Congressional Research Service
Informing the legislative debate since 1914

Federal Research Security Policies: Background and Issues for Congress

May 20, 2025

Congressional Research Service
https://crsreports.congress.gov
R48541

CRS REPORT
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

SUMMARY

R48541

May 20, 2025

Emily G. Blevins
Analyst in Science and Technology Policy

Federal Research Security Policies: Background and Issues for Congress

U.S. policies governing the conduct and results of federally funded basic and applied research generally encourage openness and information sharing with domestic and international collaborators, albeit with certain restrictions on classified research and certain export-controlled technical information. Much of the scientific community views the free and open exchange of information as integral to the process of scientific inquiry, the vetting of ideas through peer review, and the verification of research results through replication. At the same time, U.S. officials and other stakeholders have raised concerns about efforts of foreign governments, such as the People's Republic of China, to influence and exploit the openness of the U.S. research ecosystem. They warn that the ability of foreign strategic competitors to acquire U.S. advances in science and technology, and gain access to related training and talent, poses a risk to U.S. national defense and global economic competitiveness. Though policymakers may broadly agree on the goals of maintaining national security and competitiveness in science and technology, at issue for Congress is whether the risks associated with the openness of the U.S. research ecosystem may outweigh the benefits and, if so, in what ways.

In an effort to maintain the benefits of an open research system while protecting federally funded research from external threats, Congress and the executive branch have taken several actions—collectively referred to as "research security policies." Generally, research security policies apply to federally funded basic and applied research—the results of which would typically be published in the open scientific literature or would otherwise be made publicly available. These policies include disclosure requirements, prohibitions on participation in certain foreign talent recruitment programs, research security training requirements for certain researchers and federal employees, research security program requirements for certain institutions of higher education, and various information sharing and risk assessment responsibilities for federal agencies.

As opposed to controlling certain types of information or research outputs (as is the focus of classification and export control policies), the current research security policy framework is largely predicated on identifying and mitigating risks associated with certain relationships and behaviors of participants in federally funded research. Understanding the nature of the threats and the extent of the risks—to both research and security—may help elucidate specific trade-offs and inform the development of policy to maximize stated objectives while minimizing perceived costs. In reviewing existing policies to identify potential gaps and assess efficacy, congressional policymakers may face many issues. Potential issues may relate to federal agency collection of information about federally funded researchers, including the type of information and frequency with which it is collected. The consistency and efficacy of agency approaches to assessing collected information for potential affiliations and other factors that may make federal research vulnerable to foreign threats may also be an area for consideration. Another potential issue may relate to how agencies evaluate potential risks and the types of actions that may mitigate such risks.

Congressional policymakers have a variety of options regarding the security of federally funded research. They may continue overseeing federal agency implementation of existing statutory requirements and executive guidance, including by assessing the outcomes and efficacy of research security policies in accomplishing stated objectives. Either in conjunction with or as an alternative to oversight, Congress may choose to direct federal agencies via legislation, address perceived policy gaps, or codify certain policies and practices in statute. Such options could include amending the scope and frequency of required disclosures for researchers and adjusting the definition of "foreign talent recruitment program." Other options for Congress include directing harmonization of security risk assessment and mitigation activities across agencies (e.g., establishing minimum requirements) or identifying research fields (e.g., quantum research) for heightened scrutiny.

Contents

Figures

Tables

Appendixes

Contacts

Introduction

U.S. policies governing the conduct and results of federally funded basic and applied research generally encourage openness and information sharing with domestic and international collaborators.[1] Though viewed as supportive of scientific inquiry and innovation, the openness of the U.S. research ecosystem may also serve as a potential access point for foreign strategic competitors seeking to acquire U.S. advances in science and technology (S&T). Though policymakers may broadly agree on the goals of maintaining national security and competitiveness in S&T, at issue for Congress is whether the risks associated with the openness of the U.S. research ecosystem may outweigh the benefits and, if so, in what ways.

In an effort to maintain the benefits of an open research system while protecting federally funded research from external threats, Congress and the executive branch have taken several actions—collectively referred to as "research security policies." Generally, research security policies apply to federally funded basic and applied research—the results of which would typically be published in the open scientific literature or would otherwise be made publicly available. This type of research is often referred to as *fundamental research.* It is distinguished from research that has been classified for national security reasons and from later stage development work. Development projects are typically closer to commercial application and more likely subject to different types of federal control mechanisms designed to restrict foreign access to U.S. advances with particular commercial and/or defense value (e.g., export controls). Though subsequently referenced for context, these mechanisms fall outside the scope of this report.

With respect to federally funded basic and applied research, a range of research security policies have been developed; they include

- disclosure requirements,
- prohibitions on participation in certain foreign talent recruitment programs,
- research security training requirements for certain researchers and federal employees,
- research security program requirements for certain institutions of higher education, and
- various information sharing and risk assessment responsibilities for federal agencies.

This report presents an overview of research security, as defined by relevant federal policies and statutes, including analysis of the potential benefits of international research collaboration as well as the potential risks associated with foreign government initiatives that may seek to influence and exploit the federal research funding process and its results. It also synthesizes key legislative and executive branch actions related to the five research security policy approaches referenced

[1] *Basic research* generally refers to experimental or theoretical work undertaken primarily to acquire new knowledge of the underlying foundations of phenomena and observable facts. *Applied research* refers to an investigation undertaken to acquire new knowledge that is directed toward a specific practical aim or objective. The Office of Management and Budget (OMB) defines research and development (R&D) terminology in its guidance to federal agencies on preparation of the President's annual budget. In its guidance, OMB illustrates the distinction between basic and applied research, explaining that though "basic research may include activities with broad or general applications in mind, such as the study of how plant genomes change," the category generally excludes "research directed towards a specific application or requirement, such as the optimization of the genome of a specific crop species." See OMB, *Preparation, Submission, and Execution of the Budget*, Circular No. A-11, July 2024, p. 3 of Section 84, https://www.whitehouse.gov/wp-content/uploads/2018/06/a11.pdf.

above. Past and current efforts on behalf of the White House Office of Science and Technology Policy (OSTP) to coordinate and standardize federal research security policies as they evolved from ad hoc agency policies to government-wide policies and statutory requirements are also outlined.

In evaluating current federal research security policies, Congress may confront a number of complex issues related to identifying potential threats to the research enterprise, assessing associated risks, and mitigating such risks in a way that does not impede scientific progress and innovation. For example, some research security policies may disincentivize the flow of foreign-born talent into the United States, which could impact the strength of the U.S. research ecosystem. According to the Institute for Defense Analyses, over 20% of both the U.S. science, technology, engineering, and mathematics (STEM) workforce and STEM graduates from U.S. colleges and universities are foreign born.[2] The present report provides a discussion of such issues and potential options for consideration as policymakers assess research security policies and determine what changes, if any, might be made to address identified threats and other concerns.

While this report addresses federal research security policies that apply generally to federally funded research, there are also security-related policies that are specific to individual departments, agencies, and programs. The Department of Defense (DOD) supports fundamental research, which may be subject to specific DOD policies tailored to address unique risks related to mission-associated considerations.[3] Likewise, to identify potential security risks, Congress requires federal agencies to conduct due-diligence reviews of firms seeking research and development (R&D) awards through the Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) programs.[4] These tailored policies and associated issues fall outside this report's scope.

Historical Overview and Context

The scientific community generally views the free and open exchange of information as vital to the process of scientific inquiry, including the vetting of ideas and the verification of research results. The U.S. research ecosystem broadly operates on these principles, which have undergone periodic scrutiny and evaluation by scientists and policymakers during moments of heightened national security concerns. Understanding the nature of these historical debates may contextualize current policy considerations and options for Congress.

Evolution of Research Security Policies from 1940s to Present

Since at least the 1940s, concerns have been raised about the potential threat posed by adversarial nations exploiting the openness of the U.S. research ecosystem to obtain scientific and technological information that might translate into a strategic economic or military advantage. Likewise, the identification of potential threats has historically elicited debates about the relative harms and benefits associated with restricting research in order to impair the flow of knowledge to specific foreign entities.

[2] Thomas D. Olszewski et al., *Characterizing the Loss of Talent from the U.S. STEM Ecosystem*, Institute for Defense Analyses, Science and Technology Policy Institute, February 2024, p. iv, https://www.ida.org/research-and-publications/publications/all/c/ch/characterizing-the-loss-of-talent-from-the-us-stem-ecosystem.

[3] Defense Advanced Research Projects Agency (DARPA), "DARPA Fundamental Research Risk-Based Security Review Process," December 21, 2023, https://www.darpa.mil/attachments/DARPA%20Risk%20Based%20Security%20Reviews%20of%20Fundamental%20Research%20Process1.pdf.

[4] See CRS Report R43695, *Small Business Research Programs: SBIR and STTR*, by Marcy E. Gallo.

For example, in the early 1980s, concerns about the potential transfer of sensitive technology from the United States to the Soviet Union featured in congressional hearings, government reports, and news articles.[5] In 1982, the National Academies of Science, Engineering, and Medicine (NASEM; known at that time by their separate institutional names: the Institute of Medicine, the National Academy of Sciences, and the National Academy of Engineering) examined federal controls being placed on scientific communication and potential challenges involved with balancing competing national objectives. Its report, which was sponsored by DOD, the National Science Foundation (NSF), and several scientific societies and nonprofit foundations,[6] noted that

> [t]he use of American science and technology in the rapid increase in Soviet military strength over the past decade has aroused substantial concern in the current administration. This concern has been expressed frequently in recent months by high-ranking officials, who have called for tighter controls on all forms of technology transfer, including communication among scientists by such means as the publication of papers in scientific journals and by face-to-face meetings. In addition, federal agencies have already taken steps to control the flow of data and information from scientific research. These statements and actions have led to rising concern in the U.S. scientific community that such controls might impede scientific progress and its contribution to the national welfare.[7]

In 1985, President Reagan issued National Security Decision Directive 189 (NSDD-189), which indicates that the results of federally funded fundamental research should be widely available, citing "a research environment conducive to creativity" and "the free exchange of ideas" as key elements on which the strength of American science rests.[8] Per NSDD-189, in instances where national security concerns may warrant restricting the "conduct or reporting" of federally funded basic and applied research in science, technology, and engineering, classification is the appropriate control mechanism.[9]

Following the 9/11 attacks in 2001, NASEM's National Research Council revisited these concerns in the context of the terrorist threat:

> Openness and communication are foundations of modern science. The generation of new ideas arises from having access to the work of others; thus, the newest discoveries must be published or presented. However, the sharing and publication of research results, while advancing the aggregate knowledge of researchers working in a given field of science, also can provide access to those who would use such information to harm others. Policies aimed

[5] Congressional hearings include U.S. Congress, Senate Governmental Affairs Committee, Permanent Subcommittee on Investigations, *Transfer of United States High Technology to the Soviet Union and Soviet Bloc Nations*, 97th Cong., 2nd sess., May 4, 5, 6, 11, and 12, 1982; and U.S. Congress, House Science and Technology Committee, Science, Research and Technology Subcommittee and the Investigations and Oversight Subcommittee, *Impact of National Security Considerations on Science and Technology*, 97th Cong., 2nd sess., March 29, 1982. Government reports and news articles include U.S. Central Intelligence Agency, *Soviet Acquisition of Western Technology*, April 1982, https://www.cia.gov/readingroom/document/cia-rdp96b01172r000700060001-8; Caspar W. Weinberger, "Technology Transfers to the Soviet Union," *Wall Street Journal*, January 12, 1982, p. 32; and Frank Carlucci and William D. Carey, "Scientific Exchanges and U.S. National Security," *Science*, vol. 215, no. 4529 (January 8, 1982), pp. 139-141.

[6] Additional cited sponsors included the American Association for the Advancement of Science, the American Chemical Society, the American Geophysical Union, and a consortium of private foundations.

[7] Institute of Medicine et al., *Scientific Communication and National Security*, 1982, p. ix, https://www.nap.edu/catalog/253/scientific-communication-and-national-security.

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

[9] NSDD-189 defines fundamental research as "basic and applied research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community, as distinguished from proprietary research and from industrial development, design, production, and product utilization, the results of which ordinarily are restricted for proprietary or national security reasons."

> at limiting access by malicious parties, if not well conceived, can constrain the efforts of those desiring to put such information to good use. Thus, developing and implementing measures to control access to sensitive information must balance the overall costs of such controls to the research community and the public against the anticipated effectiveness of such measures to enhance security.[10]

The framework established by NSDD-189 has largely persisted and is reflected in current federal research policy, which also includes additional expectations related to the openness and public availability of federally sponsored research. For example, a federal-government-wide public access policy directs federal agencies to require that publications and their supporting data resulting from federally funded research be made publicly accessible "*without an embargo on their free and public release*."[11] In addition to fostering scientific progress and innovation, the public access policy rationalizes the benefits of unrestricted R&D in terms of delivering returns on taxpayer investments.

Potential Benefits of International Collaboration

Affirming the importance of openness and the unrestricted exchange of ideas to scientific inquiry, federal policies have generally encouraged U.S. participation in international S&T collaborations. Tasked by Congress with coordinating the international S&T activities of federal agencies, the OSTP Director, acting through the National Science and Technology Council's (NSTC's) Subcommittee on International Science and Technology Coordination, is also required to report on such activities to Congress every two years.[12] The subcommittee's 2024 *Biennial Report to Congress on International Science & Technology Cooperation* describes the value of international collaboration:

> By bringing together a wide range of viewpoints and resources that lead to scientific discoveries and technological innovations, international [S&T] cooperation generates vital economic, political, societal, national security, development, and diplomatic benefits for both the United States and the world.[13]

The report also asserts that, in addition to furthering scientific advances and innovation, international S&T collaboration has served as "a pillar of U.S. foreign policy and national security since the end of World War II."[14] International S&T cooperation may involve a variety of collaborative arrangements, including informal collaborations between U.S. and foreign

[10] The National Research Council is the principal operating agency of the National Academies of Science, Engineering, and Medicine (NASEM), through which it provides services to the government, the public, and the scientific and engineering communities. National Research Council, *Science and Security in a Post 9/11 World: A Report Based on Regional Discussions Between the Science and Security Communities*, 2007, p. 27, https://www.nap.edu/catalog/12013/science-and-security-in-a-post-911-world-a-report. See especially Chapter II, "Policies for Openness and Information Control."

[11] Emphasis in the original, see memorandum from Alondra Nelson, Deputy Assistant to the President and Deputy Director for Science and Society Performing the Duties of Director, Office of Science and Technology Policy (OSTP), to heads of executive departments and agencies, "Ensuring Free, Immediate, and Equitable Access to Federally Funded Research," August 25, 2022, https://bidenwhitehouse.archives.gov/wp-content/uploads/2022/08/08-2022-OSTP-Public-Access-Memo.pdf.

[12] P.L. 114-389, §208, American Innovation and Competitiveness Act, 42 U.S.C. §6625(e).

[13] Subcommittee on International Science and Technology Coordination, National Science and Technology Council (NSTC), *Biennial Report to Congress on International Science and Technology Cooperation*, February 2024, p. 1, https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/02/2024-Biennial-Report-to-Congress-on-International-Science-Technology-Cooperation.pdf.

[14] Subcommittee on International Science and Technology Coordination, NSTC, *Biennial Report to Congress on International Science and Technology Cooperation*, p. 1.

researchers and academic institutions. More formal and legally binding structures include international agreements, which may be multilateral or bilateral and may promote S&T collaboration between nations at the government-wide or technical agency level.[15] The State Department's Office of Science and Technology Cooperation has facilitated such formal mechanisms, including the bilateral Science and Technology Agreement (STA). The office has reported that, as of March 2025, the United States had nearly 60 bilateral STAs and over 2,000 sub-agreements in force, which provided "valuable access for U.S. government scientists to foreign scientific capabilities, facilities, and expertise, while also exposing other countries to U.S. science procedures, norms, and values."[16]

Potential Risks Associated with International Collaboration

At the same time, perceived challenges to U.S. economic and technological leadership have led some policymakers to reevaluate the potential risks associated with international research collaborations and the openness of the U.S. research ecosystem. For example, although the JASON group's 2024 report, *Safeguarding the Research Enterprise*, ultimately concludes that the principles expressed in NSDD-189 remain valid, it documented a number of ways that the economic and technological landscape has changed since 1985, including

- the increasingly important role that innovations in the civilian commercial sector are playing in military performance and national defense;
- the growing connection between academic research and commercial applications;
- the globalization of the research enterprise facilitated by the internet;
- the competitive challenge posed by the People's Republic of China (PRC, or China) to U.S. technological and economic leadership, along with concerns about PRC military-civil fusion policies; and
- the evolving landscape in the United States with respect to research security regulations and policies.[17]

The nature of potential threats facing the U.S. research ecosystem have also shifted in response to this changing landscape (see "Examples of Potential Threats and Risks"). For example, sources have documented efforts on behalf of foreign governments (most notably the PRC) to influence and exploit the openness of the U.S. research ecosystem through talent recruitment programs.[18] Others have asserted that joint research collaborations with nations deemed to be economic competitors with the United States, such as those facilitated by formal agreements such as the

[15] Bridget M. Dolan, "Science and Technology Agreements as Tools for Science Diplomacy: A U.S. Case Study," *Science & Diplomacy*, December 10, 2012, https://www.sciencediplomacy.org/article/2012/science-and-technology-agreements-tools-for-science-diplomacy.

[16] Office of Science and Technology Cooperation, "Key Topics: Science and Technology Agreements," accessed April 11, 2025, https://www.state.gov/key-topics-office-of-science-and-technology-cooperation.

[17] The National Science Foundation (NSF) commissioned the JASON group—an independent scientific advisory group that has historically provided consulting services for the U.S. government on defense-related science and technology matters—to prepare the report. See JASON, *Safeguarding the Research Enterprise*, JSR-23-12, March 21, 2024, pp. 9-10, https://nsf-gov-resources.nsf.gov/files/JSR-23-12-Safeguarding-the-Research-Enterprise-Final.pdf?VersionId=ZVhvRaTIrxMsdZql6E_yz5pN6Ssw0fSl.

[18] Smriti Mallapaty, "China Hides Identities of Top Scientific Recruits Amidst Growing US Scrutiny," *Nature*, October 24, 2018, https://www.nature.com/articles/d41586-018-07167-6; National Institutes of Health (NIH) Advisory Committee to the Director (ACD), *ACD Working Group for Foreign Influences on Research Integrity*, December 2018, https://acd.od.nih.gov/documents/presentations/12132018ForeignInfluences_report.pdf; and U.S. Congress, House Committee on Foreign Affairs, Subcommittee on Asia, the Pacific and Nonproliferation, *U.S. Responses to China's Foreign Influence Operations*, 115th Cong., 2nd sess., March 21, 2018.

U.S.-China STA, may benefit China asymmetrically if PRC collaborators do not consistently demonstrate reciprocity in sharing research data and results.[19]

Though China is a principal U.S. peer competitor, intelligence community threat assessments and related analysis have also cited state-level threats posed by Russia, Iran, and North Korea, as well as "lesser state and nonstate risks [that] abound in the acutely interconnected world of scientific R&D."[20] In a May 2025 letter to the President of Harvard University, some Members of Congress expressed concern about the alleged involvement of Harvard researchers with projects funded by the Iranian government.[21]

Understanding the Trade-Offs

Though aspects of the context may have shifted, an underlying tension at the heart of the policy debate persists: research restrictions and controls intended to enhance national and economic security may indirectly limit the pace of scientific discovery and technological advancement, which, in turn, may create a cost to national and economic security. Understanding the nature of the threats and the extent of the risks—to both research and security—may help elucidate specific trade-offs and inform the development of policy to maximize stated objectives while minimizing perceived costs. Though policymakers may broadly agree on the goals of maintaining national security and S&T competitiveness, much of the past and ongoing policy debate has centered on whether the risks associated with the openness of the U.S. research ecosystem may outweigh the benefits and, if so, in what ways.

The principles outlined in NSDD-189, which largely govern federal research policy today, hold that with respect to fundamental research, the benefits of openness outweigh the risks. Largely in line with this policy, the current research security framework seeks to mitigate risks associated with certain relationships and behaviors involving foreign entities within the research ecosystem as opposed to controlling access to information.

Research security policies exist within a larger suite of tools established by Congress and the executive branch to protect U.S. S&T advances and may be considered within this broader framework. Though fundamental research, generally, is exempt from many of these controls, additional international and federal requirements may apply to specific fields of research. For example, policies have been established to control biological research, including fundamental research, that may pose risks to public health, economic security, and national security, among other factors. Oversight of the life sciences, in particular laboratory biosafety and biosecurity, is exercised pursuant to a mixture of federal law, federal guidance, and self-governance, dependent on the types of experiments and biological agents being used.[22]

[19] See CRS In Focus IF12510, *U.S.-China Science and Technology Cooperation Agreement*, by Karen M. Sutter and Emily G. Blevins.

[20] NASEM, *National Science, Technology, and Security Roundtable Capstone: Proceedings of a Workshop*, 2025, pp. 129-130, https://nap.nationalacademies.org/catalog/27976/national-science-technology-and-security-roundtable-capstone-proceedings-of-a.

[21] House Select Committee on the Chinese Communist Party (CCP), "Lawmakers Demand Answers from Harvard Over Ties to Chinese Military, Sanctioned Entities, and Iranian Government," press release, May 19, 2025, https://selectcommitteeontheccp.house.gov/media/press-releases/lawmakers-demand-answers-harvard-over-ties-chinese-military-sanctioned.

[22] For more information on this policy framework, see CRS Report R48155, *Oversight of Laboratory Biosafety and Biosecurity: Current Policies and Options for Congress*, by Todd Kuiken.

What Is Research Security?

Broadly, *research security* describes a constellation of statutory and executive requirements as well as institutional programs and practices intended to protect federally funded research from foreign influence and exploitation. Though Congress has enacted a range of research security policies, such provisions do not include a statutory definition of *research security*. Rather, executive branch policies and guidance documents have offered a formal definition.

On January 14, 2021, President Trump, through National Security Presidential Memorandum-33 (NSPM-33), established a national security policy intended to "strengthen protections of United States Government-supported Research and Development (R&D) against foreign government interference and exploitation."[23]

NSPM-33 implementation guidance, as clarified and updated, issued by OSTP provides uniform definitions for key terms, such as *research security*, which it describes as

> [s]afeguarding the research enterprise against the misappropriation of research and development to the detriment of national or economic security, related violations of research integrity, and foreign government interference.[24]

Specifically citing "violations of research integrity," NSPM-33's definition of research security points to linkages between the two concepts—research security and research integrity.[25] Before NSPM-33's usage of the term *research security*, federal agency heads primarily described threats to the research ecosystem in terms of foreign efforts to compromise research integrity. For example, in 2018, after discovering a series of policy violations involving foreign actors (see "Examples of Potential Threats and Risks"), the National Institutes of Health (NIH) Advisory Committee to the Director established a Working Group for Foreign Influences on Research Integrity.[26] The National Science Board also issued a 2018 statement on "security and science" that emphasized the importance of protecting research integrity "in light of the importance of American technological preeminence for our economy and security."[27]

Research integrity, an already established policy framework governing transparency and professional norms in the research process, formed the policy foundation for research security as a new concept specific to foreign threats.[28] *Research integrity* remains key to concretizing explicit

[23] White House, "Presidential Memorandum on United States Government-Supported Research and Development National Security Policy," National Security Presidential Memorandum-33 [NSPM-33], January 14, 2021, https://trumpwhitehouse.archives.gov/presidential-actions/presidential-memorandum-united-states-government-supported-research-development-national-security-policy/.

[24] NSF, "National Security Presidential Memorandum-33 Implementation Guidance. Appendix: Definitions," November 1, 2023, https://www.nsf.gov/bfa/dias/policy/researchprotection/nspm33definitions.pdf.

[25] NSF, "National Security Presidential Memorandum-33 Implementation Guidance. Appendix: Definitions."

[26] NIH ACD, "ACD Working Group for Foreign Influences on Research Integrity," December 2018, https://acd.od.nih.gov/documents/presentations/12132018ForeignInfluences_report.pdf.

[27] Diane L. Souvaine, "State of the National Science Board on Security and Science," NSB-2018-42, October 23, 2018, https://www.nsf.gov/nsb/publications/2018/NSB-2018-42-statement-on-security-and-science.pdf.

[28] *Research misconduct* is a related term that may be discussed in the context of research integrity. For background on federal policies relating to both, see OSTP, "Executive Office of the President; Federal Policy on Research Misconduct; Preamble for Research Misconduct Policy," 65 *Federal Register* 76260, December 6, 2000, https://www.federalregister.gov/documents/2000/12/06/00-30852/executive-office-of-the-president-federal-policy-on-research-misconduct-preamble-for-research; OSTP, "Proposed Federal Policy on Research Misconduct to Protect the Integrity of the Research Record," 64 *Federal Register* 55722, October 14, 1999, https://www.federalregister.gov/documents/1999/10/14/99-26608/proposed-federal-policy-on-research-misconduct-to-protect-the-integrity-of-the-research-record; and OMB, "Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of (continued...)

practices and actions that federal agency policies continue to prohibit, regardless of foreign involvement, and is defined by NSPM-33 to include

> the use of honest and verifiable methods in proposing, performing, and evaluating research; reporting research results with particular attention to adherence to rules, regulations, and guidelines; and following commonly accepted professional codes or norms.[29]

In establishing a national security policy for federally supported R&D, NSPM-33 also outlined the contours of threats facing the U.S. research ecosystem, potential associated risks, and proposed risk mitigation measures:

> Unfortunately, some foreign governments, including the People's Republic of China, have not demonstrated a reciprocal dedication to open scientific exchange, and seek to exploit open United States and international research environments to circumvent the costs and risks of conducting research, thereby increasing their economic and military competitiveness at the expense of the United States, its allies, and its partners. While maintaining an open environment to foster research discoveries and innovation that benefit our Nation and the world, the United States will also take steps to protect intellectual capital, discourage research misappropriation, and ensure responsible management of United States taxpayer dollars. This includes steps to ensure that participants with significant influence on the United States R&D enterprise fully disclose information that can reveal potential conflicts of interest and conflicts of commitment.[30]

To mitigate potential risks posed by such threats, NSPM-33 directed federal agencies to establish policies prohibiting recipients of federal R&D support from participating in foreign talent recruitment programs and requiring them to disclose current and pending support when applying for federal funding. NSPM-33 required federal agencies to share information about potential threats to research security and related policy violations with one another and with institutions of higher education. It also directed agencies to provide research security training for federal employees engaged in R&D or making funding decisions as well as to require certain institutions of higher education to establish research security programs.

NSPM-33 directed OSTP and the NSTC—a Cabinet-level body composed of federal science agency and department heads, created by executive order in 1993 to advise the President and coordinate S&T policy—to coordinate agency implementation.[31]

Examples of Potential Threats and Risks

The U.S. intelligence community, federal research agencies, think tanks, and federal advisory bodies have identified various threats to the security of U.S. research. The types of threats described roughly fall into two categories: actions that threaten to exert foreign influence over the U.S. research enterprise, and actions intended to exploit federally funded research for the benefit of foreign adversaries and economic competitors (see **Figure 1**).

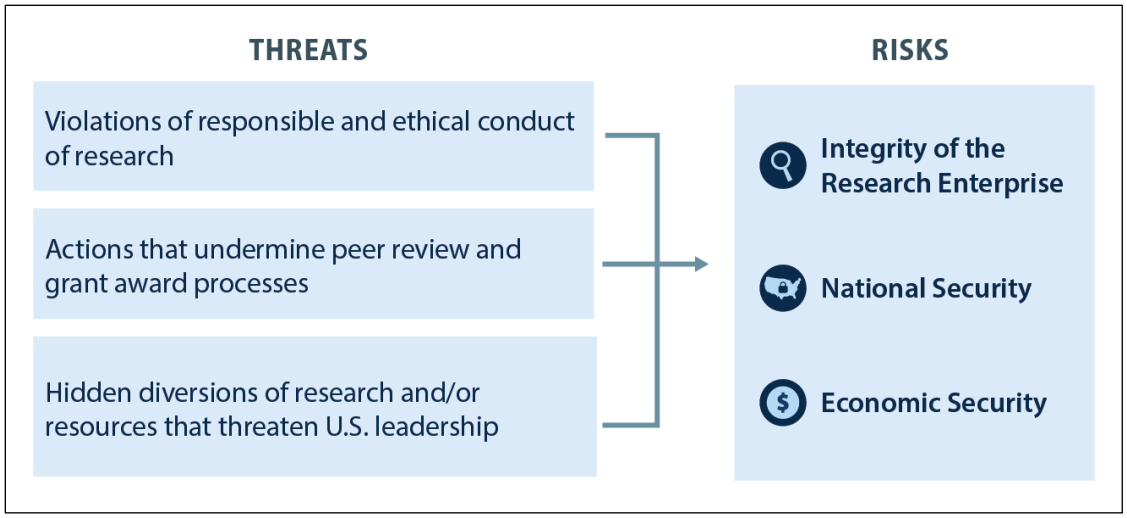
Information Disseminated by Federal Agencies; Republication," 67 *Federal Register* 8452, February 22, 2002, https://www.federalregister.gov/documents/2002/02/22/R2-59/guidelines-for-ensuring-and-maximizing-the-quality-objectivity-utility-and-integrity-of-information.

[29] NSF, "National Security Presidential Memorandum-33 Implementation Guidance. Appendix: Definitions."

[30] NSPM-33.

[31] For additional information about the NSTC, see CRS Report R47410, *The Office of Science and Technology Policy (OSTP): Overview and Issues for Congress*, by Emily G. Blevins.

Figure 1. Overview of Potential Threats and Associated Risks



Source: CRS, based on Office of Science and Technology Policy, "Enhancing the Security and Integrity of America's Research Enterprise," October 15, 2020, p. 9, https://trumpwhitehouse.archives.gov/wp-content/uploads/2020/07/Enhancing-the-Security-and-Integrity-of-Americas-Research-Enterprise.pdf.

U.S. intelligence and law enforcement agencies have warned about foreign adversaries taking advantage of the openness of U.S. research for many years. For example, a 2011 Federal Bureau of Investigation (FBI) report warned that "the United States is a society of openness and freedom, values especially central to campuses of higher education. Foreign adversaries and competitors take advantage of that openness and have been doing so for many years."[32] In 2015, the FBI issued another report that described the growing practice of "academic espionage" perpetrated by "foreign adversaries and economic competitors [who] can take advantage of the openness and collaborative atmosphere that exists at most learning institutions in order to gain an economic and/or technical edge through espionage."[33] The report further described the unique risks faced by institutions of higher education:

> While information is shared on campuses, there is still an ethical, and sometimes legal, responsibility to protect research. With the extensive amount of primary research done at universities, many academics hope to gain recognition for innovative research. When IP [intellectual property] is stolen from academic institutions, they ... not only [face] the loss of potentially valuable information and technology, but also risk rendering obsolete the years of work and research that went into the foundation of the IP. Such a loss could preclude the ability to conduct related research and development in the future. Research is often funded by private companies or the government who may need a first-to-market practical application from the research to make it worth their investment. Stealing the research could then equate to stealing money from the funding organization/agency.[34]

By 2018, Congress and federal research agencies warned of the threats described by the FBI. For example, during the 115th Congress, the House Committee on Science, Space, and Technology

[32] Federal Bureau of Investigation (FBI), *Higher Education and National Security: The Targeting of Sensitive, Proprietary and Classified Information on Campuses of Higher Education*, April 2011, p. 1, https://www.fbi.gov/file-repository/higher-education-national-security.pdf/view.

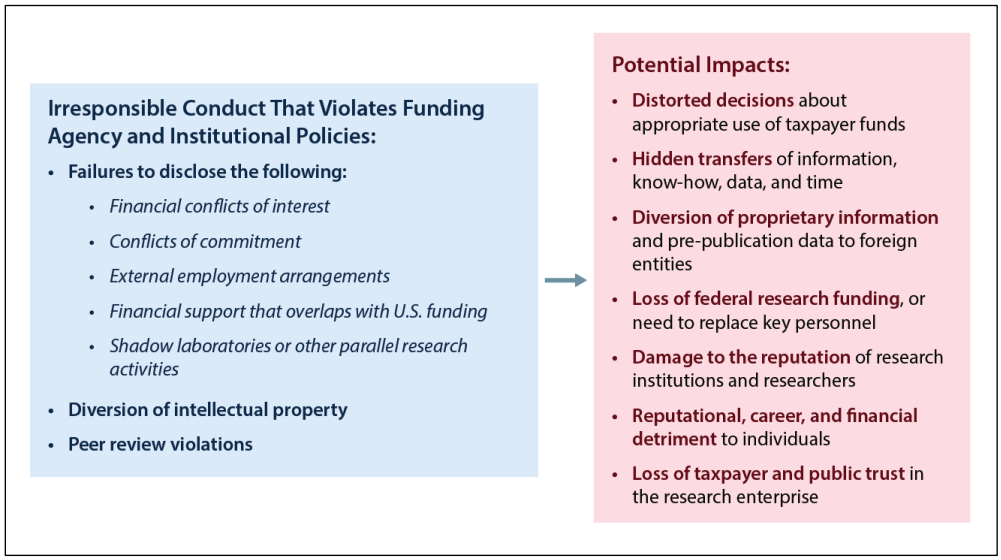
[33] FBI, *Counterintelligence Strategic Partnership Intelligence Note (SPIN): Preventing Loss of Academic Research*, June 2015, p. 1, https://info.publicintelligence.net/FBI-SPIN-ProtectingAcademicResearch.pdf.

[34] FBI, *Counterintelligence Strategic Partnership Intelligence Note (SPIN): Preventing Loss of Academic Research*, p. 1.

held a hearing titled "Foreign Plots Targeting America's Research and Development" to explore "foreign nations' exploitation of U.S. academic institutions for the purpose of accessing and engaging in the exfiltration of valuable [S&T R&D]."[35] On August 20, 2018, then-NIH Director Francis Collins penned a letter to the U.S. academic research community warning of the threats posed by "foreign entities [that] have mounted systematic programs to influence NIH researchers and peer reviewers and to take advantage of the long tradition of trust, fairness, and excellence of NIH-supported research activities" and reaffirming long-standing NIH policies requiring researchers to disclose sources of research support.[36] NIH subsequently, in late 2018, released a report prepared by the Working Group for Foreign Influences on Research Integrity, established under the Advisory Committee to the Director, issuing recommendations related to (1) increasing awareness across the U.S. academic research community of threats posed by talent recruitment programs and (2) strengthening disclosure requirements across the federal government.[37]

Figure 2 provides an overview of the types of reported threats as well as the potential impacts such threats may have on the overall health and performance of the U.S. research ecosystem.

Figure 2. Selected Threats to Research Security and Their Potential Impacts



Source: CRS, based on Office of Science and Technology Policy, "Enhancing the Security and Integrity of America's Research Enterprise," October 15, 2020, p. 11, https://trumpwhitehouse.archives.gov/wp-content/uploads/2020/07/Enhancing-the-Security-and-Integrity-of-Americas-Research-Enterprise.pdf.

Various subsequent reports have specifically highlighted the threats posed by China, which, according to one DOD-sponsored report, aims to establish global economic and military supremacy built on a foundation of technological leadership.[38] Such reports have cited examples

[35] U.S. Congress, House Committee on Science, Space, and Technology, Subcommittee on Oversight, *Foreign Plots Targeting America's Research and Development*, Joint Hearing Before the Subcommittee on Oversight and Subcommittee on Research and Technology, 115th Cong., 2nd sess., April 11, 2018, https://docs.house.gov/meetings/SY/SY21/20180411/108175/HHRG-115-SY21-20180411-SD003.pdf.

[36] Letter from Francis S. Collins, NIH Director, to colleagues, August 20, 2018, https://acd.od.nih.gov/documents/presentations/12132018ForeignInfluences_report.pdf.

[37] NIH ACD, *ACD Working Group for Foreign Influences on Research Integrity*.

[38] Michael Brown and Pavneet Singh, *China's Technology Transfer Strategy: How Chinese Investments in Emerging Technology Enable a Strategic Competitor to Access the Crown Jewels of U.S. Innovation*, January 2018, prepared for the Department of Defense's (DOD's) Defense Innovation Unit Experimental (DIUx). DIUx became DIU later in 2018.

of PRC-backed initiatives, which aim to threaten the integrity of U.S. academic research.[39] For example, the Hoover Institution's 2018 report, *China's Influence & American Interests: Promoting Constructive Vigilance*, documented a number of initiatives directly and indirectly led by the PRC to expropriate U.S. R&D and technical knowledge, including through joint research collaborations, research funding, the sponsorship of Confucius Institutes, and talent recruitment programs.[40]

In 2020, OSTP issued a strategy document, "Enhancing the Security and Integrity of America's Research Enterprise," that included examples of past incidents whereby foreign entities sought to influence or exploit U.S. academic research. These examples included cases of undisclosed conflicts of interest and commitment, distortion of the grant review process, and grant fraud resulting from engagement with foreign entities.[41]

Policy Responses

Concerns about such documented threats and risks, informed the development of federal policies focused on the security of federally funded fundamental research. With the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (P.L. 115-232), the 115th Congress directed the Secretary of Defense to establish an initiative to work with academic institutions to "limit undue influence, including through foreign talent programs, by countries to exploit United States technology within the [DOD] research, science and technology, and innovation enterprise," among other objectives.[42]

The following year, in May 2019, the executive branch convened a group of representatives from federal science agencies to share information and coordinate agency-level research security policies and practices—the Research Security Subcommittee under the NSTC's newly formed Joint Committee on Research Environments (JCORE).[43] Congress codified in statute the work of the NSTC's JCORE Subcommittee on Research Security through the National Defense Authorization Act for Fiscal Year 2020 (P.L. 116-92). The law directed OSTP (acting through the

[39] DOD, "Summary of the 2018 National Defense Strategy," January 19, 2018, https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf; and White House, *National Security Strategy of the United States*, December 2017, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905-2.pdf. For additional background on the state of U.S.-China relations during this period, see CRS Report R45898, *U.S.-China Relations*, coordinated by Susan V. Lawrence.

[40] Working Group on Chinese Influence Activities in the United States, *China's Influence & American Interests: Promoting Constructive Vigilance*, revised, ed. Larry Diamon and Orville Schell (Hoover Institution Press, 2019), https://www.hoover.org/sites/default/files/research/docs/diamond-schell_chineseinfluence_oct2020rev.pdf.

[41] OSTP, "Enhancing the Security and Integrity of America's Research Enterprise," July 2020, https://trumpwhitehouse.archives.gov/wp-content/uploads/2020/07/Enhancing-the-Security-and-Integrity-of-Americas-Research-Enterprise.pdf.

[42] Initiative to Support Protection of National Security Academic Researchers from Undue Influence and Other Security Threats (P.L. 115-232, §1286).

[43] OSTP, *Update from the National Science and Technology Council Joint Committee on Research Environments*, July 9, 2019, https://trumpwhitehouse.archives.gov/wp-content/uploads/2019/07/Update-from-the-NSTC-Joint-Committee-on-Research-Environments-July-2019.pdf; JCORE, *Summary of the 2019 White House Summit of the Joint Committee on the Research Environment (JCORE)*, November 2019, https://trumpwhitehouse.archives.gov/wp-content/uploads/2019/11/Summary-of-JCORE-Summit-November-2019.pdf; and OSTP, "Request for Information on the American Research Environment," 84 *Federal Register* 65194, November 26, 2019, https://www.federalregister.gov/documents/2019/11/26/2019-25604/request-for-information-on-the-american-research-environment. For information about the NSTC's current structure, see CRS Report R47410, *The Office of Science and Technology Policy (OSTP): Overview and Issues for Congress*, by Emily G. Blevins.

NSTC and in consultation with the National Security Advisor) to establish or designate an interagency working group, which would terminate after 10 years, to

> coordinate activities to protect federally funded research and development from foreign interference, cyber attacks, theft, or espionage and to develop common definitions and best practices for Federal science agencies and grantees, while accounting for the importance of the open exchange of ideas and international talent required for scientific progress and American leadership in science and technology.[44]

P.L. 116-92 also specifically directed the working group to update unclassified policy recommendations and that such recommendations should include

- "descriptions of known and potential threats to federally funded [R&D] and the integrity of the [U.S.] scientific enterprise";
- "common definitions and terminology for categorization of research and technologies that are protected";
- the identification of "areas of research or technology that might require additional protections";
- "recommendations for how control mechanisms can be utilized to protect federally funded [R&D] from foreign interference, cyber attacks, theft or espionage, including any recommendations for updates to existing control mechanisms";
- "recommendations for best practices for Federal science agencies, universities, and grantees to defend against threats ... including [the] coordination and harmonization of any relevant reporting requirements";
- "a remediation plan for grantees and universities to mitigate the risks [of] such threats before research grants or contracts are cancelled";
- "recommendations for providing opportunities and facilities for academic researchers to perform controlled and classified research in support of Federal missions";
- "assessments of potential consequences that any proposed practices would have on international collaboration" and U.S. S&T leadership; and
- "a classified addendum, as necessary, to further inform Federal science agency decisionmaking."[45]

P.L. 116-92 also requires the OSTP Director to provide a summary report to relevant congressional committees detailing JCORE's activities and the most current version of research-security-related policy guidance. The OSTP Director is required to issue updated summary reports at least every two years.

JCORE's activities and recommendations informed aspects of the January 2021 NSPM-33, which, as previously noted, established a national security policy for U.S.-government-supported R&D.[46] The following section describes selected provisions from NSPM-33, related

[44] 42 U.S.C. §6601 note; P.L. 116-92, Div. A, Title XVII, §1746.

[45] 42 U.S.C. §6601 note; P.L. 116-92, Div. A, Title XVII, §1746.

[46] JCORE Subcommittee on Research Security, NSTC, *Recommended Practices for Strengthening the Security and Integrity of America's Science and Technology Research Enterprise*, January 2021, p. 1, https://trumpwhitehouse.archives.gov/wp-content/uploads/2021/01/NSTC-Research-Security-Best-Practices-Jan2021.pdf.

implementation guidance issued by OSTP, subsequently enacted legislation, and federal agency implementation actions.

Summary of Key Research Security Policies

Policies and requirements currently governing the security of federally funded research have resulted from an interplay between statutory direction and executive branch guidance. **Table 1** summarizes selected research security policies that aim to prevent foreign interference and exploitation of federally funded R&D. It provides the following for each policy area: stated objectives, relevant statutory authority and/or executive guidance, and relevant deadlines and implementation actions.

Table 1. Overview of Selected U.S. Federal Research Security Policies

As of May 15, 2025

Policy	Summary	*U.S. Code* for Relevant Statute(s)	Relevant Executive Guidance (issue date)	Implementation Status/Deadlines
Disclosure requirements	Specified individuals applying for federal research and development (R&D) support are required to disclose certain information to help funding agencies identify potential conflicts of commitment.	42 U.S.C. §6605	NSPM-33, §4(b)(vi)[a] Common disclosure forms (November 1, 2023)[b] OSTP policy regarding agency use of common disclosure forms (February 14, 2024)[c]	Agencies with extramural research expenditures over $1 million are required to submit an implementation plan to OSTP within 90 days of OSTP's February 14, 2024, policy.[d]
Foreign talent recruitment programs (FTRPs)	Specified federal personnel are prohibited from participating in FTRPs; specified researchers are required to disclose participation in FTRPs; specified researchers are prohibited from participating in malign FTRPs.	42 U.S.C. §19231-2 42 U.S.C. §19237	NSPM-33, §4(c)(ii) Common disclosure forms (November 1, 2023) OSTP policy guidance for agencies on FTRPs (February 14, 2024)[e]	Once fully implemented, common disclosure forms are to require researchers to disclose FTRP participation and certify that they are not party to a malign FTRP at the time of application submission and annually thereafter.
Research security training	Specified federal personnel and researchers applying for federal R&D funding are required to complete research security training.	42 U.S.C. §19234	NSPM-33, §4(f) OSTP guidelines for research security programs (July 9, 2024)[f]	On January 30, 2024, NSF released four online training modules for use by agencies and researchers.[g]

Policy	Summary	*U.S. Code* for Relevant Statute(s)	Relevant Executive Guidance (issue date)	Implementation Status/Deadlines
Research security programs	Covered institutions (defined as those receiving more than $50 million in federal science and engineering support annually) are required to operate research security programs.	42 U.S.C. §19234	NSPM-33, §4(g) OSTP guidelines for research security programs (July 9, 2024)	Agencies must submit planned policy updates to OSTP and OMB by January 9, 2024. Agency policies should take effect no later than six months after final plans are submitted. Covered institutions are expected to implement requirements within 18 months of agency policies taking effect
Information sharing	NSF is required to enter into an agreement with a qualified independent organization to establish a research security and integrity information sharing analysis organization.	42 U.S.C. §19037	NSPM-33, §4(e)	On July 24, 2024, NSF announced a five-year, $67 million award establishing the Safeguarding the Entire Community of the U.S. Research Ecosystem (SECURE) Center to be led by the University of Washington with support from nine other institutions of higher education.[h]

Source: Compiled by CRS from sources cited below.

Notes: OSTP = Office of Science and Technology Policy; NSF = National Science Foundation; OMB = Office of Management and Budget.

a. White House, "Presidential Memorandum on United States Government-Supported Research and Development National Security Policy," NSPM-33, January 14, 2021, https://trumpwhitehouse.archives.gov/presidential-actions/presidential-memorandum-united-states-government-supported-research-development-national-security-policy/.

b. NSF, "Current and Pending (Other) Support Common Form," November 1, 2023, https://www.nsf.gov/bfa/dias/policy/researchprotection/commonform_cps.pdf; and NSF, "Biographical Sketch Common Form," November 1, 2023, https://www.nsf.gov/bfa/dias/policy/researchprotection/commonform_biographicalsketch.pdf.

c. Memorandum from Arati Prabhakar, OSTP Director, to heads of federal research agencies, "Policy Regarding Use of Common Disclosure Forms for the 'Biographical Sketch' and the 'Current and Pending (Other) Support' Sections of Applications by Federal Research Funding Agencies," February 14, 2024, https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/02/OSTP-Common-Disclosure-Form-Policy.pdf.

d. OSTP has not publicly reported whether federal agencies have satisfied this requirement.

e. Memorandum from Arati Prabhakar, OSTP Director, to heads of federal research agencies, "Guidelines for Federal Research Agencies Regarding Foreign Talent Recruitment Programs," February 14, 2024, https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/02/OSTP-Foreign-Talent-Recruitment-Program-Guidelines.pdf.

f. Memorandum from Arati Prabhakar, OSTP Director, to heads of federal research agencies, "Guidelines for Research Security Programs at Covered Institutions," July 9, 2024, https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/07/OSTP-RSP-Guidelines-Memo.pdf.

g. NSF, "NSF Research Security Training Modules Now Available," January 30, 2024, https://new.nsf.gov/news/nsf-research-security-training-modules.

h. NSF, "NSF-Backed SECURE Center Will Support Research Security, International Collaboration," July 24, 2024, https://new.nsf.gov/news/nsf-backed-secure-center-will-support-research.

Though their individual objectives may vary, the research security policies summarized in **Table 1** share common features. For example, they target foreign threats to federally funded fundamental research, the results of which would typically be made publicly available. Collectively, these research security policies comprise a framework that is largely predicated on identifying and mitigating risks associated with certain relationships and behaviors.

Issues for Congress

Seeking to protect future U.S. S&T advances that may arise from fundamental research, federal research security policies target foreign threats of influence and exploitation. Consistent with the policy established by NSDD-189, the policies generally do not involve restricting the conduct or results of federally supported basic and applied research. For example, recently established policies have directed federal research agencies to collect information regarding any outside sources of research support that an investigator might expect to receive during the course of a federal research award. Additional policies and prohibitions relate to researcher participation in foreign-government-sponsored programs seeking to recruit U.S. S&T talent. In both examples, the primary policy focus is on researcher relationships and behaviors during a federally supported research project rather than the nature or content of the research conducted. Any potential limitations on foreign access to the information or results of such projects, therefore, would likely occur, if at all, as an indirect result of these policies.

This approach raises a number of questions for federal agencies as well as for Congress. For example, what relationship or behavior might pose a significant risk to research security? How should federal research funding agencies respond when potentially risky relationships are identified? Should all such agencies be required to agree on a standard notion of risk? Should they follow a common framework in making funding decisions based on identified risks?

In reviewing existing policies to identify potential gaps and assess efficacy, congressional policymakers may face many issues. This section discusses some of the issues related to identifying potential research security threats as well as assessing and mitigating associated risks.

Collection of Information

Congress and the executive branch have established disclosure requirements and related policies that direct agencies to collect specified information from researchers applying for federal research support. Disclosure policies require agencies to use collected information to identify certain types of relationships and associations that may make federal research investments vulnerable to threats of foreign interference and exploitation. A number of issues related to the scope of disclosure requirements may be relevant to consider.

In January 2021, with the enactment of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (P.L. 116-283), Congress mandated that each federal agency require individuals applying for federal research funding to disclose all current and

pending research support during the application process.[47] NSPM-33 provided executive guidance regarding newly established disclosure requirements.[48] Both P.L. 116-283 and NSPM-33 direct agencies to require the disclosure of nonfinancial resources expected to be made available to an individual in support of their R&D efforts. Also referred to as "in-kind contributions," this type of support may include the provision of office or laboratory space, equipment, supplies, employees, or students in exchange for a researcher's commitment of time or resources.[49] Many federal agencies had already required applicants to disclose current and pending financial support, so the direction to disclose nonfinancial support was an expansion of the types of disclosures most agencies required at the time.[50] For example, a December 2020 Government Accountability Office (GAO) report found that, as of FY2018, most agencies did not require applicants to disclose information about nonfinancial conflicts of interest, nor had they established policies to address them.[51]

P.L. 116-283 specifies that federal research agencies may reject a funding application if the disclosed current and pending support violates federal law or agency terms and conditions.[52] It further specifies a number of actions that agencies may take if current and pending support is knowingly omitted from the required disclosure. These actions include steps related to the specific application or award, such as rejecting the application or suspending or terminating the related award. They may also include broader actions, such as temporarily or permanently discontinuing all agency support and/or all future federal support and referring the violation to the agency's inspector general or to federal law enforcement to determine whether any criminal or civil laws were violated.[53]

P.L. 116-283 and NSPM-33 also direct agencies to standardize required disclosure policies. NSPM-33 specifically directed the Office of Management and Budget (OMB) to work with OSTP, the Office of Government Ethics, and other agencies to coordinate the standardization of disclosure policies and forms.[54] On November 1, 2023, NSF released final versions of standardized disclosure forms on behalf of the NSTC Research Security Subcommittee:[55]

- the "Biographical Sketch Common Form," which must be completed by each individual identified as a senior/key person on a federally funded research project, is intended for use by federal agencies to "assess how well qualified the individual, team, or organization is to conduct the proposed activities";[56]

[47] National Defense Authorization Act for Fiscal Year 2021 (P.L. 116-283, §223); 42 U.S.C. §6605.

[48] NSPM-33.

[49] 42 U.S.C. §6605(d).

[50] Preexisting agency policies requiring the disclosure of foreign and domestic sources of financial support are referenced in NIH ACD, *ACD Working Group for Foreign Influences on Research Integrity*, p. 8; and letter from France Córdova, NSF Director, to colleagues, July 11, 2019, https://www.nsf.gov/pubs/2019/nsf19200/research_protection.pdf.

[51] Government Accountability Office (GAO), *Federal Research: Agencies Need to Enhance Policies to Address Foreign Influence*, GAO-21-130, December 17, 2020, https://www.gao.gov/products/gao-21-130.

[52] 42 U.S.C. §6605(c)(1).

[53] 42 U.S.C. §6605(c)(2)(A)-(G).

[54] NSPM-33, §4(b)(vi).

[55] NSF, "NSTC Research Security Subcommittee NSPM-33 Implementation Guidance Disclosure Requirements & Standardization," accessed May 2, 2025, https://www.nsf.gov/bfa/dias/policy/nstc_disclosure.jsp.

[56] NSF, "Biographical Sketch Common Form," November 1, 2023, https://www.nsf.gov/bfa/dias/policy/researchprotection/commonform_biographicalsketch.pdf.

- the "Current and Pending (Other) Support Common Form,"[57] which must also be completed by senior/key personnel on a research project, is used to assess capacity or conflicts of commitment that may impact an applicant's ability to carry out the proposed research effort and also helps federal agencies "assess any potential scientific and budgetary overlap/duplication with the project being proposed"; and
- an updated list of key terms used in NSPM-33 as well as the common forms (e.g., *covered individual or senior/key person*, *conflict of commitment*, *current and pending (other) support*), the definitions for which provide key details regarding the scope of information to be collected.[58]

A February 14, 2024, OSTP memorandum further directs all federal agencies with annual extramural research expenditures over $100 million to require the use of the common forms in all applications for federal research funding.[59] The memorandum also directs agencies to submit implementation plans to OSTP within 90 days of its issuance.[60] Though it is unclear by reviewing publicly available information whether agencies have submitted such plans to OSTP, some agencies have established policies requiring funding applicants to complete the common forms. For example, the most recent version of NSF's *Proposal and Award Policies and Procedures Guide* (*PAPPG*), which outlines policies and requirements that apply to all agency awards as of May 20, 2024, indicates that funding applicants must complete the common forms.[61] Though NIH initially designated May 25, 2025, as the deadline by which all applications should include completed common forms,[62] on March 25, 2025, the agency announced its decision to postpone the requirement, stating

> [t]o further support a successful transition to the Common Forms, NIH is postponing the May 25, 2025 implementation for all applications and Research Performance Progress Reports (RPPRs). NIH will issue future Guide Notices outlining the new effective date and additional implementation details as they are finalized.[63]

Scope of Required Disclosures

Once federal agencies fully incorporate the common disclosure forms into their funding application processes, the forms may facilitate agency identification of potential vulnerabilities

[57] NSF, "Current and Pending (Other) Support Common Form," November 1, 2023, https://www.nsf.gov/bfa/dias/policy/researchprotection/commonform_cps.pdf.

[58] NSF, "National Security Presidential Memorandum-33 Implementation Guidance. Appendix: Definitions."

[59] *Extramural research* generally refers to federally funded research performed by businesses, universities and colleges, other nonprofit institutions, state and local governments, and foreign organizations. See NSF, "Research and Development: U.S. Trends and International Comparisons," *Science and Engineering Indicators 2024*, NSB-2024-6, May 21, 2024, https://ncses.nsf.gov/pubs/nsb20246.

[60] Memorandum from Arati Prabhakar, OSTP Director, to heads of federal research agencies, "Policy Regarding Use of Common Disclosure Forms for the 'Biographical Sketch' and the 'Current and Pending (Other) Support' Sections of Applications by Federal Research Funding Agencies," February 14, 2024, https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/02/OSTP-Common-Disclosure-Form-Policy.pdf.

[61] NSF, "Summary of Changes to the PAPPG (NSF 24-1)," p. IV-2, https://www.nsf.gov/policies/pappg/24-1/summary-changes. PAPPG refers to the *Proposal & Award Policies and Procedures Guide*, NSF-24-1.

[62] NIH, "NIH's Adoption of Common Forms for Biographical Sketch and Current and Pending (Other) Support by May 25, 2025," NOT-OD-24-163, July 31, 2024, https://grants.nih.gov/grants/guide/notice-files/NOT-OD-24-163.html.

[63] See "Timing" section of NIH, "Common Forms for Biographical Sketch and Current and Pending (Other) Support," accessed May 2, 2025, https://grants.nih.gov/policy-and-compliance/implementation-of-new-initiatives-and-policies/common-forms-for-biosketch; and "Related Announcements" section of "NIH's Adoption of Common Forms for Biographical Sketch and Current and Pending (Other) Support by May 25, 2025," NOT-OD-24-163, July 31, 2024.

that could be exploited by foreign adversaries. The quantity and character of potential vulnerabilities identified, however, may depend on the type of information required to be disclosed. The "Current and Pending (Other) Support Common Form" provides the following description of what constitutes current and pending (other) support, which must be submitted to a funding agency along with a funding application:

> (a) All resources made available, or expected to be made available, to an individual in support of the individual's research and development efforts, regardless of (i) whether the source is foreign or domestic; (ii) whether the resource is made available through the entity applying for a research and development award or directly to the individual; or (iii) whether the resource has monetary value; and (b) includes in-kind contributions requiring a commitment of time and directly supporting the individual's research and development efforts, such as the provision of office or laboratory space, equipment, supplies, employees, or students.[64]

This description indicates that sources of foreign support, whether financial or nonfinancial, may not need to be disclosed if they do not specifically support an applicant's professional R&D efforts. Policymakers may consider whether collecting information about foreign sources of support more broadly would reveal a wider range of potential vulnerabilities and whether such collection might be viewed as intrusive or violative of a person's privacy.

In addition, considering who is required to disclose such information may raise relevant issues. The common forms indicate that each individual identified as a "senior/key person on a Federally funded research project" will be required to complete each form when submitting a funding application. The common forms state that a *covered individual or senior/key person* is

> an individual who (a) contributes in a substantive, meaningful way to the scientific development or execution of a research and development project proposed to be carried out with a research and development award from a Federal research agency; and (b) is designated as a covered individual by the Federal research agency concerned. Consistent with NSPM-33, this means principal investigators (PIs) and other senior/key person seeking or receiving Federal research and development funding (i.e., extramural funding) and researchers at Federal agency laboratories and facilities (i.e., intramural researchers, whether or not federally employed), including Government-owned, contractor-operated laboratories and facilities.[65]

The "Current and Pending (Other) Support Common Form" further clarifies who may not be considered a senior/key person, stating that "In accordance with the NSPM-33 Implementation Guidance, senior/key persons typically do not include graduate students."[66] Congress might consider whether the scope of the *senior/key person* definition enables agency identification through disclosures of the full range of possible vulnerabilities.

Another potential issue relates to the frequency with which disclosures are required to be updated. In addition to requiring disclosures at the time of application submission, the "Current and Pending (Other) Support Common Form" provides the following direction on when disclosures should be updated:

> The individual agrees to update this disclosure at the request of the Federal research funding agency prior to the award of support and at any subsequent time the agency

[64] NSF, "National Security Presidential Memorandum-33 Implementation Guidance. Appendix: Definitions."

[65] NSF, "National Security Presidential Memorandum-33 Implementation Guidance. Appendix: Definitions."

[66] NSF, "Current and Pending (Other) Support Common Form," footnote 1.

> determines appropriate during the term of the award. (Refer to the Federal research funding agency's policy on updating award support).[67]

Congress might consider whether federal agencies should be required to harmonize policies relating to post-award disclosures. Variations in agency policies may be burdensome for researchers and institutions—a complication the common forms were intended to address. Congress may also consider whether to specify the frequency with which agencies require post-award disclosures, if at all. Though requiring disclosure updates throughout the life of an award (e.g., annually, quarterly, or within a certain time period after a change occurs) may reveal new vulnerabilities related to researcher affiliations, it would also increase administrative costs for agencies as well as researchers and institutions tasked with providing the updated information.

Identification of Potential Vulnerabilities

Federal Agency Review of Researcher Disclosures

Congress may evaluate existing statutory and executive direction to agencies on reviewing disclosures for potential vulnerabilities. Relevant questions for consideration may include the following: What do federal agencies seek to learn from information disclosed by researchers? What specific guidance has Congress and the executive branch given to agencies on reviewing disclosures for potential vulnerabilities? NSPM-33 provides that "participants with significant influence on the United States R&D enterprise [should] fully disclose information that can reveal potential conflicts of interest and conflicts of commitment."[68] *Conflict of interest* is defined primarily in terms of financial relationships that may be of concern. NSPM-33 defines *conflict of commitment* in a way that encompasses a wider scope of potentially concerning scenarios:

> the term "conflict of commitment" or "conflicts of commitments" means a situation in which an individual accepts or incurs conflicting obligations between or among multiple employers or other entities. Many institutional policies define conflicts of commitment as conflicting commitments of time and effort, including obligations to dedicate time in excess of institutional or funding agency policies or commitments. Other types of conflicting obligations, including obligations to share improperly information with, or to withhold information from, an employer or funding agency, can also threaten research security and integrity, and are an element of a broader concept of conflicts of commitment.[69]

It further directs agencies to "identify, in cooperation with agency Inspectors General and law enforcement agencies as appropriate and as consistent with applicable law, disclosures that have the potential negatively to impact research funding, security, or integrity."[70] Though the "Current and Pending (Other) Support Common Form" states that agencies are to use information collected via the form to "assess the capacity or any conflicts of commitment that may impact the ability of the individual to carry out the research effort as proposed," it does not indicate that agencies are to assess disclosures for potential security vulnerabilities.[71] Likewise, the "Biographical Sketch Common Form" indicates that agencies are to use the information collected for a narrower

[67] NSF, "Current and Pending (Other) Support Common Form."

[68] NSPM-33.

[69] NSPM-33.

[70] NSPM-33, §3(iii).

[71] NSF, "Current and Pending (Other) Support Common Form."

purpose than NSPM-33 describes, specifically, to "assess how well qualified the individual, team, or organization is to conduct the proposed activities."[72]

Neither P.L. 116-283 nor NSPM-33 provide unified guidance to agencies regarding how to determine whether specific behaviors or affiliations constitute a conflict of commitment, whether such disclosed information might constitute a vulnerability capable of compromising the security of federal research, and what, if anything, an agency should do in response. Rather, in P.L. 116-283, Congress provides agencies discretion in making such substantive assessments by stating that "[a] Federal research agency may reject an application for a research and development award if the current and pending research support disclosed by an individual … violates Federal law or agency terms and conditions."[73]

In practice, federal agencies seemingly focus reviews of disclosures on identifying instances where researchers have intentionally omitted or falsified disclosed information. P.L. 116-283 provides specific guidance on the types of actions agencies may take in response to knowingly failing to disclose the required information. Such actions include rejecting the application, suspending or terminating an ongoing R&D award, temporarily or permanently discontinuing any or all funding made to a particular individual or entity, and temporarily or permanently suspending or debarring an individual or entity from receiving any future federal support.[74] Actions reportedly taken by NIH and NSF have largely focused on identifying and penalizing violations of disclosure policies.[75]

Congress may weigh whether to provide specific guidance to federal agencies on their review of required disclosures for research security vulnerabilities in addition to conflicts of commitment and research qualifications. Though specific statutory guidance might provide clearer direction to agencies and researchers regarding how disclosures are to be reviewed, establishing fixed definitions of vulnerabilities may limit federal agency abilities to adjust review criteria in response to an evolving threat landscape. More broadly, Congress might weigh the possible benefits of requiring researcher disclosures via the common forms against the potential costs. For example, policymakers might consider whether the administrative costs associated with disclosure form implementation (for agencies, universities, and individual researchers) outweigh the potential benefits associated with identifying conflicts of commitment. In considering these trade-offs, Congress might assess whether the types of information collected help agencies identify potential vulnerabilities that need to be addressed in order to mitigate the threats of foreign influence and exploitation facing the U.S. research enterprise.

[72] NSF, "Biographical Sketch Common Form," November 1, 2023.

[73] 42 U.S.C. §6605(c)(1).

[74] 42 U.S.C. §6605(c)(2).

[75] See NSF, "Research Security," February 2023, https://nsf-gov-resources.nsf.gov/2023-03/ResearchSecurity_Feb2023.pdf?VersionId=mhC5j7Cn1EC.MY_vZ63ixcRITJYQ18t; NIH, "Foreign Interference Data," accessed April 15, 2025, https://grants.nih.gov/policy-and-compliance/policy-topics/foreign-interference/fi-data; Jeffrey Mervis, "NSF's Handful of Foreign Influence Cases May Be Due to How It Investigates Them," *Science*, July 14, 2020, https://www.science.org/content/article/nsf-s-handful-foreign-influence-cases-may-be-due-how-it-investigates-them-0; Jeffrey Mervis, "Fifty-Four Scientists Have Lost Their Jobs as a Result of NIH Probe into Foreign Ties," *Science*, June, 12, 2020, https://www.science.org/content/article/fifty-four-scientists-have-lost-their-jobs-result-nih-probe-foreign-ties; and Andrew Silver, "Exclusive: US National Science Foundation Reveals First Details on Foreign-Influence Investigations," *Nature*, July 7, 2020, https://www.nature.com/articles/d41586-020-02051-8.

Vulnerabilities Associated with Foreign Talent Recruitment Programs

Statute and executive guidance have also identified participation in certain foreign talent recruitment programs as exposing U.S. academic research to foreign influence. OSTP defines a *foreign talent recruitment program* as

> any program, position, or activity that includes compensation in the form of cash, in-kind compensation, including research funding, promised future compensation, complimentary foreign travel, things of non de minimis value, honorific titles, career advancement opportunities, or other types of remuneration or consideration directly provided by a foreign country at any level (national, provincial, or local) or their designee, or an entity based in, funded by, or affiliated with a foreign country, whether or not directly sponsored by the foreign country, to an individual, whether directly or indirectly stated in the arrangement, contract, or other documentation at issue.[76]

NSPM-33 directed agency heads to establish or clarify existing policies that prohibit federal personnel who are also participants in the U.S. R&D enterprise from participating in foreign-government-sponsored talent recruitment programs.[77] Through Section 10631 of P.L. 117-167 (commonly known as the CHIPS and Science Act), Congress directed OSTP, in coordination with the NSTC Subcommittee on Research Security, to publish a uniform set of guidelines for research agencies that shall

- prohibit all federal research agency personnel from participating in a foreign talent recruitment program;
- require covered individuals (e.g., researchers receiving federal funds) to disclose if they are "party to a foreign talent recruitment program contract, agreement, or other arrangement"; and
- require federal funding recipients (e.g., universities) "to prohibit covered individuals participating in malign foreign talent recruitment programs from working on projects supported by" federal R&D awards, to the extent practicable.[78]

"Covered individuals" who are involved in federally sponsored R&D projects are required to disclose their participation in foreign talent recruitment programs. These are understood to be principal investigators and other senior/key persons seeking or receiving federal R&D funding and researchers at federal agency laboratories and facilities. Section 10631 of P.L. 117-167 prohibits "covered individuals" from participating in a federally funded research project if they are currently participating in a malign foreign talent recruitment program. The definition of *malign foreign talent recruitment program* is codified at 42 U.S.C. §19237 (for the full definition, see the **Appendix**).

Congress might consider whether the scope of the malign foreign talent recruitment program prohibition is sufficient to address potential risks. In addition to describing characteristics of such programs, the statutory definition references lists maintained by DOD pursuant to Section 1286 of P.L. 115-232 that identify "foreign institutions engaging in problematic activity" and "foreign

[76] Memorandum from Arati Prabhakar, OSTP Director, to heads of federal research agencies, "Guidelines for Federal Research Agencies Regarding Foreign Talent Recruitment Programs," February 14, 2024, p. 4, https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/02/OSTP-Foreign-Talent-Recruitment-Program-Guidelines.pdf.

[77] NSPM-33, §4(c)(ii).

[78] 42 U.S.C. §19231.

talent programs that pose a threat to national security."[79] In July 2024, DOD updated these lists and identified new and previously known "foreign institutions engaging in problematic activity," and provided an unchanged list of five foreign talent programs.[80] A 2024 majority staff report of the House Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party referred to the DOD's list of malign talent programs as "wildly underinclusive."[81] Potential limitations of the DOD lists were also referenced during a March 2025 hearing of the House Science, Space, and Technology Committee's Investigations and Oversight Subcommittee.[82] Hearing witness Jeffrey Stoff, President of the Center for Research Security and Integrity, noted in testimony that the Section 1286 lists do not include a number of institutions collaborating with PRC organizations that could pose risks.[83]

On the other hand, expanding the definition of malign foreign talent recruitment programs may increase challenges to international collaboration. For example, OSTP's February 2024 policy memorandum emphasizes that certain international collaboration activities should be excluded from foreign talent recruitment prohibitions, stating that

> [t]his exclusion allows federal research agency personnel to engage in these activities. These activities primarily involve open and reciprocal exchange of scientific information aimed at advancing international scientific understanding.[84]

In addition, the memorandum and the common disclosure forms reiterate the specific types of international collaborations outlined in P.L. 117-167 that generally should not be prohibited unless they are "funded, organized, or managed" by an academic institution or a foreign talent recruitment program included on the lists managed by DOD, per P.L. 115-232.[85] Such activities include

> (i) making scholarly presentations and publishing written materials regarding scientific information not otherwise controlled under current law;
>
> (ii) participation in international conferences or other international exchanges, research projects or programs that involve open and reciprocal exchange of scientific information,

[79] DOD, "DOD Releases Updated List of Foreign Institutions Engaging in Problematic Activities to Counter Unauthorized Technology Transfer," press release, July 19, 2024, https://www.defense.gov/News/Releases/Release/Article/3844699/.

[80] DOD, "Introduction to FY23 Lists Published in Response to Section 1286 of the National Defense Authorization Act for Fiscal Year 2019 (P.L. 115-232), as amended," July 2024, https://rt.cto.mil/wp-content/uploads/2024/07/FY23-Lists-Published-in-Response-to-Section-1286-of-NDAA-2019_clearedv2.pdf.

[81] U.S. Congress, House Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party, *CCP on the Quad: How American Taxpayers and Universities Fund the CCP's Advanced Military and Technological Research*, majority staff report, 118th Cong., 2nd sess., September 2024, p. 58, https://selectcommitteeontheccp.house.gov/sites/evo-subsites/selectcommitteeontheccp.house.gov/files/evo-media-document/RS%20Report%20Cover%20Final%20(1)-merged-compressed%20(2).pdf.

[82] U.S. Congress, House Science, Space, and Technology Committee, Investigations and Oversight Subcommittee, *Assessing the Threat to U.S. Funded Research*, hearing, 119th Cong., 1st sess., March 5, 2025, https://science.house.gov/2025/3/assessing-the-threat-to-u-s-funded-research.

[83] Written testimony of Jeffrey Stoff, U.S. Congress, House Science, Space, and Technology Committee, Investigations and Oversight Subcommittee, *Assessing the Threat to U.S. Funded Research*, hearing, 119th Cong., 1st sess., March 5, 2025, https://science.house.gov/2025/3/assessing-the-threat-to-u-s-funded-research.

[84] Memorandum from Arati Prabhakar, OSTP Director, to heads of federal research agencies, "Guidelines for Federal Research Agencies Regarding Foreign Talent Recruitment Programs," February 14, 2024, p. 3, https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/02/OSTP-Foreign-Talent-Recruitment-Program-Guidelines.pdf.

[85] 42 U.S.C. §19232(d).

> and which are aimed at advancing international scientific understanding and not otherwise controlled under current law; [and]
>
> (iii) advising a foreign student enrolled at an institution of higher education or writing a recommendation for such a student, at such student's request.[86]

How Congress conceptualizes the scope of foreign talent recruitment programs, especially those identified as malign, might directly or indirectly impact the modes of international collaboration available to researchers. For example, a 2021 American Physical Society press release asserted that research security policies resulted in a chilling effect on international scientific collaboration, causing researchers to "withdraw from international collaborations that bring new scholars, ideas and techniques to the U.S. research and development ecosystem."[87] Others might argue that the perceived risk associated with international collaboration outweighs any positive impact from a narrowing of or exceptions to research security policies.

Assessment and Mitigation of Security Risks

To date, executive and congressional direction has focused on ensuring that U.S. agencies and institutions of higher education maintain compliance with required disclosures and strengthening processes and responses to confirmed violations of disclosure policies. Congress, however, has separately directed certain individual agencies to assess security risks when making awards. How agencies assess risk on the basis of researcher disclosures—how they define risk, how they determine risk levels, and the consistency with which they do so—may raise challenges.

P.L. 117-167, authorized the NSF Director, acting through the Office of Research Security and Policy and in coordination with the NSF's Office of Inspector General, to conduct risk assessments of research applications and researcher disclosures.[88] In response, the most recent version of NSF's *PAPPG*, from 2024, lists a number of reasons NSF may return a proposal prior to the merit review stage, including if it "has the potential to negatively impact research security due to credible information of a national security concern (note: NSF envisions that such returns without review on this basis will be rare)."[89]

Congress has also directed other individual agencies and programs to develop risk assessment tools and frameworks:

- P.L. 117-328, Division FF, Title II, Subtitle C, Section 2322, requires the Secretary of the Department of Health and Human Services (HHS) to develop a comprehensive framework and policies for assessing and managing national security risks before and after making funding awards as well as risks associated with granting access to data that may pose national security concerns.
- P.L. 117-183 (15 U.S.C. §638(vv)) requires the head of each federal agency with an SBIR or STTR program to establish and implement a "due diligence program" to assess potential security risks associated with a small business seeking an award under the program. The due diligence program is required to assess, among other aspects, foreign ownership of a small business seeking an award,

[86] NSF, "National Security Presidential Memorandum-33 Implementation Guidance. Appendix: Definitions."

[87] American Physical Society, "US Approach to Research Security Threatens Scientific Enterprise," press release, December 20, 2021, https://www.aps.org/about/news/2021/12/research-security-scientific-enterprise.

[88] P.L. 117-167, Div. B, Title III, §10336.

[89] NSF, "Chapter IV.B: Proposed Not Accepted or Returned Without Review," in *Proposal and Award Policies and Procedures Guide*, NSF-24-1, effective May 20, 2024, p. IV-2, https://nsf-gov-resources.nsf.gov/files/nsf24_1.pdf?VersionId=ImnVCR.NDkOKTGKuDHHmterZQY3cXEDn.

including the financial ties and obligations of the small business and employees of the small business to a foreign country, foreign person, or foreign entity.

- P.L. 117-167, Division B, Title I, Section 10114, requires the Secretary of Energy to develop and maintain tools and processes to manage and mitigate research security risks.

Agencies such as NSF,[90] NIH,[91] and the Department of Energy (DOE)[92] have developed risk matrices and associated policies that indicate how security risks might be evaluated in each agency's context. It is unclear whether additional agencies will develop similar risk assessment tools to guide research funding decisions. As previously noted, agency implementation of disclosure requirements and policies outlined in OSTP's February 2024 memorandum is ongoing.[93] Congress might continue to monitor ongoing implementation efforts in order to assess the extent to which agencies are evaluating disclosures, as well as proposals more broadly, for potential security risks. Policymakers also might consider whether agencies may need additional statutory direction, authorities, and/or funding to enable risk assessment activities.

In evaluating existing risk assessment tools developed by individual agencies, Congress might consider the extent to which agencies should or should not rely on a consistent conception of risk. In response to statutory direction, individual agencies have developed risk assessment tools that appear to vary in the types of factors they identify as posing a potential risk (see **Table 2**).

[90] Office of the Chief of Research Security Strategy and Policy (OCRSSP), "Trusted Research Using Safeguards and Transparency (TRUST)," June 5, 2024, https://nsf-gov-resources.nsf.gov/files/NSF%20OCRSSP%20TRUST%20Policy%20Memo.pdf.

[91] NIH, "NIH Decision Matrix for Assessing Potential Foreign Interference for Covered Individuals or Senior/Key Personnel," August 15, 2024, https://grants.nih.gov/sites/default/files/NIH%20Decision%20Matrix%20for%20Assessing%20Potential%20Foreign%20Interference%20for%20Covered%20Individuals%20or%20Senior%207%2026%2024%20clean.pdf.

[92] David M. Turk, "Department of Energy Research, Technology, and Economic Security Framework for Financial Assistance and Loan Activities," Department of Energy, November 26, 2024, https://www.energy.gov/sites/default/files/2024-11/DOE%20RTES%20Framework%20Memorandum%2011.26.2024.pdf.

[93] As of March 25, 2025, NIH has postponed its transition planned for May 25, 2025, to implement the common forms for all research applications. See NIH, "Common Forms for Biographical Sketch and Current and Pending (Other) Support: Timing," accessed April 13, 2025, https://grants.nih.gov/policy-and-compliance/implementation-of-new-initiatives-and-policies/common-forms-for-biosketch#timing.

Table 2. Selected Federal Agency Risk Review Processes

Risk Factors and Specific Mitigation Measures Cited by Each Agency

Federal Agency (Scope of Review)	Key Risk Factor(s)	Mitigation Measures	Related Agency Review Policies Cited
Department of Energy (DOE) (DOE and National Nuclear Security Administration financial assistance and loan activities)	Identifies the following as potential risk factors: specified activities/affiliations of individuals and entities; timing of activity/entity and whether it constitutes an isolated incident or pattern; and specified technology considerations	Specifies that the following mitigation measures may be used: (1) certifications, (2) tailored mitigation agreements, (3) reporting, and (4) special terms and conditions Does not indicate specific instances where mitigation measures may be used	None specified
National Institutes of Health (NIH) (NIH grant applications and ongoing awards)	Identifies the following as potential risk factors: indicators of undisclosed or incompletely disclosed past or ongoing foreign sources of funding, affiliations, or participation in FTRPs or MFTRPs	Indicates instances where mitigation measures may be suggested or required; does not indicate specific mitigation measures	Cites NIH grant policy GPS 4.1.37, which prohibits awardees from using federal funds for certain telecommunications and video surveillance services or equipment per P.L. 115-232[a] Cites NIH grant policy GPS 8.1.2, which indicates prior approval is needed from NIH for all projects involving "foreign components"[b]
National Science Foundation (NSF) (Subset of research proposals and ongoing projects focused on specific subject areas)[c]	Identifies the following as potential risk factors: concerning appointments and research support, noncompliance with disclosure and other requirements, and potential risks to national security	Indicates that based on results of the review, mitigation measures may be required Does not indicate specific instances that may warrant mitigation or specific mitigation measures that may be used	None specified

Source: CRS analysis of David M. Turk, "Department of Energy Research, Technology, and Economic Security Framework for Financial Assistance and Loan Activities," Department of Energy, November 26, 2024, https://www.energy.gov/sites/default/files/2024-11/DOE%20RTES%20Framework%20Memorandum%2011.26.2024.pdf; National Institutes of Health (NIH), "NIH Decision Matrix for Assessing Potential Foreign Interference for Covered Individuals or Senior/Key Personnel," August 15, 2024, https://grants.nih.gov/sites/default/files/NIH%20Decision%20Matrix%20for%20Assessing%20Potential%20Foreign%20Interference%20for%20Covered%20Individuals%20or%20Senior%207%2026%2024%20clean.pdf; and Office of the Chief of Research Security Strategy and Policy, "Trusted Research Using Safeguards and Transparency (TRUST)," NSF, June 5, 2024, https://nsf-gov-resources.nsf.gov/files/NSF%20OCRSSP%20TRUST%20Policy%20Memo.pdf.

Notes: FTRP = foreign talent recruitment program; MFTRP = malign foreign talent recruitment program.

a. NIH, "Prohibition on Certain Telecommunications and Video Surveillance Service Equipment," Grants Policy Statement (GPS) 4.1.37, April 2024, https://grants.nih.gov/grants/policy/nihgps/HTML5/section_4/4.1.37_prohibition_on_certain_telecommunications_and_video_surveillance_services_or_equipment.htm.

b. Foreign components defined at National Institute of Neurological Disorders and Stroke, "Applications with Foreign Components," accessed on April 15, 2025, https://www.ninds.nih.gov/funding/manage-your-award/pre-award/applications-foreign-components; NIH, "Prior Approval Requirements," GPS 8.1.2, April 2024, https://grants.nih.gov/grants/policy/nihgps/HTML5/section_8/8.1.2_prior_approval_requirements.htm; and NIH, "Foreign Component Added to a Grant to a Domestic or Foreign Organization," GPS 8.1.2.10, April 2024, https://grants.nih.gov/grants/policy/nihgps/HTML5/section_8/8.1.2_prior_approval_requirements.htm#Foreign.

c. As of 2024, NSF intended to deploy the TRUST framework in three phases. During the first phase, which NSF anticipated beginning during FY2025, the review framework would be applied to "quantum-related proposals after they undergo merit review." During the second phase, the "pilot will be expanded to include other *CHIPS and Science Act* key technology areas." During the third phase, the "scope of projects" would be expanded to include "all *CHIPS and Science Act* key technology areas" (see Office of the Chief of Research Security Strategy and Policy, "Trusted Research Using Safeguards and Transparency (TRUST)," NSF, June 5, 2024). Key technology areas referenced are included in Section 10387 of the CHIPS and Science Act (P.L. 117-167; 42 U.S.C. §19107).

Risk assessment frameworks developed by individual agencies may also vary in scope and focus. For example, the 2024 DOE framework indicated that the rubric is expected to be used to review, what at least appears to be, all "financial assistance and loan activities," and the NIH framework indicates that the rubric would be used to review, what at least appears to be, all "grant applications and ongoing awards."[94] By contrast, the 2024 NSF framework indicated a phased process by which the rubric is expected to be used to review a subset of funding proposals identified on the basis of specified criteria. According to NSF in 2024, beginning in FY2025, NSF intended to apply its Trusted Research Using Safeguards and Transparency (TRUST) framework to quantum-related proposals once the proposals have undergone merit review.[95]

In considering whether to direct agency risk assessment activities, Congress might weigh whether certain fields of fundamental research may involve greater degrees of risk than others. For example, fundamental research related to critical and emerging technologies may involve heightened risks given that research outcomes in these areas could enable both economic and military advances. Therefore, the DOE and NSF frameworks both consider research subject matter when assessing potential risk factors associated with a particular researcher, project, or collaboration. DOE indicates that if risk factors are identified during review of a proposed or an existing project, such risks would be weighed against "technology considerations." Specifically, in such cases, DOE would consider whether the project also falls within a critical and emerging technology area, involves physical or cyber access to critical infrastructure, or would be conducted in proximity to a military installation.[96]

According to NSF in 2024, beginning with quantum-related research, NSF intended to review selected proposals for "potential foreseeable national security concerns" based on the extent to which they involve research related to the key technology focus areas established by Congress in P.L. 117-167.[97] If sufficient national security risks were identified, NSF planned to work with the

[94] NIH, "NIH Decision Matrix for Assessing Potential Foreign Interference for Covered Individuals or Senior/Key Personnel."

[95] OCRSSP, "Trusted Research Using Safeguards and Transparency (TRUST)."

[96] David M. Turk, "Department of Energy Research, Technology, and Economic Security Framework for Financial Assistance and Loan Activities."

[97] 42 U.S.C. §19107.

researcher's institution to explore "the necessity and options for mitigating those risks."[98] It is unclear what potential mitigation measures might involve.

Though research in fields such as quantum information science or artificial intelligence may pose unique risks, whether those risks may be great enough to warrant curbing international collaboration remains an open question. Congress might weigh such risks against potential benefits of international collaboration in these fields. For example, the previously referenced NSTC report, *Biennial Report to Congress on International Science and Technology Cooperation*, acknowledges that the national security implications inherent to research in fields such as quantum information science pose challenges to international research collaboration. The report also highlights a number of potential benefits to such collaboration—particularly among nations that support transparency in science—including, diversifying

> the U.S. scientific portfolio, increasing opportunities for access to discoveries as they occur, and allowing the United States to benefit from the range of research strategies and priorities being pursued by allies and partners. Standards-setting, talent management, and supply chains are other areas that will require international cooperation to secure U.S. leadership in a rules-based global [quantum information science] ecosystem.[99]

Options for Congress

Congressional policymakers have a variety of options regarding the security of federally funded research. They may oversee the executive branch development and implementation of the current research security policy framework. Congressional policymakers might increase oversight activities and direct the Administration, either through hearings, report language, or legislation, to take specific actions to address issues insufficiently addressed by existing policies. Congress may disagree with excluding federally funded basic and applied research from information and technology controls and remove or revise such exclusions. Should they hold this view, policymakers may view incremental changes to existing policies as insufficient and decide to employ substantively different mechanisms to secure research through alternative frameworks.

Oversee Current Policy Framework

Policymakers may choose to continue allowing the current research security policy framework to develop as implementation of relevant statutory and congressional guidance is ongoing. Federal agencies are developing rules and procedures to implement disclosure policies and risk-based reviews of research funding proposals. Citing the burdens associated with implementing additional research security requirements, groups that represent institutions of higher education, such as the Association of American Universities (AAU) and the Association of Public and Land-Grant Universities (APLU), generally support this approach. For example, in a joint letter to the House and Senate Armed Services Committees regarding research security provisions under consideration prior to enactment of the FY2025 National Defense Authorization Act (P.L. 118-159), the presidents of AAU and APLU urged Congress to

> allow for existing requirements to be fully implemented and for their outcomes to be assessed before adding additional regulations. We believe that this would allow for more well-informed legislative approaches to address any remaining or newly evolved security

[98] OCRSSP, "Trusted Research Using Safeguards and Transparency (TRUST)."

[99] Subcommittee on International Science and Technology Coordination, NSTC, *Biennial Report to Congress on International Science & Technology Cooperation*, February 2024, p. 9, https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/02/2024-Biennial-Report-to-Congress-on-International-Science-Technology-Cooperation.pdf.

> gaps and prevent the creation of duplicative, conflicting, unnecessary, and, in some cases, potentially counterproductive new research security requirements.[100]

Congress could decide that agencies need additional time to complete implementation and determine whether current policies adequately address potential threats of foreign exploitation and influence over the U.S. research ecosystem. Congress may also closely monitor the speed and consistency with which federal agencies implement statutory requirements through oversight activities, such as requests for information from the Administration, or through additional oversight hearings.[101]

Measure Outcomes

Congress's ability to evaluate the extent to which existing and future policies achieve desired levels of security and openness in federally funded research depends on access to certain information and data. The scope and significance of research security threats, as well as related policy violations, may inform policymakers' perceptions.

Congress might direct individual agencies to regularly report on research security violations, mitigation measures required, and the progress of implementing disclosure requirements. Congress might require the generation of centralized, comprehensive data on the frequency and potential severity of research security policy violations as well as agency-mandated mitigation measures across federal R&D funding agencies. Without such data, it may be difficult to both measure the outcomes and evaluate the efficacy of current research security policies and requirements.

Congress has established such reporting requirements for certain agencies. In 2022, Congress enacted the Prepare for and Respond to Existing Viruses, Emerging New Threats, and Pandemics Act, as part of the Consolidated Appropriations Act, 2023 (P.L. 117-328, Division FF, Title II).[102] It included a number of provisions that directed the Secretary of HHS and the Director of NIH to establish certain policies and take specific actions to prevent undue foreign influence in biomedical research. Section 2326 of P.L. 117-328 required the HHS Secretary to report to specified congressional committees no later than December 29, 2023, on actions taken to prevent, address, and mitigate instances of noncompliance with disclosure requirements as well as actions taken to address noncompliance with disclosure requirements.[103] In November 2023, NIH published a report that summarizes various characteristics and outcomes of the agency's "foreign interference compliance reviews" from 2018 to 2023.[104] In addition, NIH has semiannually published data on foreign interference cases on its website.[105]

---

[100] Association of American Universities (AAU), "AAU Submits Joint Letter on FY25 NDAA," press release, September 25, 2024, https://www.aau.edu/key-issues/aau-submits-joint-letter-fy25-ndaa.

[101] U.S. Congress, House Science, Space, and Technology Committee, Full Committee, *Examining Federal Science Agency Actions to Secure the U.S. Science and Technology Enterprise*, 118th Cong., 2nd sess., February 15, 2024, https://science.house.gov/2024/2/full-committee-hearing-examining-federal-science-agency-actions-to-secure-the-u-s-science-and-technology-enterprise.

[102] For a more detailed analysis of research-security-related provisions of P.L. 117-328, which are specific to the Department of Health and Human Services (HHS) and NIH, as well as additional provisions of the act, see CRS Report R47649, *PREVENT Pandemics Act (P.L. 117-328, Division FF, Title II)*, coordinated by Kavya Sekar.

[103] P.L. 117-328, §2326.

[104] Michael Lauer and Patricia Valdez, "Brief Summary of NIH Foreign Interference Cases," NIH, November 28, 2023, https://grants.nih.gov/sites/default/files/Foreign-Interference-11-26-23-report.pdf.

[105] NIH, "Foreign Interference Data," accessed April 15, 2025, https://grants.nih.gov/policy-and-compliance/policy-topics/foreign-interference/fi-data.

Congress might expand the existing HHS reporting requirement in P.L. 117-328, or establish a similar independent reporting requirement, to apply to other research agencies; alter the requirement on the basis of desired data to be collected; or draft a substantively different reporting requirement. Though potentially useful for measuring efficacy, tasking agencies with additional reporting requirements might place further resource demands on such research agencies. Given that these agencies have reportedly terminated employees in government-wide staffing reductions,[106] the additional effort available for such reporting may be limited.

Alternatively, Congress could task an existing interagency body, such as an entity within the NSTC, with reporting on research-security-related metrics as a way to consolidate and streamline review of such metrics from multiple agencies. Though doing so might relieve individual agencies of some administrative burden and provide for greater coordination, this approach could also create challenges, including resource constraints. For example, Section 1746 of P.L. 116-92 authorized an interagency working group and required it to report to Congress biennially on a number of research-security-related policy developments; the act stipulated that the group should terminate 10 years after establishment.[107] The OSTP Director chose to carry out the duties assigned to the interagency working group through the existing Research Security Subcommittee of JCORE.[108] It is unclear whether the group remains active, and it has not issued subsequent biennial reports publicly.

Another option might involve specifically tasking a nongovernmental entity with tracking and reporting on research-security-related data. Such an approach might raise questions about the appropriateness or inefficiency related with such information transfer to a third party. The 117th Congress pursued a similar approach with the establishment of a research security and integrity information sharing analysis organization (RSI-ISAO) to share best practices for research security. P.L. 117-167 required the NSF Director to establish an RSI-ISAO via an agreement with a qualified independent organization and specified that its duties should include "enabl[ing] standardized information gathering and data compilation, storage, and analysis for compiled incident reports."[109] In 2024, NSF announced the establishment of the Safeguarding the Entire Community of the U.S. Research Ecosystem (SECURE) Center to "serve as a clearinghouse for information to empower the research community to identify and mitigate foreign interference that poses risks to the U.S. research enterprise."[110] According to the University of Washington, the SECURE Center is "in the initial stages of planning."[111] In evaluating this option, Congress might consider the federal financial support needed to sustain such an independent organization's activities across a specified length of time, the scope of statutory responsibilities relative to the SECURE Center, and their suitability for the purposes of reporting data to Congress, among other potentially relevant factors.

---

[106] Carla K. Johnson, "Mass Layoffs Are Underway at the Nation's Public Health Agencies," *Federal News Network*, April 1, 2025, https://federalnewsnetwork.com/workforce/2025/04/layoffs-begin-at-the-nations-health-agencies; Mitch Ambrose, "Science Agencies Brace for Mass Layoffs," American Institute of Physics, February 7, 2025, https://ww2.aip.org/fyi/science-agencies-brace-for-mass-layoffs; and Kritika Agarwal, "Uncertainties at Science Agencies Continue as Layoffs Begin," Association of American Universities, February 21, 2025, https://www.aau.edu/newsroom/leading-research-universities-report/uncertainties-science-agencies-continue-layoffs-begin.

[107] 42 U.S.C. §6601 note; P.L. 116-92, Div. A, Title XVII, §1746.

[108] OSTP, *Update from the National Science and Technology Council Joint Committee on Research Environments*, July 9, 2019, https://trumpwhitehouse.archives.gov/wp-content/uploads/2019/07/Update-from-the-NSTC-Joint-Committee-on-Research-Environments-July-2019.pdf.

[109] 42 U.S.C. §19037.

[110] NSF, "NSF-Backed SECURE Center Will Support Research Security, International Collaboration," July 24, 2024, https://www.nsf.gov/news/nsf-backed-secure-center-will-support-research.

[111] For more information, see University of Washington, "Secure Center," https://www.securecenter.uw.edu/.

Evaluate Efficacy

Additional information may aid congressional policymakers in accurately characterizing risk—understanding the likelihood that the threats of foreign exploitation and influence will harm national and economic security—and evaluating the extent to which existing research security policies effectively mitigate that risk. For example, Congress may decide that the threats facing federally funded research and associated risks may be overstated or do not require extensive federal oversight. Some evidence indicates that the number of documented incidents of espionage involving U.S. universities is low—fewer than 10 between 2000 and 2020.[112] Former member of the National Intelligence Council John Gannon has asserted that the major challenge posed by China is not "its illicit and disruptive interference with U.S. research" but its "global competitiveness in scientific research."[113]

Alternatively, Congress could affirm the veracity of threats and risks but decide that the costs associated with current policies may outweigh the potential benefits. For example, Congress may decide that the administrative burden for agencies and institutions of higher education is too high or that current policies unduly impact researchers from specific ethnic backgrounds or discourage international collaboration too generally.[114] Congress could also determine that such threats and risks, though accurately described, extend beyond the scope of what research security policies are currently designed to mitigate. For example, a January 2018 report prepared for DOD's Defense Innovation Unit (DIU) documented a variety of licit and illicit means by which China seeks to acquire U.S. S&T advances (e.g., foreign direct investment, IP theft, industrial espionage), which generally do not involve access to fundamental research.[115] Therefore, Congress might view the risks associated with IP theft and industrial espionage as greater than those associated with foreign access to fundamental research and decide that such risks are more effectively mitigated by an alternative policy framework.

Revise Research Security Policy Framework

Either in conjunction with or as an alternative to oversight activities, Congress may choose to introduce legislation to provide greater direction or focus to the relevant executive branch agencies, directly address perceived policy gaps, or codify certain policies in statute.

---

[112] Center for Strategic and International Studies, *Survey of Chinese Espionage in the United States Since 2000*, March 2023, https://www.csis.org/programs/strategic-technologies-program/survey-chinese-espionage-united-states-2000.

[113] NASEM, *National Science, Technology, and Security Roundtable Capstone: Proceedings of a Workshop*, 2025, p. 16, https://nap.nationalacademies.org/catalog/27976/national-science-technology-and-security-roundtable-capstone-proceedings-of-a.

[114] L. Rafael Reif, "Letter to the MIT Community: Immigration Is a Kind of Oxygen," June 25, 2019, Massachusetts Institute of Technology (MIT) News Office, https://news.mit.edu/2019/letter-community-immigration-is-oxygen-0625; House Science, Space, and Technology Committee Democrats, "ICYMI: Ranking Member Lofgren Joins CAPAC Chair and Oversight Committee Ranking Member to Request GAO Review of Federal Investigations into Foreign Influence on Research," press release, December 12, 2023, https://democrats-science.house.gov/news/press-releases/icymi-ranking-member-lofgren-joins-capac-chair-and-oversight-committee-ranking-member-to-request-gao-review-of-federal-investigations-into-foreign-influence-on-research; and Asian Americans Advancing Justice, "Anti-Profiling, Civil Rights & National Security," accessed May 19, 2025, https://www.advancingjustice-aajc.org/anti-profiling-civil-rights-national-security.

[115] For a discussion of intellectual property theft, see CRS Report R46532, *Intellectual Property Violations and China: Legal Remedies*, coordinated by Kevin J. Hickey; and Michael Brown and Pavneet Singh, *China's Technology Transfer Strategy: How Chinese Investments in Emerging Technology Enable a Strategic Competitor to Access the Crown Jewels of U.S. Innovation*, DIUx, January 2018, https://nationalsecurity.gmu.edu/wp-content/uploads/2020/02/DIUX-China-Tech-Transfer-Study-Selected-Readings.pdf.

Expand the Scope of Disclosure Requirements

In continuing to oversee agency implementation of disclosure requirements, Congress might consider evaluating the scope of such disclosures—both in terms of the information collected as well as who is required to disclose. For example, as the nature of specific threats and foreign influence strategies continue to evolve, Congress may consider whether disclosure requirements capture relevant information that agencies may need to identify potential conflicts of commitment. Currently, required disclosures relate to financial and in-kind support (both foreign and domestic) received in support of an individual's R&D efforts. The "Current and Pending (Other) Support" common disclosure form, for example, defines "current and pending (other) support," in part, as "all resources made available, or expected to be made available, to an individual in support of the individual's research and development efforts."[116]

Congress might consider whether the disclosure of additional information, for example, any foreign support received regardless of its intended use, should be required. Such other categories of foreign financial or in-kind support (e.g., royalties received from patent licensing agreements with foreign entities) may indicate a potential conflict of commitment that could result in foreign influence or exploitation of federally supported R&D. Requiring researchers to disclose these additional categories of information, however, could be perceived as government intrusion into personal privacy.

On the other hand, expanding current disclosure requirements may result in increased costs and administrative requirements for various stakeholder groups within the R&D ecosystem. Institutions of higher education, in particular, have noted the already high costs of complying with disclosure requirements. Expanding their scope—by requiring more individuals to disclose, requiring more frequent disclosure updates, or both—might lead to higher costs. For example, the Council on Governmental Relations (COGR), an association of various research universities, affiliated medical centers, and independent research institutes, issued a November 2022 report that documented the institutional costs of complying with required disclosures.[117] To assess such costs for FY2022, COGR conducted a survey of 26 institutions and found that

> [t]he projected year one average total cost per institution for compliance with the Disclosure Requirements, regardless of institutional size, is significant and concerning. The figure ranges from an average of over $100,000 for smaller institutions to over $400,000 for mid-size and large institutions. Although some of these expenses are onetime costs, a sizeable portion will be annual recurring compliance costs. Overall, the cost impact to research institutions in year one is expected to exceed $50 million. Further, all research institutions will experience significant cost burden and administrative stress, and smaller research institutions with less developed compliance infrastructure may be disproportionately affected.[118]

As COGR's survey indicates, increased institutional costs may have disproportionate effects on smaller institutions.[119] Increased institutional costs also might disproportionately affect under-

[116] See "Current and pending (other) support" definition in NSF, "National Security Presidential Memorandum-33 Implementation Guidance. Appendix: Definitions."

[117] Council on Governmental Relations (COGR), *Research Security and the Cost of Compliance: Phase I Report,* November 2022, p. 3, https://www.cogr.edu/sites/default/files/Version%20Dec%205%202022%20research%20security%20costs%20survey%20FINAL.pdf.

[118] COGR, *Research Security and the Cost of Compliance: Phase I Report*, p. 3.

[119] The disproportionality of such effects may be further intensified by federal agency cuts to indirect cost rates. For an explanation of indirect costs and recent policy changes at NIH, see CRS Insight IN12516, *NIH Indirect Costs Policy for Research Grants: Recent Developments*, by Kavya Sekar and Marcy E. Gallo.

resourced institutions such as many historically Black colleges and universities (HBCUs) and minority-serving institutions (MSIs), broadly.[120]

Require Post-Award Disclosures

Congress might decide to change the current policy regarding updating information contained in disclosures provided at the time of submitting a federal R&D award application. For example, to identify potential conflicts of commitment that might arise after an application is submitted, Congress might direct agencies to require post-award disclosures at a specified frequency throughout the life of the award. Some have argued that the lack of a consistent requirement related to post-award disclosures allows for continued exploitation of federally funded R&D.[121]

Under current policy requirements, individual agencies may determine when to require such post-award disclosures. Congress might create statutory requirements for agencies that would specify when to require researchers to update disclosures after an award is issued. The Grant Recipient Accountability for Necessary Transparency (GRANT) Act of 2023 (H.R. 6642, 118th Congress), for example, would have required R&D award recipients to disclose certain foreign support within 30 days of receipt throughout the award term.

Require Disclosures from Graduate Students

Congress might also require disclosures from a broader range of individuals who may work on, or otherwise be involved with, federally sponsored research projects, such as graduate students. Currently, agencies are to require disclosures from each individual identified as a "senior/key person" on a federally funded research project. This does not include graduate students (or other support and technical staff), who may perform significant portions of research supported by federal awards. If Congress decided that potential conflicts of commitment held by graduate students pose a threat to research security, it might direct federal agencies to require those students to disclose information similar to that disclosed by senior/key individuals. Instituting such a requirement may pose logistical and administrative challenges, though, given that applications for federal R&D support may not contain the names of individual graduate students who may be associated with a prospective award and that graduate students may be only transiently attached to a particular award.

One approach could involve creating separate reporting and disclosure processes for graduate student researchers at specified intervals throughout the life of an award. This approach would likely involve additional financial costs borne by federal agencies and institutions of higher education. Ultimately, Congress might weigh the potential benefits (e.g., risks mitigated and their associated financial benefits) against the potential costs (e.g., resources required) of any changes to current disclosure requirements when considering their scope.

Amend the Foreign Talent Recruitment Program Definition

In addition to considering potential changes to disclosure requirements, Congress might assess how changes to the definition of malign foreign talent recruitment program (42 U.S.C. §19237;

[120] For additional information on minority-serving institutions and historically Black colleges and universities, see CRS Report R43237, *Programs for Minority-Serving Institutions Under the Higher Education Act*, by Cassandria Dortch.

[121] House Select Committee on the Strategic Competition Between the United States and Communist Party, *Reset, Prevent, Build: A Strategy to Win America's Economic Competition with the Chinese Communist Party*, December 2023, https://selectcommitteeontheccp.house.gov/sites/evo-subsites/selectcommitteeontheccp.house.gov/files/evo-media-document/reset-prevent-build-scc-report.pdf.

see the **Appendix**) might impact the identification of potential vulnerabilities to U.S. research. For example, Congress could direct DOD to revisit its "Section 1286 list"[122] of "foreign talent programs that pose a threat to national security." Congress could revise statutory guidance on what the list should include or direct DOD to update the lists more frequently than annually. For example, congressional testimony and reports have highlighted specific instances where PRC-backed talent recruitment programs have changed names once identified and targeted by U.S. policies (e.g., the PRC's renaming of its Thousand Talents Program).[123] Given the potential fluidity of foreign talent recruitment program naming conventions, Congress might weigh the challenges of maintaining a current definition with the utility of curating such a list altogether.

Congress might consider the potential outcomes from altering the scope of DOD's Section 1286 list or other changes to how malign foreign talent recruitment programs are defined in statute. Though providing additional direction or clarification might prohibit greater numbers of researchers with potentially questionable motives from contributing to federally funded research projects, additional prohibitions could limit foreign research participation in the U.S. STEM talent pool, which is heavily reliant on foreign talent.[124] In a 2024 report called *International Talent Programs in the Changing Global Environment*, the National Academies recommended that "all efforts should be taken to ensure that programs and policies intended to protect critical research from malign foreign influence do not target or inadvertently discriminate against people on the basis of national origin or ethnicity."[125]

Direct Agency Risk Assessment and Mitigation Activities

Agency-level policies seem to be evolving independently—driven primarily by statutory mandates and in response to specific mission needs. Such variations might result in uneven applications of security measures across the federal research enterprise and, as a potential outcome, gaps in the protection of research.

Harmonize Policies Across Agencies

To strengthen the consistency of research protections, Congress could direct federal research agencies to harmonize risk assessment frameworks and mitigation activities. This could involve specifying in statute common criteria and factors for agencies to consider in evaluating risks associated with research funding decisions. The specificity with which Congress addressed potential violations and agency enforcement actions related to disclosure requirements could serve as a relevant model for constructing statutory language directing agency risk assessment.[126] Alternatively, Congress could direct OSTP to develop a uniform policy and ensure consistency in agency implementation. Institutions of higher education have urged federal agencies to harmonize risk assessment and mitigation activities, citing the administrative costs associated with tracking

[122] A reference to Section 1286 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (P.L. 115-232).

[123] House Committee on Homeland Security and Government Affairs, *Threats to the U.S. Research Enterprise: China's Talent Recruitment Plans*, staff report, 2019, https://www.hsgac.senate.gov/wp-content/uploads/imo/media/doc/2019-11-18%20PSI%20Staff%20Report%20-%20China's%20Talent%20Recruitment%20Plans%20Updated2.pdf; and Defense Counterintelligence and Security Agency, *Foreign Intelligence Entities' Recruitment Plans Target Cleared Academia*, April 28, 2021, https://www.dcsa.mil/Portals/91/Documents/CI/DCSA_AD-21-001_FIE_Recruitment_Plans_Target_Cleared_Academia.pdf.

[124] NASEM, *International Talent Programs in the Changing Global Environment*, 2024, https://nap.nationalacademies.org/catalog/27787/international-talent-programs-in-the-changing-global-environment.

[125] NASEM, *International Talent Programs in the Changing Global Environment*, p. 6.

[126] 42 U.S.C. §6605(c).

and enforcing regulations that may vary by agency or specific funding opportunity. For example, in a presentation to NASEM's Strategic Council for Research Excellence, Integrity, and Trust, the president of COGR expressed concern over the degree to which "federal regulations are weighing down U.S. researchers and innovation" and called for a central mechanism to streamline and harmonize research regulations.[127]

If Congress chooses to harmonize agency risk assessment and mitigation activities, it could consider the specificity with which to prescribe evaluation criteria and risk factors. Though uniform policies may lessen administrative burdens for universities, as argued by COGR, establishing agency requirements that are highly specific and inflexible could have drawbacks. The specific mission needs of a particular agency may require tailored risk assessment and mitigation measures. To afford agencies flexibility while increasing harmonization, Congress might establish a minimum requirement for risk assessment and mitigation, which agencies could build on as needed.

Identify Research Fields for Heightened Scrutiny

If Congress chooses to establish a minimum requirement, it could opt to employ a risk criterion based on the substantive focus of research projects as described in funding applications. For example, Congress could designate certain fields of fundamental research (e.g., quantum research) as "riskier"—meaning that foreign affiliations and international collaborations among researchers working in such fields may pose greater degrees of risk to U.S. economic and national security. Congress might direct federal agencies to automatically require specified mitigation measures for all federally funded research projects in any such fields. Mitigation measures might include removing international collaborators and coauthors from federally funded research projects, requiring increased oversight of such projects (either by federal agencies or by the institutions employing the researchers), or instituting potential control mechanisms such as prepublication review.[128]

Whereas certain funding applications might be subject to heightened scrutiny under this approach, funding applications in fields deemed comparatively less risky (e.g., social science research) may be subject to less stringent research security reviews, if any. Directing agency risk assessment and mitigation activities differentially according to field of study may reduce administrative costs for federal agencies by potentially reducing the quantity of proposals needing in-depth security reviews. Other potential benefits of this approach might include streamlining and harmonizing practices across agencies, which could reduce administrative costs for institutions of higher education as well as individual researchers.

Though it could lessen administrative costs for agencies, institutions, or individual researchers, this option may also lead to certain outcomes that could run counter to intended policy objectives, namely strengthening national and economic security. For example, if international research

[127] Matt Owens, "Federal Regulations Are Weighing Down U.S. Researchers and Innovation," COGR, March 5, 2025, https://www.nationalacademies.org/documents/embed/link/LF2255DA3DD1C41C0A42D3BEF0989ACAECE3053A6A9B/file/DB084E8BDA79F03C5169DDEE19D0E37F1F3F07CED204?noSaveAs=1#:~:text=Page%206,Calibrate%20Research%20Regulations%20to%20Risk.

[128] Generally, prepublication review involves a contract clause or related requirement in a funding agreement that allows the funding institution to review research results prior to publication for national security reasons or for the purpose of determining whether proprietary information would be divulged. For additional information regarding prepublication review policies, including how they potentially conflict with the NSDD-189 fundamental research exemption, see CRS Report R42606, *Publishing Scientific Papers with Potential Security Risks: Issues for Congress*, by Frank Gottron and Dana A. Shea.

collaborations in certain fields are prohibited or so heavily scrutinized that U.S. researchers avoid them, the depth of U.S. knowledge and performance in certain S&T fields could decline as a result. Other potential costs might include reduced U.S. participation in the development of international technical standards (which could diminish the ability of U.S.-based firms to compete in global markets for various emerging technology applications).

Concluding Observations

Policymakers faced with assessing research security policies are challenged by the multidisciplinary, complex nature of such activities. Research security issues cut across traditional policy concerns, involving simultaneous consideration of national security, scientific, technological, export, and international policy. Because of the complexity of issues related to research security policies, analysis of a topic according to one set of policy priorities may lead to unforeseen complications because of its intersection with other policy priorities. Accounting for such trade-offs may allow policymakers to establish policy frameworks that more effectively maximize the benefits of international scientific collaboration while mitigating its potential risks.

Appendix. Definition of Malign Foreign Talent Recruitment Program

Following is the full definition of *malign foreign talent recruitment program*, as codified at 42 U.S.C. §19237:

> (A) any program, position, or activity that includes compensation in the form of cash, in-kind compensation, including research funding, promised future compensation, complimentary foreign travel, things of non de minimis value, honorific titles, career advancement opportunities, or other types of remuneration or consideration directly provided by a foreign country at any level (national, provincial, or local) or their designee, or an entity based in, funded by, or affiliated with a foreign country, whether or not directly sponsored by the foreign country, to the targeted individual, whether directly or indirectly stated in the arrangement, contract, or other documentation at issue, in exchange for the individual—
>
> (i) engaging in the unauthorized transfer of intellectual property, materials, data products, or other nonpublic information owned by a United States entity or developed with a Federal research and development award to the government of a foreign country or an entity based in, funded by, or affiliated with a foreign country regardless of whether that government or entity provided support for the development of the intellectual property, materials, or data products;
>
> (ii) being required to recruit trainees or researchers to enroll in such program, position, or activity;
>
> (iii) establishing a laboratory or company, accepting a faculty position, or undertaking any other employment or appointment in a foreign country or with an entity based in, funded by, or affiliated with a foreign country if such activities are in violation of the standard terms and conditions of a Federal research and development award;
>
> (iv) being unable to terminate the foreign talent recruitment program contract or agreement except in extraordinary circumstances;
>
> (v) through funding or effort related to the foreign talent recruitment program, being limited in the capacity to carry out a research and development award or required to engage in work that would result in substantial overlap or duplication with a Federal research and development award;
>
> (vi) being required to apply for and successfully receive funding from the sponsoring foreign government's funding agencies with the sponsoring foreign organization as the recipient;
>
> (vii) being required to omit acknowledgment of the recipient institution with which the individual is affiliated, or the Federal research agency sponsoring the research and development award, contrary to the institutional policies or standard terms and conditions of the Federal research and development award;
>
> (viii) being required to not disclose to the Federal research agency or employing institution the participation of such individual in such program, position, or activity; or
>
> (ix) having a conflict of interest or conflict of commitment contrary to the standard terms and conditions of the Federal research and development award; and
>
> (B) a program that is sponsored by—
>
> (i) a foreign country of concern or an entity based in a foreign country of concern, whether or not directly sponsored by the foreign country of concern;

(ii) an academic institution on the list developed under section 1286(c)(8) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (10 U.S.C. 2358 note; Public Law 115–232); or

(iii) a foreign talent recruitment program on the list developed under section 1286(c)(9) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (10 U.S.C. 2358 note; Public Law 115–232).

Author Information

Emily G. Blevins
Analyst in Science and Technology Policy

Disclaimer