, 2023, https://catalog.archives.gov/id/6879779.

5.3 Consequences of Controls

NSF asked JASON, "What are some of the potential impacts on the research community should some NSF-funded research areas be designated as areas of concern?" We discuss these impacts here.

Loss of the Fundamental Research Exclusion (FRE). Given its importance, we discussed loss of the FRE earlier (see Section 3.1). This has a definite impact on those research areas designated as highly sensitive, putting researchers under legal obligation to prevent dissemination of the results of research to foreign nationals. This will be incompatible with the normal open discussion and exchange of ideas within universities. Some universities have stated their intent not to accept research funding with CUI or other controls because of this incompatibility.

Increased Cost of Research. Protecting controlled research may require financial resources, and thus increase the cost of doing research. For instance, holders of CUI-designated information will need to comply with numerous requirements including those for physical safeguarding of documents and equipment, as well as strict requirements concerning computer storage, transmission, processing, and cybersecurity (see Section D.5 for details). Facilities for proper handling of CUI-designated information will be a significant cost to the NSF grant or the performing institution. There is a risk that only a subset of research institutions can or will accommodate the increased security overhead required for controlled research projects.

Reducing the Number of U.S. Research Organizations Engaging in Fundamental Research Important to National Defense. It is highly desirable that the United States have strong fundamental research in areas that underpin technologies important to national defense. If a significant number of U.S. research organizations decide not to accept research funding that entails controls such as CUI, that will decrease the U.S. research base in those areas. As mentioned, some research institutions have already expressed their intent not to accept research funding with CUI controls. Other research institutions may not be able to participate in controlled research because of the increased overhead of implementing and maintaining facilities needed to handle protected equipment and information.

Shrinking the Talent Pipeline. Research with CUI and other export controls will limit participation of foreign nationals, regardless of their country of origin. NSF funding supports, both directly and indirectly, a significant fraction of advanced degree education in the United States, including the M.S. and PhD degrees of many foreign nationals studying in the United States. Many of these students remain in the United States after their degrees, contributing to the strength of the U.S. R&D effort,

with many becoming citizens. For its own sake, the United States should avoid the risk of creating an impression that it is not a welcoming place for foreign students.

Inhibiting Competitive Development of New Technologies. Open research is recognized as accelerating development of technology through competition, exchange of ideas via publication, and cross-fertilization of different research areas. Controls on dissemination of the results of research could slow the pace of innovation in areas of emerging technology where diversity of thought and active debate are most important. Because many technologies are dual-use, there also could be negative economic impacts. One other aspect is the potential limitation in the number of researchers who can participate in peer review of a controlled area of research. NSF depends on high-quality peer review for evaluation and selection of much of its research.

Possible Increased Bureaucratic Overhead at NSF. NSF is recognized as maintaining a relatively low in-house bureaucratic overhead. It does this through grants, contracts, and cooperative agreements to external organizations who then carry out the desired work. NSF follows this mode in the research security arena, for instance through its outsourcing of the development of training materials for research security (NSF Program Solicitation, NSF 22-276) and its recent solicitation for a Research Security and Integrity Information Center (NSF Program Solicitation, NSF 23-163). We commend NSF for these approaches, which allow NSF to address substantive issues in research security without building a large in-house organization.

The project-oriented identification and mitigation of research risk suggested for NSF in this report (see Section 6.1.1) must be carefully implemented so as not to produce an in-house bureaucracy centered around research security compliance. We note that NSF already has training programs for its staff in research security,[38] and it could build on these to implement the project-oriented research security approach recommended.

> **Finding:** Formal controls on research, such as a CUI designation, will have unintended consequences, including: increasing the cost of doing research, diverting resources better applied to expanding U.S. research efforts in critical fields, inhibiting rigorous and competitive development of new technologies, and discouraging some individuals and research organizations from engaging in U.S. research.

[38]NSF, Office of the Chief of Research Security Strategy and Policy, "Research Security at the National Science Foundation—NSF Policies and Action," accessed December 21, 2023, https://new.nsf.gov/research-security#policies.

Recommendation: NSF should proceed with caution before adding access or dissemination controls to grants or contracts. In considering whether to apply formal controls to a sensitive research project, NSF should weigh the balance between the positive protective benefits and the unintended negative consequences of such controls. Controls can protect U.S. national security by preventing malign use of research results, but they can also hinder the beneficial free flow of research results in a way that negatively impacts broader U.S. economic and national security interests.

This Page Intentionally Left Blank

6 A NATIONAL SCIENCE FOUNDATION APPROACH TO RESEARCH SECURITY

In this section, we put forth a framework for NSF to adjudicate research proposals that may enter the realm of sensitive or highly sensitive research. Our framework aims to integrate research security seamlessly with the overall proposal process. NSF has a strong history of effective proposal review, and we want that to continue, while also meeting the needs of research security. We start with the notion that a research project, rather than a research sub-field, presents the best basis for assessing risk to national security. Because NSF supports proposals that consist of research projects, reviewing a project offers a natural basis for this type of review and further action.

NSF asks its proposers to comment on the Broader Impacts[39] of their proposal, allowing them to provide information on the impact the proposed work may have beyond advancing the field. The Broader Impacts statement provides a natural place for NSF to solicit comments from the principal investigator (PI) on possible impacts on national security.[40]

The next section outlines an implementation approach that JASON recommends to NSF to ensure research security. Section 6.2, then, considers the role the universities and other research organizations can play in protecting national security without compromising their ability to carry out their mission. Section 6.3 describes proactive measures NSF, researchers, and universities can take to bolster U.S. national security, while still allowing open communication among researchers.

6.1 A Research Security Approach Tailored to NSF

Our investigations revealed the need for each agency to develop its own approach to protecting sensitive, unclassified information, which should reflect the agency's goals and missions (see Appendix C for a description of the approaches of other agencies). NSF has its own culture, procedures, and community. In particular:

[39] NSF, "Broader Impacts," https://new.nsf.gov/funding/learn/broader-impacts, accessed December 21, 2023.

[40] NSF, *Proposal & Award Policies & Procedures Guide (PAPPG), NSF 23-1* already lists "improved national security" in Chapter 2: Proposal Preparation Instructions, Part D Proposal Contents, 2023, accessed December 21, 2023, https://new.nsf.gov/policies/pappg/23-1/ch-2-proposal-preparation#2D2di). [21]

- A very large fraction of the research funded by NSF can be considered fundamental. Even within NSF's Directorate for Technology, Innovation, and Partnerships (TIP), a very small portion of research will ultimately be sensitive or highly sensitive.
- Unlike other U.S. R&D agencies, NSF does not manage laboratories that carry out research.[41] Rather, it funds research primarily through grants and contracts to outside organizations, mostly at universities or consortia of universities, with a broad range of capacities and missions.
- NSF funding is primarily awarded in response to proposals.
- NSF is extensively involved in international collaborations and is one of the principal U.S. agencies for funding of beneficial collaborations with foreign partners.
- Much of the NSF-funded research community is likely not aware of the full extent of research security concerns.

We considered the above points in formulating our specific recommendations.

6.1.1 A Proposal-Driven Approach

NSF responds primarily to proposals from university-based investigators, frequently with a single investigator who may have grants from several sources, or a group of investigators in a collaborative center. An NSF grant will typically run 3 to 5 years, and renewal remains competitive. While NSF program officers follow the work of those they fund, they usually do not exert supervisory control over their grantees' work.[42] They do receive an annual report of the PI's work on the award. The proposal cycle, including both the submission of a proposal and any subsequent review, provides the best, and perhaps only, opportunity to gain adequate insight into a project to determine whether that project entails sensitive research. Imposing substantial changes could require the creation of a new system within NSF, potentially adding to NSF's overhead. However, given the typical time and effort needed for a technology to move

[41] NSF funds 18 major scientific research facilities, such as the U.S. South Pole Station and the U.S. Academic Research Fleet, where NSF retains discretion as to the scope of research carried out; however, for the most part, NSF does not direct research at these facilities. Research security for these large NSF facilities is a separate topic, not addressed in this report.

[42] The NSF *PAPPG* does not require any annual reporting of the progress of funded work, although it does encourage regular contact between the program officer and awardee. See Chapter 7: Award Administration, A. Monitoring Project Performance, in *PAPPG, NSF 23-1*, 2023, accessed December 21, 2023, https://new.nsf.gov/policies/pappg/23-1/ch-7-award-administration#7A1. [21]

from application concept to maturity, we assess that reviewing sponsored work on a 3- to 5-year basis provides a good starting point.

> **Finding:** The NSF proposal and reporting cycle provides the most natural means for identifying sensitive projects—i.e., those projects for which the release of information about research execution or outcomes could have a significant, direct, and predictable impact on national security.
>
> **Recommendation:** The identification of sensitive projects proposed to NSF occurs most naturally before peer or panel review. We recommend that the principal investigator (PI) and the NSF program officer, with guidance from the NSF Division Office, determine if a proposal constitutes a sensitive project. NSF may wish to implement a pilot program within some division of NSF to gain experience with the process. NSF should consult with other federal research funding agencies such as the Department of Energy (DOE), the National Institutes of Health (NIH), and the Department of Defense (DOD) to help identify sensitive research.

JASON recognizes that NSF does not currently have the in-house national security expertise to implement the preceding recommendation across all its relevant programs. Building up the requisite knowledge and expertise will be a long-term endeavor over several years. However, JASON believes that to address research security effectively, NSF *must* work toward developing an in-house culture of research security awareness and developing sufficient in-house expertise to be able to identify sensitive research. NSF could also consult with external experts to aid in its evaluation. Because of its unique portfolio of funded research, NSF is in the best position to assess on a project-by-project basis which projects might include sensitive or highly sensitive research.

> **Finding:** In order to effectively evaluate proposed research for potential sensitivity, NSF will need to develop in-house national security expertise. NSF staff with appropriate expertise would serve as consultants to support the review process.

JASON finds that the present NSF proposal-review process would work well for the purpose of identification of sensitive projects, although some modifications will be needed. Below, we describe the elements needed to add a process for identifying and adjudicating support for sensitive or highly sensitive projects without hampering the overall proposal process.

Each NSF division should develop standard guidelines about potential national security implications in its research areas to facilitate an earnest self-assessment by the

PIs. NSF should provide the tools and guidance to enable researchers to perform the assessment with minimal time burden to the research community.

We emphasize that the proposal-driven approach we recommend is quite different from the list-based approach that JASON was asked to comment on in the Statement of Work (SOW) from NSF (see Appendix A). Relying on lists of broad research areas of possible concern will be inadequate for reliably identifying specific research projects that are sensitive or highly sensitive. To be effective, the lists of sensitive research areas would need to be so granular and detailed as to be unwieldy. Such an approach would thus require a large effort to develop, approve, maintain, and update these lists across the agency. We therefore recommend a *process* for NSF to identify sensitive research, rather than a list-based approach. We describe this process next.

6.1.2 Initial PI Evaluation

The suggested process starts with a self-evaluation by the project's PI at the time the proposal is submitted. Typically, the PI understands the research better than anyone else, and NSF should take advantage of this knowledge, while also recognizing that self-evaluation is not by itself sufficient.

As part of preparing materials for submission, the PI would be asked to list the expected outcomes or applications of the research. We suggest NSF ask the PI to state whether, in their view, the proposed project has potential national security impact based on guidelines NSF would develop. If the PI marks the project as potentially sensitive, the PI should be asked to provide the following information:

- The intended use (if any) of the results of the project;
- The Technology Readiness Level (TRL) of the work initially, and that expected at the end of the project; and
- Whether the technology has features that create national security impact beyond that of technology already discussed in the open literature.

PIs will need guidance on how to assess their proposals. Only a small percent of projects will lie close to sensitive or highly sensitive research. In the large majority of non-sensitive cases, the PIs need only provide a sentence or two about why their project does not have national security sensitivity based on the NSF-developed guidelines.

Recommendation: JASON recommends NSF develop language for the *Proposal & Award Policies & Procedures Guide (PAPPG)* to help PIs assess their proposed projects for possible impact on national security, including providing guidelines on what may, or may not, constitute research with potential national security impact.

6.1.3 NSF Review

Upon receiving a proposal, regardless of how it is marked by the PI, the NSF program officer (or designee) should review the researcher's evaluation of potential sensitivity and formulate their own assessment. At this step, the program officer must decide whether to request the information above, if it has not already been provided in the PI's self-assessment. If the proposed research is not deemed sensitive, the program officer will move it through the review process as normal. If the proposed research is considered to constitute a potentially sensitive or highly sensitive project, the NSF division, NSF program, and perhaps the PI will have to work together to have the proposal appropriately reviewed. JASON recommends that NSF appoint a group of NSF staff with national security expertise to support such reviews in concert with the program officer, the division director, and others in NSF. This in-house group could also serve as consultants later in the process. The final decision about supporting any proposal must lie with the chain of command within the division—as it does now. Those providing national security expertise remain as advisors, not as reviewers.

Finding: Initial assessment by the principal investigator (PI), with review by the NSF program office (and perhaps the NSF parent division), provides the best screening for potentially sensitivite or highly sensitive proposals—i.e., those that may need mitigations or controls.

The primary criterion for risk should be whether the research will have significant, direct, and predictable impact on national security.

Recommendation: Specific mitigation strategies for sensitive research projects should be negotiated and agreed upon by the principal investigator (PI), NSF, and the sponsored projects office of the institution accepting responsibility for execution of the research. Specific mitigation steps should be proportionate to the assessed risk, relative to the associated costs.

6.1.4 Protecting Sensitive Projects

If a project involving sensitive or highly sensitive research is selected for potential funding, NSF will have to determine a mitigation plan with the research institution and the PI. Owing to the broad spectrum of work supported by NSF, specific mitigations or controls for sensitive or highly sensitive projects must be determined on a case-by-case basis. NSF's in-house national security experts can help guide the selection of appropriate mitigations or controls. Ultimately, though, all stakeholders—the PI, NSF program officer, and the institution's sponsored program office—must agree upon an appropriate way forward with the project. Any controls placed on the research by NSF must be formally written as provisions in the grant or contract language accompanying the research funding. The specific mitigations or controls applied should be based on an evaluation of relative benefits and drawbacks of applying such protections. Possible mitigations and controls, and their consequences, are discussed in Section 5.1. During this review, considerations should include:

- How the intended, or realistically foreseeable, uses of the technology might impact U.S. national security.
- The relative stage of advancement of the United States versus other countries in the research area.
- The impact of restrictions on the ability of some researchers to work on the project.
- The impact controls on communication of results of the research may have on the PI's ability to successfully carry out the research, and on the community at large.
- Additional costs, financial and otherwise, of the proposed mitigations or controls.

NSF might consider the formation of divisional boards for the purpose of assessing the risk associated with research activities proposed by PIs funded by NSF, perhaps in affiliation with other government agencies. These divisional boards would work cooperatively with university administration and proposers to determine, based on technical assessments, whether proposed research poses risk so as to be subject to restrictions currently being codified to enforce research security.

6.2 The Role of Research Institutions Such as Universities

NSF funds research institutions, such as universities, to carry out much of the research it supports. Consequently, research institutions and their PIs will be responsible for the actual implementation of research security measures. Their role will be critical. Research institutions have several responsibilities in the research security process, including:

- Working with NSF and other agencies to provide input on proposed research security guidelines and requirements.
- Ensuring that researchers at their institutions working in areas of sensitive or highly sensitive research are informed and trained in research security awareness.
- Understanding and signing off on research security guidelines and requirements in federal grants and contracts.
- Ensuring compliance with research security actions.

Finding: Research institutions and NSF have key roles to play in the process of risk identification and management. Dialogue between NSF and research institutions such as universities is critical.

Recommendation: The NSF Office of Research Security should initiate meetings and forums with universities to discuss its plans for research security and to solicit input and feedback on its procedures once they begin to be implemented. This can begin now with respect to research security training modules being developed by NSF. If NSF initiates a pilot program for the identification of sensitive or highly sensitive research and its mitigation and control, feedback from universities will be vital for tuning the program for wider implementation across the entire scope of NSF-funded research.

6.3 Proactive Steps

So far, our discussion has focused primarily on *protective* steps to enhance research security. Protective steps are aimed at lowering the risk that critical technology will be appropriated and exploited by foreign countries. However, protective steps are insufficient to address the issue of maintaining U.S. leadership in critical technology

areas. We therefore discuss several *proactive* steps to enhance the capabilities of the U.S. research enterprise in the interests of national security.

Building a Culture of Research Security Awareness.
Research security will be enhanced if individuals in the research community are aware both of the importance of research security and of the risks to that security that may exist in the research environment. Most individuals in the U.S. academic research community are relatively unaware of both the importance and the full extent of research security risks. Consequently, building a culture of awareness of research security in the United States will be a long-term, non-trivial task. However, it is JASON's view that researchers receiving federal funding for their work have a responsibility to protect the interests of the United States; therefore, it is incumbent on universities and NSF to foster an awareness of security issues related to research.

> **Finding:** Awareness of research security issues among university researchers is lower than warranted at present, but approaches are available to raise the awareness level, and such steps are mandated under the CHIPS and Science Act.

> **Recommendation:** NSF should foster a culture of research security awareness by providing substantive information to researchers about real risks, making resources available for researchers to voluntarily seek guidance, and continuously engaging with researchers and their institutions about the efficacy of research risk mitigation and control efforts.

A researcher working in a potentially sensitive area of research will be faced with numerous questions: Should I hesitate to publish these research findings? Should I work with this other individual on this sensitive research? Whom should I consult if I am not sure? These are not trivial questions, and intentional, proactive steps are needed to encourage academic practitioners to adopt behaviors that serve, collectively and over time, to reduce the probability and severity of adverse outcomes.

There is extensive literature on how to shape *safety* culture within organizations (see Uttal, 1983 [22]; and Reason, 1990, 1997, and 1998 [23, 24, 25]). While building a research security culture will be different from shaping a safety culture, there are many common considerations. The published work on security culture is less academic and more focused on best practices. Recurring themes include: risk awareness; simple, uniform, and transparent policies; security assessment; positive incentives; and communication of security priorities by leadership.

Translated into actionable steps, these themes could include:

- Designing security procedures in such a way that researchers understand what is being protected and how to implement the procedures effectively.
- Providing researchers with substantive information and examples concerning real risks.
- Providing resources for researchers to ask for research security guidance.
- Providing researchers a confidential mechanism to report concerns ("if you see something, say something"). Researchers will need to understand that their concerns will not result in bias against, or profiling of, colleagues.

We note that the CHIPS and Science Act[43] mandates that NSF establish a research security and integrity information sharing analysis organization (RSI-ISAO). The responsibilities specified for this organization in the CHIPS and Science Act include:

- "Serve as a clearinghouse for information to help enable the members and other entities in the research community to understand the context of their research and identify improper or illegal efforts by foreign entities to obtain research results, know how, materials, and intellectual property"
- "Develop a set of standard risk assessment frameworks and best practices, relevant to the research community, to assess research security risks in different contexts"
- "Share information concerning security threats and lessons learned from protection and response efforts through forums and other forms of communication"
- "Provide training and support, including through webinars, for relevant faculty and staff employed by institutions of higher education on topics relevant to research security risks and response"

Finding: Properly implemented, a research security and integrity information sharing analysis organization (RSI-ISAO) of the type described in the CHIPS and Science Act would be a proactive step toward ensuring the security of the U.S. research enterprise and would provide tools and support for the development of a culture of awareness for research security.

[43] CHIPS and Science Act, Section 10338(b).

We further note that the CHIPS and Science Act[44] also mandates a security training requirement for federal research award personnel. Security training modules[45] can be one component of a toolkit for addressing research security. However, care must be taken in the implementation of security training modules. Requirements and resources should be focused on areas of greatest risk.

We suggest that full security training should be required for those individuals working in areas of higher risk for research security, with reduced levels of training for those in low-risk areas. Requiring all researchers in all fields to take the full suite of available security training modules would be, in our opinion, an inefficient use of U.S. federal funding and university institutional resources. It may also be counterproductive, in that it could engender negative attitudes toward research security efforts.

> **Finding:** Training is an important component of an overall program to enhance research security. However, training will be most effective, in terms of impact and human resources, if required primarily in research areas where the security risk is highest.

Capitalizing on Relationships with International Allies.
Science is international in character and promotes efficiency and effective validation of results—similar to the rationale for openness and transparency of U.S. research applied more generally to the world at large. The United States benefits from other countries replicating our results, just as we benefit from seeing and learning from their new results. These arguments have become stronger over recent decades, as more nations around the world participate at the state-of-the-art level in the research enterprise (see, e.g., American Academy of Arts and Sciences–AmAcad–(2020)[26] and (2022)[27]).

U.S. allies in the European Union (EU), Asia-Pacific, North America, and elsewhere share many of the concerns about academic research security addressed in this report. We see at least two opportunities for leveraging international cooperation with like-minded colleagues in this domain.

- Discussions between NSF and counterpart organizations that fund basic scientific research in the EU and elsewhere could involve sharing best practices for suitably protecting sensitive and highly sensitive information while still enhancing the benefits that science brings to our nations' common security and prosperity. There is an opportunity to learn from allies' perspectives and to

[44]CHIPS and Science Act, Section 10634.
[45]CHIPS and Science Act, Section 10634(c).

identify how best to sustain existing cooperative scientific programs with those nations. One example is the report of the European Commission on foreign interference in research and innovation.[46] Another is the Trusted Research Program of the United Kingdom (UK) National Protective Security Authority,[47] which has many themes in common with current NSF research security initiatives. International cross-agency cooperation on the difficult topic of protecting sensitive and highly sensitive information could enhance existing scientific collaborations and strengthen the community's ability to counter threats from more secretive nations' research programs.

- Scientific societies already play a role in setting international standards of professional conduct and ethics. They could help inform researchers about how to establish and maintain balanced collaborations and other working relationships in a manner that is mutually beneficial (i.e., avoiding one nation systematically taking advantage of another.) While not a task for NSF itself, U.S. researchers should engage with international scientific societies to promote best practices of openess and fairness internationally.

Finding: There is an opportunity for NSF to work with counterpart funding agencies in nations supporting open and transparent scientific research so as to sustain the benefits to society of basic scientific research while minimizing the damage caused by necessary controls of sensitive information.

Recommendation: NSF should engage in dialogue with international partners who have like-minded approaches to research security and integrity, and who are facing similar research security problems.

Addressing Shortages in the U.S. Science, Technology, Engineering, and Mathematics (STEM) Workforce.

A significant consideration is that the United States has long benefited from foreign students obtaining degrees and starting their careers in U.S. schools, laboratories, and companies, with more than 100,000 U.S. higher-education degrees now being given to foreign students each year (JASON, 2019 [17]; Congressional Research Service (CRS), 2019 [29]). Historically, 70 percent of foreign (including 80–90 percent of Chinese) doctoral recipients choose to stay in the United States after completion of their degree.

[46] Directorate-General for Research and Innovation (European Commission), *Tackling R&I Foreign Interference — Staff Working Document*, Publications Office of the European Union, 2022, accessed December 21, 2023, https://data.europa.eu/doi/10.2777/513746. [28]

[47] U.K. National Protective Security Authority, "Trusted Research," accessed December 21, 2023, https://www.npsa.gov.uk/trusted-research.

The need for STEM students is currently so intense that the United States faces a shortfall of 5,000 students per year, in terms of U.S. persons gaining the necessary education. Foreign students, mainly from China and India (see, e.g., CRS, 2019 [29]; AmAcad (2022) [27]), make up that shortfall and help us maintain the influx of early-career researchers needed to sustain our STEM-based workforce of about 36 million[48] and GDP growth of 3 percent, driven in part by R&D innovations (see also the discussion in Section 2.4).

Through foreign students and collaborators, U.S. researchers develop a detailed understanding of the level of technical expertise present around the world, to the point of being able to identify the best educational or research programs abroad. Finally, foreign graduates from U.S. programs who return to their home country carry with them an understanding of our values and procedures, which is of long-term benefit to the United States. The same can be said of foreign research collaborations.

A challenge is how to improve research security while simultaneously ensuring that foreign students continue to see the United States as an attractive, welcoming, and open place to engage in research. NSF has an important role to play, through careful communication of the goals of its research security programs, together with its strong continuing support for research programs open to foreign students.

Increasing Investment in Technical Areas of Importance to National Security.
As discussed in Section 2.4, strategic R&D investments and the development of the U.S. STEM workforce need to be priorities for the United States. With regard to NSF, the recent establishment of the TIP Directorate, part of the CHIPS and Science Act directives, represents an investment toward development of strategic technologies.

With regard to the STEM workforce, increasing the number of degree-earning U.S. students in key technical areas should be a priority, particularly if the number of foreign students doing research in the United States declines—for example, because of increased international competition for such students. NSF could consider training grants for U.S. students in research and technology areas that are most relevant for national security.

NSF project funding is primarily awarded through a merit-based selection process that considers novelty, impact, and significance. NSF also funds people, by virtue of the NSF Graduate Research Fellowship Program (GRFP), without constraints on the type of work that the recipients perform during their fellowship tenure. Recipients

[48]National Science Board (NSB), *The State of U.S. Science and Engineering,* Figure 8, NSB-2022-1, https://ncses.nsf.gov/pubs/nsb20221/

of NSF GRFP funding must be U.S. citizens. In contrast, graduate students and post-doctoral researchers of any nationality are eligible for support in NSF-sponsored projects. These two funding mechanisms have served NSF well and are consistent with NSF policies on open science and open data, as well as the open science policies of universities.

As a technology evolves from fundamental research toward applications, and specifically toward applications that may be readily transitioned and exploited for national security uses, it would be beneficial to train more domestic students to enter the U.S. workforce in associated fields. We suggest that NSF consider a new funding program in targeted areas of national security significance that would help achieve this goal. In those areas, NSF could offer both training grants and post-doctoral fellowships as a tool to strengthen research security and provide enhanced training for a domestic science and engineering workforce. Annual meetings could be convened for the cohort of supported graduate students and post-doctoral fellows to build a community. Such a funding mechanism might be especially attractive for implementation as part of the newly established NSF TIP program. While other agencies, such as the NIH and the DOD, have similar funding programs, NSF may be able to engage a different segment of the future STEM workforce.

This Page Intentionally Left Blank

7 SUMMARY

In this report, we have considered the question of how NSF should address the issue of research security in its funded research programs. This report recommends specific steps that NSF can take to enhance awareness of research security, both within NSF and in the research community. It also suggests mechanisms for NSF to address research projects that are identified as sensitive because of their possible impact on national security. The processes we describe are compatible with the existing NSF structure and its emphasis on funding of research proposals from individual researchers and research organizations. The processes are flexible and adaptable so that they can respond to changing conditions and thinking about research security. While our recommendations focus on academic research security, many are relevant to NSF-funded R&D at organizations other than institutions of higher learning.

We provide the complete findings and recommendations of this study in the order they are discussed. The findings and recommendations are labeled with the relevant section number of the report—e.g., the label "F4-2" indicates the second finding in Section 4. Bold text indicates a key finding or recommendation also contained in the Executive Summary of this report.

7.1 Findings

F1-1 Openness and transparency in fundamental research promote scientific discovery, which improves national security.

F2-1 International collaborations with those who share the ideals of openness and transparency benefit all participants. However, recent efforts of the People's Republic of China (PRC) to preferentially direct fundamental research toward military needs, and its decision to restrict the flow of information out of the country, may severely limit the benefits of collaborations with research organizations within the PRC.

F4-1 The existing categories of Controlled Unclassified Information (CUI) do not provide useful guidance for identifying sensitive research that might be funded by NSF. The CUI guidelines themselves are silent as to what kinds of information need protecting.

F4-2 The Department of Energy (DOE) approach involves identifying specific critical areas of emerging technologies and utilizing subject matter experts in evaluating the sensitivity of the research. Regular updating and implementation of this scheme is labor intensive.

F4-3 At early stages of research, the potential applications' outcomes are notional. Most commonly, highly ambitious potential applications postulated for early-stage research are later replaced with different potential applications, addressing a range of societal, commercial, and national security needs as the research area progresses in technical maturity.

F4-4 The concept of Technology Readiness Level (TRL) is an essential component of the review to determine whether research is sensitive from a national security perspective.

F4-5 Differentiation between sensitive and non-sensitive research is most natural at the project level, not at the sub-field level. Projects in the same sub-field can have very different levels of risk.

F4-6 Risk mitigation must consider the spectrum of risk and be adaptable to changing trends in research. Resources should be concentrated on areas of maximum risk to ensure that benefits outweigh the costs.

F5-1 Access controls create hindrances for education, the progress of science, and national security. These must be weighed against hypothesized gains in preventing information transfer, especially in the context of a sophisticated and determined adversary.

F5-2 CUI-required security controls could lead to increased cost of doing research, with a resulting loss in research efficiency.

F5-3 Formal controls on research, such as a CUI designation, will have unintended consequences, including: increasing the cost of doing research, diverting resources better applied to expanding U.S. research efforts in critical fields, inhibiting rigorous and competitive development of new technologies, and discouraging some individuals and research organizations from engaging in U.S. research.

F6-1 The NSF proposal and reporting cycle provides the most natural means for identifying sensitive projects—i.e., those projects for which the release of information about research execution or outcomes could have a significant, direct, and predictable impact on national security.

F6-2 In order to effectively evaluate proposed research for potential sensitivity, NSF will need to develop in-house national security expertise. NSF staff with appropriate expertise would serve as consultants to support the review process.

F6-3 Initial assessment by the principal investigator (PI), with review by the NSF program office (and perhaps the NSF parent division), provides the best screening for potentially sensitivite or highly sensitive proposals—i.e., those that may need mitigations or controls.

F6-4 Research institutions and NSF have key roles to play in the process of risk identification and management. Dialogue between NSF and research institutions such as universities is critical.

F6-5 Awareness of research security issues among university researchers is lower than warranted at present, but approaches are available to raise the awareness level, and such steps are mandated under the CHIPS and Science Act.

F6-6 Properly implemented, a research security and integrity information sharing analysis organization (RSI-ISAO) of the type described in the CHIPS and Science Act would be a proactive step toward ensuring the security of the U.S. research enterprise and would provide tools and support for the development of a culture of awareness for research security.

F6-7 Training is an important component of an overall program to enhance research security. However, training will be most effective, in terms of impact and human resources, if required primarily in research areas where the security risk is highest.

F6-8 There is an opportunity for NSF to work with counterpart funding agencies in nations supporting open and transparent scientific research so as to sustain the benefits to society of basic scientific research while minimizing the damage caused by necessary controls of sensitive information.

7.2 Recommendations

R4-1 NSF should adopt a dynamic approach for identifying potentially sensitive research topics as they arise, instead of attempting to maintain a comprehensive list of sensitive research areas. NSF's process of identifying sensitive research projects should:

- Differentiate research projects based on the sensitivity of their potential applications,
- Include the maturity of the development path (Technology Readiness Level—TRL) for potential applications in the assessment of risk, and
- Include an assessment of the direct and predictable national security impact of the applications of each research proposal, if successful.

R5-1 NSF should proceed with caution before adding access or dissemination controls to grants or contracts. In considering whether to apply formal controls to a sensitive research project, NSF should weigh the balance between the positive protective benefits and the unintended negative consequences of such controls.

Controls can protect U.S. national security by preventing malign use of research results, but they can also hinder the beneficial free flow of research results in a way that negatively impacts broader U.S. economic and national security interests.

R6-1 The identification of sensitive projects proposed to NSF occurs most naturally before peer or panel review. We recommend that the principal investigator (PI) and the NSF program officer, with guidance from the NSF Division Office, determine if a proposal constitutes a sensitive project. NSF may wish to implement a pilot program within some division of NSF to gain experience with the process. NSF should consult with other federal research funding agencies such as the Department of Energy (DOE), the National Institutes of Health (NIH), and the Department of Defense (DOD) to help identify sensitive research.

R6-2 JASON recommends NSF develop language for the *Proposal & Award Policies & Procedures Guide (PAPPG)* to help PIs assess their proposed projects for possible impact on national security, including providing guidelines on what may, or may not, constitute research with potential national security impact.

R6-3 Specific mitigation strategies for sensitive research projects should be negotiated and agreed upon by the principal investigator (PI), NSF, and the sponsored projects office of the institution accepting responsibility for execution of the research. Specific mitigation steps should be proportionate to the assessed risk, relative to the associated costs.

R6-4 The NSF Office of Research Security should initiate meetings and forums with universities to discuss its plans for research security and to solicit input and feedback on its procedures once they begin to be implemented. This can begin now with respect to research security training modules being developed by NSF. If NSF initiates a pilot program for the identification of sensitive or highly sensitive research and its mitigation and control, feedback from universities will be vital for tuning the program for wider implementation across the entire scope of NSF-funded research.

R6-5 NSF should foster a culture of research security awareness by providing substantive information to researchers about real risks, making resources available for researchers to voluntarily seek guidance, and continuously engaging with researchers and their institutions about the efficacy of research risk mitigation and control efforts.

R6-6 NSF should engage in dialogue with international partners who have like-minded approaches to research security and integrity, and who are facing similar research security problems.

References

[1] Daniels, Mario and John Krige. *Knowledge Regulation and National Security in Postwar America*. Chicago: University of Chicago Press, 2022.

[2] National Academies of Sciences, Engineering, and Medicine, Committee on Science, Engineering, and Public Policy. *Scientific Communication and National Security*. Washington, DC: The National Academies Press, 1982. https://doi.org/10.17226/253.

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

[4] National Science and Technology Council, Office of Science and Technology Policy, Subcommittee on Research Security. *Draft Research Security Programs Standard Requirement*, 2023. https://www.whitehouse.gov/wp-content/uploads/2023/02/RS_Programs_Guidance_public_comment.pdf.

[5] Hannas, William C., James Mulvenon, and Anna B. Puglisi. *Chinese Industrial Espionage: Technology Acquisition and Military Modernisation*. New York: Routledge, 2013.

[6] The White House. "Remarks by National Security Advisor Jake Sullivan on the Biden-Harris Administration's National Security Strategy", October 12, 2022. https://www.whitehouse.gov/briefing-room/speeches-remarks/2022/10/13/remarks-by-national-security-advisor-jake-sullivan-on-the-biden-harris-administrations-national-security-strategy/.

[7] The White House. "President Biden Signs Executive Order on Addressing United States Investments in Certain National Security Technologies and Products in Countries of Concern." Press release, August 09, 2023. https://www.whitehouse.gov/briefing-room/statements-releases/2023/08/09/president-biden-signs-executive-order-on-addressing-united-states-investments-in-certain-national-security-technologies-and-products-in-countries-of-concern/.

[8] National Science Foundation, National Science Board. *Science and Engineering Indicators, Research and Development: U.S. Trends and International Comparisons, NSB 2022-5*, 2022. https://ncses.nsf.gov/pubs/nsb20225.

[9] Fedasiuk, Ryan, Alan Omar Loera Martinez, and Anna Puglisi. "A Competitive Era for China's Universities: How Increased Funding is Paving the Way". *Center for Security and Emerging Technology (CSET)*, March 2022. https://cset.georgetown.edu/wp-content/uploads/CSET-A-Competitive-Era-for-Chinas-Universities.pdf.

[10] National Science Foundation, National Science Board. *Science and Engineering Indicators, Publications Output: U.S. Trends and International Comparisons, NSB-2021-4*, 2021. https://ncses.nsf.gov/pubs/nsb20214/international-collaboration-and-citations.

[11] Remco, Zwetsloot, Jack Corrigan, Emily S. Weinstein, Dahlia Peterson, Diana Gehlhaus, and Ryan Fedasiuk. "China is Fast Outpacing U.S. STEM PhD Growth". *Center for Security and Emerging Technology (CSET)*, 2021. https://doi.org/10.51593/20210018.

[12] National Science Foundation, National Science Board. *Science and Engineering Indicators 2022, The State of U.S. Science and Engineering 2022, NSB-2022-1*. https://ncses.nsf.gov/pubs/nsb20221/conclusion.

[13] PRC Ministry of Science and Technology. "The '13th Five-Year' Special Plan for S&T Military-Civil Fusion Development". Center for Security and Emerging Technology (CSET), 2020. https://cset.georgetown.edu/publication/the-13th-five-year-special-plan-for-st-military-civil-fusion-development/.

[14] Jash, Amrita. "China's Military-Civil Fusion Strategy: Building a Strong Nation with a Strong Military". *Claws Journal*, 13(2):42–62, 2020. https://www.neliti.com/publications/330719/chinas-military-civil-fusion-strategy-building-a-strong-nation-with-a-strong-mil.

[15] Bitzinger, Richard A. "China's Shift from Civil-Military Integration to Military-Civil Fusion". *Asia Policy*, 16(1), 2021.

[16] People's Republic of China. *Outline of the People's Republic of China 14th Five-Year Plan for National Economic and Social Development and Long-Range Objectives for 2035*, 2021. https://cset.georgetown.edu/wp-content/uploads/t0284_14th_Five_Year_Plan_EN.pdf.

[17] Long, Gordon. *Fundamental Research Security: JASON Report* JSR-19–21. McLean, VA: MITRE Corporation, 2019. https://www.nsf.gov/news/special_reports/jasonsecurity/JSR-19-2IFundamentalResearchSecurity_12062019FINAL.pdf.

[18] Foster, Richard N. "Working the S-Curve: Assessing Technological Threats". *Research Management*, 29(4):17–20, 1986.

[19] Ergin, Tolga, Nicolas Stenger, Patrice Brenner, John B. Pendry, and Martin Wegener. "Three-Dimensional Invisibility Cloak at Optical Wavelengths". *Science*, 328(5976):337–339, 2010. https://www.science.org/doi/10.1126/science.1186351.

[20] Jacobs, Josh. "'Invisibility Cloak' Metamaterials Make Their Way Into Products". *Financial Times*, 2018. https://www.ft.com/content/c6864c76-de7d-11e7-a0d4-0944c5f49e46.

[21] National Science Foundation. *Proposal & Award Policies & Procedures Guide (PAPPG) (NSF 23-1)*, 2023. https://new.nsf.gov/policies/pappg.

[22] Uttal, Bro. "The Corporate Culture Vultures". *Fortune*, 108(8):66–72, 1983.

[23] Reason, James. *Human Error*. Cambridge: Cambridge University Press, 1990.

[24] Reason, James. *Managing the Risks of Organizational Accidents*. London: Routledge, 1997.

[25] Reason, James. "Achieving a Safe Culture: Theory and Practice". *Work & Stress*, 12(3):293–306, 1998.

[26] Challenges for International Science Partnerships (CISP). *America and the International Future of Science*, 2020. American Academy of Arts and Sciences, Cambridge, MA, https://www.amacad.org/publication/international-science.

[27] Challenges for International Science Partnerships (CISP). *Global Connections: Emerging Science Partners*, 2022. American Academy of Arts and Sciences, Cambridge, MA, https://www.amacad.org/sites/default/files/publication/downloads/2022-CISP_Global-Connections-Emerging-Science-Partners.pdf.

[28] Directorate-General for Research and Innovation (European Commission). *Tackling R&I Foreign Interference – Staff Working Document*, 2022. https://data.europa.eu/doi/10.2777/513746.

[29] Granovskiy, Boris and Jill Wilson. *Foreign STEM Students in the United States. CRS Report IF11347*. Congressional Research Service, 2019. https://crsreports.congress.gov/product/pdf/IF/IF11347.

[30] Ison, Jeremy. "Update for COGR on Research, Technology and Economic Security", 2023. U.S. Department of Energy, Office of Science. https://www.cogr.edu/sites/default/files/Multi-Agency%20Research%20Security%20Panel_0.pdf.

This Page Intentionally Left Blank

Appendix A STATEMENT OF WORK

Study Background:

In the 2019 JASON report on "Fundamental Research Security," JASON assessed whether any type of fundamental research needed to have additional controls imposed. The JASON report assessed the concept of "Controlled Unclassified Information" and confusion attendant to that concept and recommended that control of research should be as stated in National Security Decision Directive 189 (NSDD-189). Namely, NSDD-189 stated that the method for control of research essential to national security should be the formal classification system, and that the products of fundamental research should be unrestricted.

In the three years since the 2019 JASON report was completed, there has been much discussion in the U.S. government and elsewhere about whether particular research or technology areas need further protection or safeguards. Various federal agencies have attempted to define critical technologies and to develop lists of technology that may need further protection, but the U.S. government has found it challenging to articulate the need for protection or safeguards in a way that is useful to the research community and that does not shut off the open flow of information that enables the research enterprise to succeed.

CHIPS-and-Science Act

Section 10339 of the CHIPS-and-Science Act passed in 2022 imposes a new requirement on NSF, specifically to "identify research areas ... that may involve access to controlled unclassified or classified information" and "exercise due diligence in granting access ... to individuals working on such research who are employees of the Foundation or covered individuals on research and development awards funded by the Foundation." This may be particularly, though not exclusively, relevant to the new Directorate for Technology, Innovation, and Partnerships that was initiated by NSF in 2022.

Congressional FY23 Appropriations Language

Congress clarified its guidance to the NSF in its FY23 Appropriations bill:

> "**Open Source Research Risks**.—The Committee is concerned that certain open source research capabilities at NSF could be used by adversaries against U.S. allies or U.S. interests. The Committee therefore directs the

> NSF to collaborate with the Secretary of Defense and the Director of National Intelligence to compile and maintain a list of all NSF-funded open source research capabilities that are known or suspected to have an impact on foreign military operations. Such list shall be reviewed and updated at least annually by the NSF in collaboration with the Secretary of Defense and the Director of National Intelligence, and subsequently shall be reported to the Committee."

Objectives:

NSF seeks advice on how to identify the research areas referenced in Section 10339 of the CHIPS and Science Act of 2022, and how to decide when research crosses into the realm that may need control. Such controls may also impact both the quality and quantity of research, as well as the translation of research results into benefits for the nation. Given the broad scope of research that could be affected, JASON should combine general considerations with a detailed assessment of one or more particular research/technology areas, such as quantum information science. Such a detailed assessment could lead to development of a set of questions or evaluation criteria that NSF might use in fulfilling the Section 10339 requirements and Congressional guidance for maintaining a list of NSF-funded research areas of concern.

Specific questions to be addressed in the JASON study:

1. What are the general principles that NSF might use in developing lists of research/technology areas of concern?
2. What existing structure and guidance for federal Controlled Unclassified Information (CUI) might be applicable to identifying NSF-funded research/technology areas of concern?
3. What processes might NSF establish for annually reviewing its list of research/technology areas of concern?
4. Using one or more specific research/technology areas, as examples, what detailed evaluation criteria might NSF use for identifying research/technology areas of concern?
5. What are some of the potential impacts on the research community should some NSF- funded research areas be designated as areas of concern?
6. What processes and restrictions might be implemented to carry out research that falls within the NSF-designated CUI category?

Appendix B JSR-19-2I EXECUTIVE SUMMARY

A previous JASON Report JSR-19-2I,[49] discussed the issue of research security for fundamental research. We provide the Executive Summary of that report for reference.

[49]Gordon Long, "JSR-19-2I Fundamental Research Security," MITRE Corporation (2019), accessed December 18, 2023, https://www.nsf.gov/news/special_reports/jasonsecurity/JSR-19-2IFundamentalResearchSecurity_12062019FINAL.pdf. [17]

EXECUTIVE SUMMARY: JASON REPORT JSR-19-2I, *Fundamental Research Security*

The National Science Foundation (NSF) celebrates its 70th anniversary this year (2019). Over seven decades it has transformed U.S. fundamental research and enabled a world-leading scientific enterprise built upon open intellectual exchange, collaboration, and sharing. Several incidents in recent years have led to concern that the openness of our academic fundamental research ecosystem is being taken advantage of by other countries. This sense of unfair competition is entwined with concerns about U.S. economic and national security in a rapidly changing world. The NSF wishes to assess these concerns and respond to them where appropriate, while also adhering to core values of excellence, openness, and fairness.

NSF has charged JASON to produce an unclassified report that can be widely disseminated and discussed in the academic community, providing technical or other data about specific security concerns in a classified appendix.

JASON was asked:

1. What is the value and what are the risks of openness generally associated with fundamental research?

2. How should the principles of scientific openness be affirmed or modified?

3. Are there areas of fundamental research that should be more controlled rather than openly available? What are those areas?

4. What controls, if any, could be placed on particular types of information, and how can this be managed in a way that maintains the maximum benefit of the open research environment for fundamental research?

5. What good practices could be put into place by academic researchers to balance the open environment of fundamental research with the needs for national (and economic) security?

6. What good practices could be put into place by funding agencies such as NSF to balance the open environment of fundamental research with the needs for national (and economic) security?

To address these questions, JASON engaged with NSF leadership, senior university administrators, the intelligence community, and others. This report details the results from the ensuing inquiry, discussions, and debates engaged with NSF, senior university administrators, the intelligence community, law enforcement, and others.

Four main themes emerged from the study:

- The value of, and need for, foreign scientific talent in the United States,
- The significant negative impacts of placing new restrictions on access to fundamental research,
- The need to extend our notion of research integrity to include disclosures of commitments and potential conflicts of interest,
- The need for a common understanding between academia and U.S. government agencies about how to best protect U.S. interests in fundamental research while maintaining openness and successfully competing in the global marketplace for science talent.

Our Findings and Recommendations amplify these themes and propose steps the NSF can take to improve the security of fundamental research.

Findings

1. There is a long and illustrious history of foreign-born scientists and engineers training and working in the United States, and they make essential contributions to our preeminence in science, engineering and technology today. Maintaining that leading position will require that the United States continues to attract and retain the best science talent globally.

2. The United States upholds values of ethics in science, including objectivity, honesty, accountability, fairness and stewardship (NAS 2017 *Fostering Integrity in Research*). These values protect research integrity, upon which credibility of the fundamental research enterprise, and the entire academic system, is based.

3. Actions of the Chinese government and its institutions that are not in accord with U.S. values of science ethics have raised concerns about foreign influence in the U.S. academic sector. JASON reviewed classified and open-source evidence suggesting that there are problems with respect to research transparency, lack of reciprocity in collaborations and consortia, and reporting of commitments and potential conflicts of interest, related to these actions.

4. The scale and scope of the problem remain poorly defined, and academic leadership, faculty, and front-line government agencies lack a common understanding of foreign influence in U.S. fundamental research, the possible risks derived from it, and the possible detrimental effects of restrictions on it that might be enacted in response.

5. Conflicts of interest and commitment in the research enterprise can be broader than those that are strictly financial, including those that might occur in foreign research

collaborations or result from required reporting obligations for scholarships or grants.

6. There are many stakeholders with responsibility for the integrity of fundamental research, from U.S. government agencies to individual scholars, each with particular perspectives, roles and responsibilities. Universities and research funding agencies have policies and guidelines regarding some of these responsibilities, but these are often insufficient for individuals to assess risk and take appropriate actions.

7. National Security Decision Directive (NSDD) 189, established in 1985 a clear distinction between fundamental research and classified research. This remains a cornerstone to the fundamental-research enterprise, as officially reaffirmed in 2001 and 2010 and it continues to inform policy today.

8. Universities have mechanisms to handle Controlled Unclassified Information (CUI) under existing categories, such as HIPAA, FERPA, Export control, and Title XIII. CUI protection is difficult, but suited to these tasks, however it is ill-suited to the protection of fundamental research areas.

9. International researchers in the United States are partners in our research enterprise, and, consequently, in the effort to strengthen research integrity nationally and globally.

Recommendations

1. The scope of expectations under the umbrella of research integrity should be expanded to include full disclosure of commitments and actual or potential conflicts of interest.

2. Failures to disclose commitments and actual or potential conflicts of interest should be investigated and adjudicated by the relevant office of the NSF and by universities as presumptive violations of research integrity, with consequences similar to those currently in place for scientific misconduct.

3. NSF should take a lead in working with NSF-funded universities and other entities, as well as professional societies and publishers to ensure that the responsibilities of all stakeholders in maintaining research integrity are clearly stated, acknowledged, and adopted. Harmonization of these responsibilities with those of other federal research-funding agencies is encouraged.

4. NSF should adopt, and promulgate to all stakeholders, project assessment tools that facilitate an evaluation of risks to research integrity for research collaborations, and for all non-federal grants and research agreements.

5. Education and training in scientific ethics at universities and other institutions performing fundamental research should be expanded beyond traditional research integrity issues to include information and examples covering conflicts of interest and commitment.

6. NSF should support reaffirmation of the principles of NSDD-189, which make clear that fundamental research should remain unrestricted to the fullest extent possible, and should discourage the use of new CUI definitions as a mechanism to erect intermediate-level boundaries around fundamental research areas.

7. NSF should engage with intelligence agencies and law enforcement to communicate to academic leadership and faculty an evidence-based description of the scale and scope of problems posed by foreign influence in fundamental research, as well as to communicate to other government agencies the critical importance of foreign researchers and collaborations to U.S. fundamental research.

8. NSF should further engage with the community of foreign researchers in the United States to enlist them in the effort to foster openness and transparency in fundamental research, nationally and globally, as well as to benefit from their connections to identify, recruit and retain the best scientific talent to the United States.

9. NSF and other relevant U.S. government agencies should develop and implement a strategic plan for maintaining our competitiveness for the top science and engineering talent globally, taking advantage of new opportunities for engagement that might arise, even as others become more challenging.

Conclusion

JASON concludes that many of the problems of foreign influence that have been identified are ones that can be addressed within the framework of research integrity, and that the benefits of openness in research and of the inclusion of talented foreign researchers dictate against measures that would wall off particular areas of fundamental research. We expect that a reinvigorated commitment to U.S. standards of research integrity and the tradition of open science by all stakeholders will drive continued preeminence of the United States in science, engineering, and technology by attracting and retaining the world's best talent.

This Page Intentionally Left Blank

Appendix C APPROACHES OF OTHER AGENCIES: DEPARTMENT OF DEFENSE AND DEPARTMENT OF ENERGY

While JASON was undertaking this study, the DOD and the Department of Energy (DOE) were both working on their own efforts to identify unclassified domains of research that merit additional protections for national security reasons. JASON was briefed by these agencies on their approaches. We review these approaches here.

C.1 Department of Defense Approach: Researcher-Based Exclusion Lists

On June 29, 2023, the Office of the Under Secretary of Defense for Research and Engineering released the *Policy for Risk-Based Security Reviews of Fundamental Research* that is to be applied to *all* projects selected for funding. This review centers around a Decision Matrix to Inform Fundamental Research Proposal Mitigation Decisions.[50] In principle, the construction of this matrix recognizes both that international collaboration is "an important mechanism for participating in the global scientific commons and promoting progress in fundamental research" and the potential for foreign influence to result in the misappropriation of R&D efforts. In application, the risk matrix focuses specifically on identifying investigators with potential associations with a Foreign Country of Concern (FCOC), principally the People's Republic of China (PRC), with an aspirational goal of not substantially increasing the time to award and thereby delaying research progress. This matrix both identifies actions that would preclude an investigator or institution from receiving funding and describes conditions under which mitigation is required or recommended. As such, the Decision Matrix focuses on the *people* who would conduct the research and is agnostic to the research area.

At the top level, the DOD Decision Matrix, in alignment with §10632 of the CHIPS and Science Act, expressly excludes researchers who have participated in a malign foreign talent program, and those whose institutions do not have policies directly addressing malign foreign talent programs, from receiving DOD research funding. On the next-lower level of concern, the matrix identifies individuals who have other con-

[50]U.S. DOD, Under Secretary of Defense for Research and Engineering, "Countering Unwanted Influence in Department-Funded Research at Institutions of Higher Education," June 29, 2023, accessed December 21, 2023, https://media.defense.gov/2023/Jun/29/2003251160/-1/-1/1/COUNTERING-UNWANTED-INFLUENCE-IN-DEPARTMENT-FUNDED-RESEARCH-AT-INSTITUTIONS-OF-HIGHER-EDUCATION.PDF.

crete indicators of a conflict of commitment, including participation in other foreign talent recruitment programs, receipt of funding from an FCOC, a patent application history that is indicative of funding from an FCOC, or direct affiliation with an entity on the U.S. Bureau of Industry and Security (BIS) Entity List. Risk mitigations extend along a range of options, such as the removal or replacement of a co-principal investigator from a multi-investigator proposal, risk awareness training, and increased reporting frequency. Negotiations on these mitigations occur between the sponsor agency and the sponsored-projects office of the proposing institution, not the principal investigator (PI).

While the considerations listed above are relatively concrete indicators of previous or ongoing associations or affiliations with FCOCs, mitigation measures are also recommended or suggested for those who appear to have historical co-authorship with an individual who is now on the BIS Denied Persons List. While this is expressly *not* grounds for the rejection of a proposal, it will increase the burden associated with proceeding with the work, which may itself be a disincentive. Given that the the Entity and Denied Persons Lists contain more than 1,000 entries, the fraction of U.S. PIs who might be affected may be significant.

C.2 Department of Energy Approach: Critical Technology Identification

The DOE approach attempts to balance the protection of research results and intellectual property in a small number of identified technology areas with recognition of the importance of international collaboration to maintaining U.S. S&T competitiveness. As a result, it is constructed with the intent of continuing international S&T engagement with countries, including China, in a majority of research fields, while implementing restrictions in areas where its "scientific community assessed there was not a net-gain for U.S. interests and scientific progress." The DOE's Science and Technology Risk Matrix focuses on specific emerging technology topics associated with economic competitiveness, national security, or scientific leadership (e.g., quantum, batteries, AI); and on potential engagements with a specific country of risk, entities, or individuals (e.g., China, Russia, North Korea, and Iran).

Importantly, this approach strongly leverages the existing DOE laboratory research security environment and builds on existing DOE Integrated Safeguards and Security Management (ISSM). The effort is led by the 17 DOE National Laboratory Chief Research Officers. Subject matter experts are engaged to evaluate the current state of progress in each topic area and to create and update a categorization scheme as to which research developments constitute fundamental and non-sensitive insights

(Green), have the potential to be sensitive from an economic or national security standpoint (Yellow), or require additional protective measures (Red), as illustrated in Figure 6.[51] The Red category is meant to be a very select set of research areas, to minimize the overall impact of extra protections. This categorization guide is updated on an annual or more frequent basis to reflect developments in each field. Unlike the DOD approach, the matrix applies only to activities at the DOE National Laboratories (not universities). Further, it targets only the restriction of activities such as foreign engagements, cooperative R&D agreements, official travel, and foreign national engagement and access to the projects and data that involve countries of risk (China, Russia, Iran, and North Korea).

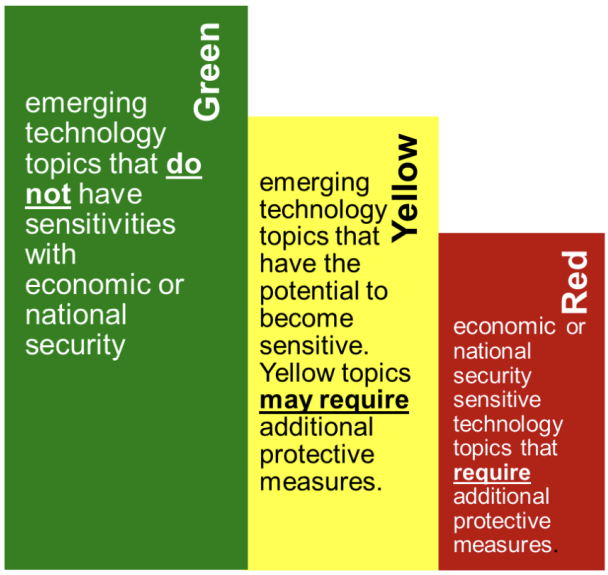

Figure 6: DOE approach to categorizing research security risk.

[51] U.S. DOE, Office of Science, slides from a presentation by Jeremy Ison at COGR Multi-Agency Panel on Research Security Risk Assessment & Analysis, October 26, 2026, accessed January 8, 2024, https://www.cogr.edu/sites/default/files/Multi-Agency%20Research%20Security%20Panel_0.pdf. [30]

This Page Intentionally Left Blank

Appendix D CONTROLLED UNCLASSIFIED INFORMATION

NSF tasked JASON with evaluating whether Controlled Unclassified Information (CUI), established by the Obama administration in 2009, could be a framework for identifying and protecting unclassified but sensitive research at academic institutions. JASON does not have legal expertise; but, as an understanding of CUI authorities and their limits is necessary to recommend a path forward, we review these here to best of our abilities. Earlier in this report, we discussed the federal origins of CUI in Section 2.3, commented on CUI as a basis for identifying sensitive research (Section 4.1), and commented on possible consequences of CUI designation (Section 5.3). We add additional information on CUI in this appendix.

D.1 CUI as a Basis for Identifying Technologies

JASON was asked "What existing structure and guidance for federal Controlled Unclassified Information (CUI) might be applicable to identifying NSF-funded research/technology areas of concern?"

The National Archives is the executive agent for CUI and operates the CUI Registry, the government-wide online repository for guidance regarding CUI policy and practice. The CUI Registry details specific categories of information the government protects and includes 18 organizational index groupings, such as critical infrastructure, defense, export control, financial, immigration, intelligence, international agreements, personal health information, proprietary business information, etc. JASON reviewed these but did not identify any existing CUI categories that would give NSF guidance for identifying technologies that need protection.

In general, technical information designated as CUI is protected because of its proprietary or physical-security nature. The one exception is technical information protected under export controls, which is a CUI category. Export controls exist for a wide range of political, economic, and national security reasons.[52] Export control law is complex and beyond JASON expertise; and export control lists are extensive, with ambiguities that often need to be resolved in the export-license review process. How-

[52]Michael Mastanduno, "The United States Defiant: Export Controls in the Postwar Era," *Daedalus*, vol. 120, no. 4, Fall 1991, pp. 91–112, accessed December 21, 2023, https://www.amacad.org/sites/default/files/daedalus/downloads/Daedalus_Fa91_Searching-for-Security-in-a-Global-Economy.pdf; Mario Daniels and John Krige, *Knowledge Regulation and National Security in Postwar America* (Chicago:University of Chicago Press, 2022). [1]

ever, we observe that, in general, export controls apply to high-Technology Readiness Level (TRL) technologies, usually artifacts, that have particular features specific to sensitive applications that are not themselves articulated in the export control lists. By contrast, fundamental research usually occurs at low TRLs, with notional but unproven applications (see Section 4.3). For this reason, the export control lists do not provide a foundation for identifying domains of fundamental research that merit extra control.

D.2 Does CUI Create an NSF Obligation to Control?

CUI was established by Executive Order 13556 in an attempt to unify protection standards applied by government agencies to a patchwork of sensitive information categories. The rules governing the implementation of CUI are codified in 32 Code of Federal Regulations (CFR) Section 2002. The protections that apply to CUI depend on the specific subcategory of CUI. Where specific controls are already specified in law, regulation, or government-wide policy, those pre-specified protection standards apply and are collectively categorized as *CUI-Specified* protections. Otherwise, *CUI-Basic* provisions outlined in 32 CFR 2002 apply. Although agencies may enhance CUI safeguards internally, §2002.22 prohibits such extra safeguards from being extended to entities outside of the agency absent a law, regulation, or government-wide policy specifically permitting this.

CUI-handling rules are not automatically binding on private entities that might obtain CUI-eligible data. To the extent that private entities are subject to CUI, that happens through contracts. 32 CFR 2002 encourages agencies to enter into written contracts with private organizations before "sharing" CUI with those entities. Those contracts are supposed to promulgate the safeguard provisions outlined in §2002.14, which apply to all kinds of CUI, whether *Basic* or *Specified*.[53] Only in this way do CUI controls become binding on private entities. Such contracts are logical for organizations that might, for example, conduct data processing on behalf of the U.S. Government. This limits the application of safeguards to the scope of the contract. For example, were CUI contracts used in a research setting, identical work occurring in the same laboratory, but funded by a nonprofit, would not be subject to CUI safeguards. Violations of contract provisions are but violations of the contract itself, with limited recourse unless other sanctions are defined in law.

Although this mechanism exists, the envisaged "sharing" conditions are quite differ-

[53] Agencies are technically allowed to furnish CUI data to private entities without contractual provisions in place if doing so serves the mission of the agency.

ent from what occurs in the course of fundamental research. In most fundamental research, NSF does not transfer any technical information (CUI or otherwise) to researchers. Rather, the concern here is that potentially sensitive information may be generated *de novo* in the course of research. Whether this creates an obligation upon NSF to insert CUI controls into the terms and conditions of its awards may depend, in part, on who owns the information being created in the course of research; and, in part, on whether CUI contracts can be applied to information that does not derive from government custody. These questions are discussed further in Section D.3.

D.3 Can NSF Use CUI to Create New Controls for Fundamental Research?

In order for an agency to create new CUI categories, the agency must have specific authorization to do so by law, regulation, or government-wide policy. We interpret Public Law 81-507 §15(b)(2) as potentially granting NSF the authority to create new CUI categories, although this interpretation should be reviewed by legal experts. If this authority exists, then the same question arises here as in the discussion above: Does NSF have the power to pre-designate information as CUI before its discovery in the course of fundamental research? Again, the answer may depend, in part, on who owns the information being created; and, in part, on whether CUI contracts can be applied to information that does not derive from government custody.

With respect to ownership, the terms and conditions of NSF awards convey information about the ownership of intellectual property in two ways: patent rights and copyright. In both cases, NSF awards generally leave those rights with the researcher but grant the U.S. Government a nonexclusive, nontransferable, irrevocable, paid-up license.[54] In this sense, the intellectual products of the research are not "work for hire," and NSF's ability to designate newly created information as CUI may be limited because CUI is established by executive order, and an executive order cannot regulate private property.[55] The type and/or terms of NSF awards may need to change (e.g., from grants to contracts) if NSF is set on using CUI provisions as a foundation for research controls.

[54]https://www.nsf.gov/pubs/2002/nsf02151/gpm7.jsp#731.3, https://www.nsf.gov/pubs/2002/nsf02151/gpm7.jsp#732.2.

[55]Limits to executive power have recently been re-litigated with respect to vaccine mandates. In all cases to date, the executive has lost. See Congressional Research Service, "Georgia: 2021 WL 5779939 at *12" and "Kentucky: 2021 WL5587446 at *13–14" in *State and Federal Autority to Mandate COVID-19 Vaccination*, May 17, 2022, accessed December 21, 2023, https://crsreports.congress.gov/product/pdf/R/R46745.

With respect to the authority, under CUI rules, to establish contracts protecting newly created information that does not derive from government-furnished information or a preexisting legally protected category, 32 CFR 2002 offers a variety of ambiguous interpretations.[56] A legal opinion is needed before determining whether CUI rules require or permit NSF to create contracts that extend CUI safeguards to not-yet-discovered fundamental research information.

It is unclear if the framework of CUI can provide a general vehicle for controlling fundamental research outside of government. At minimum, to use CUI for an NSF-designated technology area of concern would require that NSF create a regulation (see Section D.4). Whether the CUI information protection rules are substantively useful as a template for research controls is discussed in Section D.5.

D.4 Alternative Authorities to CUI

In general, there are two ways a government agency like NSF may regulate private activities: through a rulemaking process authorized in law, or by contractual terms. For example, academics handling medical records must comply with privacy standards specified by the U.S. Department of Health and Human Services (HHS). HHS obtains this authority to regulate private entities' handling of privately generated medical data through a law.[57] Similarly, if Census data is used for social-science research, that data must be protected under Title XIII of the U.S. Code. It is protected foremost because there is a law. However, in the case of Census data, the data are also designated as CUI, are owned by the government, and are obtained by researchers from the government. This means when the U.S. Census Bureau provides these data to private researchers, the Census Bureau is encouraged to enter into a contractual agreement with those researchers that would impose additional CUI-handling provisions on the researchers. (In practice, the Census Bureau protects such information by furnishing

[56] 32 CFR 2002.1(f), along with 2002.4(c) and 2002.16(a), clarifies that contracts with private entities to protect CUI are to be used when "agencies intend to share CUI with a non-executive branch entity." The language in these sections is suggestive of CUI that is already existing, and with information flowing from the government to private entities, not the reverse. At the same time, a strict reading of "share" could be interpreted to have a more bidirectional sense. Additionally, §2002.4(h) says "CUI does not include... information a non-executive branch entity possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an executive branch agency." This expressly articulates the possibility of CUI being created anew by outside entities on behalf of the government through a work-for-hire mechanism. However, later, paragraph (mm) appears to envisage private companies collecting extant CUI on the government's behalf, such as collecting social security numbers to process a loan application.

[57] U.S. Congress, *Health Insurance Portability and Accountabiity Act of 1996*, 104th Congress, Public Law 104-191, title II, §§261, 264(a)–(b), 110 Stat. 1936, 2021, 2033 (1996), accessed December 21, 2023, https://www.congress.gov/104/plaws/publ191/PLAW-104publ191.pdf.

researchers with Title XIII–qualified computer systems and Research Data Centers.[58])

In the law establishing NSF, Public Law 81-507, Section 15(b)(2) allows the Foundation to "establish security requirements and safeguards, including restrictions with respect to access to information and property, as it deems necessary." If this can be interpreted as a rulemaking authority in law, then NSF could go through a rulemaking process to identify domains of research that must be protected according to rules that NSF sees fit to impose. Rulemaking is, however, a slow and inflexible process. The procedures are set forth in the Administrative Procedure Act of the U.S. Code (5 USC 551 et seq.). Typically, an agency must give the public notice of a proposed rule before it goes into effect. Notice is accomplished by publishing the proposed rule in the Federal Register, and then the public is given an opportunity to submit comments on the proposed rule. The agency may take the comments into consideration before the final rule is published. In addition to the procedures outlined in the Act, there are a variety of other laws and executive orders that restrict regulations. In the case of NSF-sponsored research, the following may be relevant: If the proposed rule will have significant impact on small institutions, an additional defense of the economic impact is required (5 USC 603–614). Similarly, federal agencies cannot create rules that impose economic burdens on state government–funded institutions, such as state universities, without offsetting those costs (Executive Order 13132). Finally, if the rule can be construed as imposing limits on speech, additional defenses are required (Executive Order 12630). The final rule is then subject to actions by the President and by Congress before it goes into effect. Thus, if rulemaking is being considered, NSF should ensure whatever rules it puts forward are compatible with the rapidly changing states of knowledge in fundamental research domains. A rule governing the dissemination of information in a specific research sub-area, for example, could easily become obsolete by the time the rule is put in place. Rulemaking is also risky in that if a rule turns out to be harmful to academic competitiveness or to a specific discipline, or overtaken by events, it will take time and effort to remove it.

A more flexible alternative to rulemaking is to establish security mitigations and/or controls by the terms and conditions of the award. Such provisions can be adapted to suit the needs of each project and amended mid-stream, responding quickly to changes in the state of the art. These agreements do not create CUI. Over the course of this study, JASON did not become aware of any reason why NSF should favor rulemaking actions over customizing the terms and conditions of awards.

[58]U.S. Census Bureau, Data Stewardship Executive Policy Committee, "Policy on Controlling Non-Employee Access to Title 13 Data," 2009, accessed December 21, 2023, https://www2.census.gov/foia/ds_policies/ds006.pdf.

While there are many potential unintended consequences of implementing research controls (see Section 5.3), we highlight a particularly important one here: *Any* vehicle that imposes *access or dissemination* restrictions on information will *automatically* eliminate the Fundamental Research Exclusion (FRE) articulated in National Security Decision Directive (NSDD)-189. If such research, information, or technology falls into an export-controlled category, then even casual engagements with foreign nationals—such as research seminars, conferences, and eventually publication—could become deemed exports that are criminal actions. Publication of this material may require an export license. For these reasons, we urge NSF to use caution before imposing access or dissemination restriction on information stemming from research, and to do so in a narrowly scoped way.

D.5 CUI as a Template for Research Controls

NSF asked JASON, "What processes and restrictions might be implemented to carry out research that falls within the NSF-designated CUI category?" We interpret this more broadly to mean an NSF-designated domain of research requiring control.

To the extent that NSF might be looking to CUI as a template for research controls, we note that the CUI-Basic protections outlined in 32 CFR 2002 were not designed to protect national security–sensitive information, which might limit the utility. Specifically,

- CUI-Basic may be shared with foreign entities, 32 CFR 2002.16(a)(5)(iii); and
- CUI-Basic may be shared without a formal agreement, if doing so serves the mission, 32 CFR 2002.16(a)(5)(ii).

Adequate protection of national security–sensitive information would require the definition of a new CUI-Specified category defined by law, regulation, or government-wide policy. However, 32 CFR 2002.14 does not distinguish between CUI-Basic and CUI-Specified in requiring that all authorized holders of any type of CUI must:

- Establish controlled environments;
- Prevent unauthorized individuals from overhearing or observing CUI;
- Require direct control or physical barriers to CUI;
- Use only printers, copiers, and scanners that do not retain data;

- Delete electronic data in a method that makes the data irrecoverable; and
- Store, transmit, and process data only on information systems meeting the NIST SP 800-171 standard, which outlines 110 computer security provisions that must be satisfied.

These rules could be construed as a notional set of research controls, should NSF judge controls necessary. These controls constitute access controls, with supporting policies to prevent either (a) unintentional, or (b) intentional access to protected information.

Again, we note that any access control is largely incompatible with the mission of educational institutions. Such controls would disadvantage students involved with a controlled project by denying them the opportunity to engage in the free exchange of ideas, peer review, and practice at science communication. These activities are central to a student's education as scientist and engineer. As such, these controls could compromise the educational mission of universities and NSF, and their necessity should be weighed against this cost.

Such controls could additionally impede creativity and innovation in the protected sectors. President Reagan's NSDD-189 states that "an environment [with] the free exchange of ideas is a vital component" of academic research, and that such openness is therefore "an essential element in our physical and national security."[59] Slowing research in areas of national interest would impose a negative national security cost that must be weighed against the benefit of preventing controlled information from easily leaking to foreign nations; while realizing that if an adversarial peer country is determined to acquire the protected information, such controls are unlikely to stop them.

The supporting apparatus for access controls would impose significant cost on the conduct of research and reduce research funding efficiency. JASON received from NSF cost estimates for what the University of Oklahoma has spent to support such work, for example. A warehouse-type building for CUI experiments was estimated to have cost $2M, and a new office building with access control adequate for classified work cost $7M. Building construction costs are only about 10–20% of their life-cycle ownership costs, translating to roughly $1–2M per year for both buildings. Required security and compliance staff add cost of four full-time equivalent personnel, equating to another $1M per year. Thus, a medium to large ($1–3M/year) research program

[59] Office of the President of the United States, *National Policy on Transfer of Scientific, Technical and Engineering Information*. National Security Decision Directive 189. September 21, 1985, accessed December 21, 2023, https://catalog.archives.gov/id/6879779.

might incur security costs around $1–3M per year above the baseline research cost, roughly doubling the cost of carrying out that research. This would constitute a serious loss of research efficiency. Slowing research by half could easily allow countries like the People's Republic of China (PRC) to pull ahead in strategic fundamental research areas.

Appendix E ACRONYMS

AAU	American Association of Universities
AI	Artificial Intelligence
BIS	U.S. Bureau of Industry and Security
CFR	Code of Federal Regulations
CHIPS	Creating Helpful Incentives to Produce Semiconductors
CMI	Civil–Military Integration
COGR	Council on Governmental Relations
CRS	Congressional Research Service
CSET	Center for Security and Emerging Technology
CTI	Controlled Technical Information
CUI	Controlled Unclassified Information
CUI//SP-CTI	CUI Category: Specified Controlled Technical Information
DARPA	Defense Advanced Research Projects Agency
DOD	Department of Defense
DOE	Department of Energy
EAR	Export Administration Regulations
ESA	European Space Agency
EU	European Union
FCOC	Foreign Country of Concern
FERPA	Family Educational Rights and Privacy Act
FRE	Fundamental Research Exclusion
GDP	Gross Domestic Product
GPS	Global Positioning System
GRFP	NSF Graduate Research Fellowship Program
HHS	U.S. Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act
IR	Infrared
ISSM	Integrated Safeguards and Security Management (DOE)
ITAR	International Traffic in Arms Regulations
LIDAR	Laser Imaging, Detection, and Ranging
MCF	Military–Civilian Fusion
ML	Machine Learning
MOE	Ministry of Education (PRC)
MOST	Ministry of Science and Technology (PRC)
NAS	National Academy of Sciences
NIH	National Institutes of Health
NIST	National Institute of Standards and Technology

NSB	National Science Board
NSDD	National Security Decision Directive
NSF	National Science Foundation
NSPM	National Security Presidential Memorandum
NSTC	National Science and Technology Council
PhD	Doctor of Philosophy
PAPPG	NSF *Proposal & Award Policies & Procedures Guide*
PI	Principal Investigator
PPP	Purchasing Power Parity
PRC	Peoples' Republic of China
QED	Quantum Electrodynamics
R&D	Research and Development
RF	Radio Frequency
RSI-ISAO	Research Security and Integrity Information Sharing Analysis Organization
S&T	Science and Technology
SDI	Strategic Defense Initiative
SOW	Statement of Work
STEM	Science, Technology, Engineering, and Mathematics
TIP	NSF Directorate for Technology, Innovation, and Partnerships
TRL	Technology Readiness Level
U.S.	United States