RECOMMENDED PRACTICES FOR STRENGTHENING THE SECURITY AND INTEGRITY OF AMERICA'S SCIENCE AND TECHNOLOGY RESEARCH ENTERPRISE

Product of the

SUBCOMMITTEE ON RESEARCH SECURITY

JOINT COMMITTEE ON THE RESEARCH ENVIRONMENT

of the

NATIONAL SCIENCE & TECHNOLOGY COUNCIL

January 2021

About the National Science and Technology Council

The National Science and Technology Council (NSTC) is the principal means by which the Executive Branch coordinates science and technology policy across the diverse entities that make up the Federal research and development enterprise. A primary objective of the NSTC is to ensure science and technology policy decisions and programs are consistent with the President's stated goals. The NSTC prepares research and development strategies that are coordinated across Federal agencies aimed at accomplishing multiple national goals. The work of the NSTC is organized under committees that oversee subcommittees and working groups focused on different aspects of science and technology. More information is available at http://www.whitehouse.gov/ostp/nstc.

About the Office of Science and Technology Policy

The Office of Science and Technology Policy (OSTP) was established by the National Science and Technology Policy, Organization, and Priorities Act of 1976 to provide the President and others within the Executive Office of the President with advice on the scientific, engineering, and technological aspects of the economy, national security, homeland security, health, foreign relations, the environment, and the technological recovery and use of resources, among other topics. OSTP leads interagency science and technology policy coordination efforts, assists the Office of Management and Budget with an annual review and analysis of Federal research and development in budgets, and serves as a source of scientific and technological analysis and judgment for the President with respect to major policies, plans, and programs of the Federal Government. More information is available at http://www.whitehouse.gov/ostp.

About the Subcommittee on Research Security

The Subcommittee on Research Security is an interagency group organized under the NSTC Joint Committee on the Research Environment (JCORE). The purpose of the Subcommittee on Research Security is to coordinate Federal Government efforts to enhance the security and integrity of America's science and technology research enterprise without compromising American values or the openness of the innovation ecosystem. The Subcommittee is focused on coordinating appropriate and effective risk management, coordinating Federal efforts to effectively communicate and provide outreach to academic and research organizations, developing guidance for agencies on security and integrity of the Federally-funded research enterprise, and developing recommended practices for academic and research organizations.

About this Document

This document was developed by the Subcommittee on Research Security, in coordination with the National Security Council staff, and was reviewed by JCORE. The document outlines recommended guidelines for organizations that conduct research.

Copyright Information

NATIONAL SCIENCE AND TECHNOLOGY COUNCIL

Kelvin K. Droegemeier, Chair

Tracie Lattimore, Executive Director
Grace Diana, Deputy Executive Director

JOINT COMMITTEE ON THE RESEARCH ENVIRONENT

Co-Chairs
Paul Dabbar, Under Secretary for Science, Department of Energy
Kelvin K. Droegemeier, Director, Office of Science and Technology Policy
Francis Collins, Director, National Institutes of Health
Walter Copan, Under Secretary of Commerce for Standards and Technology and Director, National Institute of Standards and Technology
Sethuraman Panchanathan, Director, National Science Foundation

SUBCOMMITTEE ON RESEARCH SECURITY

Co-Chairs
Steve Binkley, Department of Energy
Helena Fu, Office of Science and Technology Policy
Rebecca Keiser, National Science Foundation
Mike Lauer, National Institutes of Health
Aaron Miles, Office of Science and Technology Policy

Members

Departments
Department of Agriculture
Department of Defense
Department of Education
Department of Energy
Department of Homeland Security
Department of Justice
Department of State
Department of Transportation

Agencies
Federal Bureau of Investigation
Food and Drug Administration
National Aeronautics and Space Administration
National Institute of Standards and Technology
National Institutes of Health
National Oceanic and Atmospheric Administration
National Science Foundation
National Security Agency
Office of the Director of National Intelligence
United States Geological Survey
United States Patent and Trademark Office

Executive Office of The President
National Security Council
Office of Management and Budget
Office of Science and Technology Policy

Abbreviations and Acronyms

DHS	Department of Homeland Security
DOJ	Department of Justice
DOS	Department of State
ED	Department of Education
FBI	Federal Bureau of Investigation
HSI	Homeland Security Investigations
ICE	Immigration and Customs Enforcement
ODNI	Office of the Director of National Intelligence
NSF	National Science Foundation
NSTC	National Science and Technology Council

Table of Contents

Use of this Document

The purpose of this document is to offer recommendations research organizations (e.g., universities, private companies, independent research institutes) can take to better protect the security and integrity of America's research enterprise. It serves as a complementary document to National Security Presidential Memorandum 33 (NSPM-33), titled, "U.S. Government Supported Research and Development National Security Policy." NSPM-33 directs Federal departments and agencies to act to protect federally-funded research, including from foreign interference, and incorporates recommendations that the JCORE Subcommittee on Research Security developed in partnership with the National Security Council staff, working across Federal agencies and informed by inputs from across America's research enterprise, including universities, companies, associations, and scientific societies. The recommendations for research organizations contained in this report were likewise informed by extensive engagement across the U.S. research enterprise and with international partners. These recommendations constitute recommended practices that will strengthen and protect the security and integrity of America's research enterprise. Users of this document are strongly encouraged to read NSPM-33 to ensure an appropriate breadth and depth of understanding of the complex issues associated with research security and integrity.

Background and Motivation

The open and collaborative nature of the U.S. science and technology (S&T) research enterprise, along with the integrity and public trust with which it operates, underpin America's innovation, S&T leadership, economic vitality, and national security. Maintaining an open research environment is critical to fostering research discoveries and innovations that benefit our Nation and the world. Principled international collaboration and foreign contributions are critical to the success of the U.S. research enterprise. In particular, they enable cutting-edge research that cannot otherwise be achieved, strengthen scientific and diplomatic ties, leverage resources, and support training of a robust S&T workforce capable of solving global problems. At the same time, this open environment must be balanced by mechanisms that protect intellectual capital; discourage misappropriation of research plans, pre-publication data, and outcomes; and ensure responsible management of U.S. taxpayer dollars.

The integrity of the research enterprise rests on foundational principles and values, which are also consistent with American values:

- **Openness and transparency** enable productive collaboration and help ensure appropriate disclosure of potential conflicts of interest[1] and conflicts of commitment.[2]
- **Accountability and honesty** help acknowledge errors and correct behaviors that can hamper progress.
- **Impartiality and objectivity** protect against improper influence and distortion of scientific knowledge.
- **Respect** helps create an environment where all can be heard and contribute.
- **Freedom of inquiry** allows individual curiosity to guide scientific discovery.
- **Reciprocity** ensures that scientists and institutions exchange materials, knowledge, data, access to facilities and natural sites, and training in a way that benefits all collaborating partners.
- **Merit-based competition** helps ensure a level playing field where the best ideas and innovations can advance.

---

[1] Definitions for conflict of interest vary across Federal agencies and research organizations. In the context of research security and integrity, and for the purposes of this document, the National Science and Technology Council (NSTC) Subcommittee on Research Security considers a conflict of interest to be a situation in which an individual, or the individual's spouse or dependent children, has a financial interest or relationship that could directly and significantly affect the design, conduct, reporting, or funding of research. United States government officers and employees engaged in the Federally funded research enterprise are subject to restrictions in law (18 U.S.C. §201-209) and U.S. Office of Government Ethics regulations related to their personal and imputed financial interests (where imputed financial interests include those of spouse, minor child, general partner, organization in which the individual is serving as officer, director, trustee, general partner or employee, or any person or organization with whom the individual is negotiating or has any arrangement concerning prospective employment).

[2] Definitions for conflict of commitment vary across Federal agencies and research organizations. In the context of research security and integrity, and for the purposes of this document, the NSTC Subcommittee on Research Security considers a conflict of commitment to be a situation in which an individual accepts or incurs conflicting obligations between or among multiple employers or other entities. Many organizational policies define conflicts of commitment as conflicting commitments of time, including obligations to dedicate time in excess of institutional or funding agency policies or commitments. Other types of conflicting obligations, including obligations to share information improperly 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.

Some of these foundational principles—like openness, transparency, and accountability—are relevant to all, from individual researchers, to research organizations, to governments. Others—including impartiality, objectivity, honesty, and respect—are at the core of how individuals and organizations should conduct research to ensure rigor and reproducibility. Others—including freedom of inquiry, reciprocity, and merit-based competition—are the responsibility of all, but especially governments, to protect and foster.

Behaviors that violate these foundational principles and values jeopardize the *integrity* of the research enterprise. Behaviors that threaten the integrity of the research enterprise often also pose risks to the *security* of the research enterprise, which we term research security. For example, surreptitious diversion of confidential grant applications to foreign government entities can threaten research security while also compromising the fairness of processes intended to provide merit-based allocation of research and development (R&D) funding. Therefore, research security and the integrity of the research enterprise are inexorably linked.

Unfortunately, the governments of some countries do not demonstrate a reciprocal dedication to these same principles and values. Instead, they seek to exploit the global research enterprises to circumvent the costs and risks of conducting their own research, thereby increasing their economic and military competitiveness at the expense of the United States and its allies and partners.

Over the past several years, some individuals and foreign governments have exhibited increasingly sophisticated efforts to exploit, influence, and undermine U.S. research activities and environments. Recent breaches of research integrity within America's research enterprise include failures to disclose the following: funding (in some individual cases totaling hundreds of thousands of dollars in research subsidies, salaries, and personal payments); parallel laboratories; employment, affiliations, and appointments (including leadership positions in foreign research organizations); and conflicting financial interests (including investment in and even ownership of private companies specializing in the same work performed at individuals' U.S. research organizations). Often it is foreign funding sources and appointments that are not disclosed.

Beyond these disclosure failures, other inappropriate or exploitive behaviors have included conducting undisclosed research for foreign governments or companies while being funded for that same research effort or time by U.S. agencies; diversion of intellectual property (IP) or other legal rights; and breaches of contract and confidentiality in or surreptitious gaming of the peer-review process (including surreptitious provision of grant applications to foreign scientists). In addition to violating ethical norms and Federal agency policies, some recent incidents involve illegal activities, including theft of research data enabled by hacking thousands of computer accounts at hundreds of research organizations across the globe and grant fraud associated with applying for Federal grants to conduct research already completed at a parallel foreign laboratory.

Such behaviors can and have resulted in very real and negative impacts on individuals and research organizations, and threaten to weaken the whole of the research enterprise. These behaviors can distort decisions about appropriate use of public and private funds. They can also result in hidden transfers of information, know-how, data, and time; diversion of confidential or proprietary information and pre-publication data to foreign entities; loss of Federal research funding; reputational, career, and financial damage; and loss of public trust in the research enterprise. In individual cases, some researchers have resigned, research organizations have returned millions of dollars in public funding, and some individuals have faced criminal indictments and convictions.

Many of these behaviors have been associated with undisclosed participation in certain foreign government-sponsored talent recruitment programs.[3] Many countries sponsor talent recruitment programs to attract researchers in targeted fields. Many programs utilize legitimate, transparent mechanisms of talent recruitment, including use of research fellowships, student and scholar exchanges, and grants. However, some programs provide direction or levy requirements, including through language in binding contracts, that create conflicts of interest and/or conflicts of commitment for researchers; some have been shown to encourage or direct unethical and even criminal behaviors. Such programs amount to foreign interference in American R&D.

Data regarding the prevalence of behaviors that threaten research security and integrity are still incomplete, but suggest widespread and systemic activity across geographic locations, sizes of organizations, and research disciplines. For example, as of September 2020, the National Institutes of Health identified research security and integrity concerns with more than 200 scientists and sent associated notices to more than 90 research organizations. Incidents of concern are not limited to any one background, ethnicity, or nationality. Nor are they unique to the United States; other countries have identified similar behaviors in their research enterprises.

In order to address effectively the challenges to research security and integrity, Federal agencies and research organizations must work together to protect America's research enterprise without compromising our values or our ability to maintain the innovation ecosystem that has helped underpin our global leadership in S&T. This must include ensuring an approach that is balanced as well as risk- and evidence-based.

A balanced, risk-based approach must recognize the benefits of open, international collaboration as well as the risks. This approach must seek to apply protective measures commensurate with identified risks, accounting for both likelihood of occurrence and impact, weighed against tangible benefits and any accompanying cost or administrative burden resulting from mitigation measures. Mitigation measures should be considered as part of an integrated approach to research enterprise integrity management that avoids undue administrative burden for researchers, research organizations, and funding organizations. Finally, there should be measures that target specific behaviors and seek to uphold the same foundational principles and values across the research enterprise, independent of the nature of a collaboration and the makeup of its participants, including their country of origin, nationality, and ethnicity.

[3] A foreign government-sponsored talent recruitment program is an effort directly or indirectly organized, managed, or funded by a foreign government, including state-owned enterprises, or a foreign institution to recruit science and technology professionals or students (regardless of citizenship or national origin, and whether having a full-time or part-time position). Some foreign government-sponsored talent recruitment programs operate with the intent to import or otherwise acquire from abroad, through illicit as well as licit means, proprietary technology or software, unpublished data and methods, and intellectual property to further the military modernization goals and/or economic goals of a foreign government. Many, but not all, programs aim to incentivize the targeted individual to relocate physically to the foreign state for the above purpose. Some programs allow for or encourage continued employment at U.S. research facilities or receipt of Federal research funds while concurrently working at and/or receiving compensation from a foreign institution. Compensation could take many forms including cash, research funding, complimentary foreign travel, honorific titles, career advancement opportunities, promised future compensation, or other types of remuneration or consideration, including in-kind compensation.

This document recommends practices for research organizations to help enhance the security and integrity of America's research enterprise. These recommended practices outline a balanced, behavior- and risk-based approach that supports five high-level objectives:

- Demonstrate organizational leadership and oversight;
- Establish an expectation of openness and transparency;
- Provide and share training, support, and information;
- Ensure effective mechanisms for compliance with organizational policies; and
- Manage potential risks associated with collaborations and data.

By working to implement these recommendations, research organizations can make significant contributions to enhancing the security and integrity of America's research enterprise.

Recommended Practices for Research Organizations Regarding Research Security and Integrity

Research organizations play a critical role in the security and integrity of America's research enterprise, complementing the role of the Federal Government. Many of the practices that research organizations implement are focused more on protecting the overall integrity of research than specifically addressing national security risks; however, research organization policies designed to protect research integrity also help guard against behaviors that pose significant national security risk.

In fulfilling their role as stewards of research, including training the next generation of researchers, organizations should demonstrate robust leadership and oversight; establish and administer policies to promote transparency and guard against conflicts of interest and commitment; provide training, support, and information on research security; ensure effective mechanisms for compliance with organizational policies; and implement processes to assess and manage potential risks associated with collaborations and data.

The National Science and Technology Council (NSTC) Joint Committee on the Research Environment (JCORE) Subcommittee on Research Security recommends that research organizations consider taking the following actions to help protect the security and integrity of America's research enterprise. The Subcommittee recognizes that the need and ability for research organizations to implement some of the suggested actions depends upon a number of factors, including but not limited to the nature, structure, and mission of the organization, the level and types of research activity it conducts, and available resources. Consequently, the implementation of policies and practices should evolve thoughtfully and appropriately to meet current and future challenges, including foreign government efforts to exploit, interfere with, or undermine our research activities and environment.

Demonstrate Organizational Leadership and Oversight

1. ***Convey the importance of research security and integrity at the leadership level.*** Leaders of organizations shape organizational cultural and are uniquely positioned to communicate information, especially values and priorities. In the context of research security and integrity, this capability is critically important and should be leveraged to the maximum extent possible.

   Leaders of research organizations (e.g., governing boards, chancellors, presidents, executive directors) should consistently and regularly message the importance of research security and integrity in their written and oral communications to their organizations, and to external stakeholders and partners, along with actions their organizations are taking to ensure that security is balanced with openness. Those charged with leading or managing their organizations' research enterprises, such as vice presidents/vice chancellors of research and their subordinate organizations, should actively engage in matters related to research security and integrity and ensure that the heads of their organizations remain fully informed regarding the latest developments and policies.

2. ***Ensure an organizational approach to research security.*** Because research security and integrity are the shared responsibility of individuals, formal and informal research groups, organizational centers or other components, and organizations more broadly, the most appropriate approach for ensuring security and integrity is one that spans entire organizations. Consequently, organizations should develop written research security implementation plans, and should designate a chief research security officer or equivalent to oversee research security management. For the latter, it should be made clear that research security is everyone's responsibility, and that the role of the

research security officer is principally to maintain up-to-date knowledge, and to coordinate, facilitate, communicate, and educate.

3. ***Establish research security and integrity working groups and task forces.*** In order to most effectively develop and implement policies and practices, organizations should include in the process employees at all levels. Such inclusion helps employees understand the issues, see them from multiple points of view, feel valued, and actively participate in work that impacts their careers. This is particularly true for researchers and their employing organizations, where policies regarding research security and integrity are foundational to both individual and organizational success.

   Research organizations therefore should establish and make visible cross-organization working groups and task forces consisting of senior leaders, researchers , other relevant staff, and students where appropriate, to discuss, develop, implement, and evaluate strategies to better coordinate and address concerns regarding strengthening the security and integrity of the research enterprise. Importantly, this work should emphasize the value of understanding and adhering to those principles and values that are foundational to both research security and integrity (see Background and Motivation section above).

4. ***Establish and operate a comprehensive research security program.*** A comprehensive program that considers multiple vectors of potential interference and works with researchers, security officers, and administrators across the organization is one of the most effective mechanisms to coordinate activities internally toward the goal of ensuring research security. Organizations should develop a "risk profile" that assesses the potential risks (e.g., legal, reputational, economic) associated with the loss of research data and IP and the potential for significant commercial or national security impacts.

   Research security programs should include, at a minimum, elements of cyber security, foreign travel security, insider threat awareness and education, and export control training. Depending on the organization's individual risk profile and resources, cyber security elements can include robust access and device registration protocols, hardware encryption, and incorporating use of commercial threat management and commercial compliance solutions into internal due diligence programs. Economies of scale often can be realized by coordinating with other organizations (e.g., within a university system or regionally) to leverage physical and intellectual assets and avoid unnecessary duplication.

Establish an Expectation of Openness and Transparency

5. ***Establish and administer organizational policies regarding conflicts of interest, conflicts of commitment, and disclosure.*** Transparency and accountability are cornerstones of the research enterprise. Disclosing information related to potential conflicts is paramount to maintaining the security and integrity of that enterprise.

   Research organizations should require disclosure of information that will enable reliable determinations of whether and where conflicts of interest and commitment exist, and should develop and implement appropriate risk management plans. Although this document recommends practices for organizations that conduct research, NSPM-33 standardizes requirements for disclosure of information related to potential conflicts of interest and commitment from individuals with significant influence on America's R&D enterprise, including those leading federally funded research projects and those involved in the allocation and awarding

of Federal R&D[4] funding. When appropriate, research organizations should report conflicts of interest or commitment to funding agencies, especially in instances where a research organization is unable to mitigate or manage the conflict. In instances where nondisclosure suggests illegal activity, organizations should also notify law enforcement agencies as appropriate.

As a practical matter, it should be made clear to all researchers, including any students involved in research, that when in doubt about any matter regarding research security or integrity, the appropriate action is to consult the relevant organizational official, who should be clearly designated by the organization. This is particularly true in the context of prospective participation in foreign government-sponsored talent recruitment programs, which often provide contracts directly to researchers with the expectation of signature by the individual alone. Any such contract should be disclosed to the researcher's employer organization for review to protect both the organization and researcher.

6. ***Require disclosure to the organization of all information necessary to identify and assess potential conflicts of interest and commitment.*** Research organizations should require the filing of relevant disclosures to the organization, and maintain a repository of such filings, from organizational employees and affiliates engaged in the research enterprise, regardless of whether those individuals are supported by Federal funding or involved in projects supported by Federal funding.

   A. Research organizations should require disclosure from key segments of the R&D enterprise, including:
      1. Researchers (including postdoctoral researchers and other staff);
      2. Graduate students engaged in research activities; and
      3. Visiting scholars performing research over an extended period of time.

   B. Research organizations should require that disclosures from research enterprise employees and contractors include the following information:
      1. Organizational affiliations and employment.
      2. Other support, contractual or otherwise, direct and indirect, including current and pending private and public sources of funding or income, both foreign and domestic. For researchers, other support should include all resources made available to a researcher in support of and/or related to all of their professional R&D efforts, including resources provided directly to the individual rather than through the research organization, and regardless of whether or not they have monetary value (e.g., even if the support received is only in-kind, such as office/laboratory space, equipment, supplies, or employees). This should include resource and/or financial support from all foreign and domestic entities, including but not limited to, gifts provided with terms or conditions, financial support for laboratory personnel, and participation of student and visiting researchers supported by other sources of funding.
      3. Current or pending participation in, or applications to, programs sponsored by foreign governments, instrumentalities, or entities, including foreign government-sponsored talent recruitment programs. While many countries sponsor talent recruitment programs for legitimate purposes of attracting talent in targeted fields, some programs encourage or direct

[4] Federal Research & Development (R&D) funding constitutes all funding for scientific research and development provided by the Federal Government. Research means a systematic investigation—including research, development, testing, and evaluation—designed to develop or contribute to generalizable knowledge. Activities that meet this definition constitute research for purposes of this policy, whether or not they are conducted or supported under a program that is considered research for other purposes. For example, some demonstration and service programs may include research activities.

unethical and criminal behaviors. In order to fully assess risk, organizations should require that individuals disclose associated contract(s) upon request, in addition to the fact of participation.

4. All positions and professional appointments both domestic and foreign that are relevant to the individual's relationship to the research organization, including affiliations with foreign entities or governments. This includes titled academic, professional, or organizational appointments, whether or not remuneration is received, and whether full-time, part-time, or voluntary (including adjunct, visiting, or honorary).

C. Research organizations should require initial disclosures upon hiring or assignment of relevant duties, and annual updates to disclosure reporting. Annual updates are important to account for individuals' changing situations. Additionally, organizations should consider whether some types of changes might require prompt disclosure in addition to the initial and annual updates.

D. Research organizations should assist their employees, affiliates, and students with disclosures that are required for the organization to comply with Federal funding agency disclosure requirements. The administrative burden may be minimized by using online forms that allow updates while maintaining a record of prior disclosures.

7. ***Ensure compliance with Department of Homeland Security requirements for reporting foreign students and foreign researcher information.*** Research organizations should ensure that foreign students and foreign researcher information included in the Student and Exchange Visitor Information System (SEVIS) is updated regularly by Designated School Officials (DSOs) and consistent with U.S. Department of Homeland Security (DHS), Immigration and Customs Enforcement, Homeland Security Investigations (DHS/ICE/HSI) requirements[5] and by Exchange Visitor Program Responsible Offices (ROs) consistent with U.S. Department of State (DOS) requirements. SEVIS is the web-based system that DHS uses to maintain information on Student and Exchange Visitor Program (SEVP)-certified schools and nonimmigrant students who come to attend those schools, and that DOS uses to maintain information on DOS-designated schools and exchange visitors who come to attend those schools. It is a critical tool that DHS uses to protect national security while supporting legal entry of nonimmigrants to the United States for education and cultural exchange. Research organizations should ensure that foreign students and foreign researchers fully understand the disclosure requirements associated with SEVIS and that they adhere to relevant deadlines and procedures. Students and research organizations that fail to report any required information to DHS in a timely manner may face adverse consequences including but not limited to decertification, revocation of funding, or loss of immigration status.

8. ***Establish policies regarding digital persistent identifiers.*** Research organizations should establish policies regarding requirements for research enterprise employees, contractors, and affiliates to be registered with a service that provides a digital persistent identifier (DPI) for that individual and provide organizations access to relevant information disclosed through the DPI in a manner consistent with applicable laws, which may include employment, research funding, professional R&D affiliations, and published research. DPIs represent a valuable mechanism for accurately linking researchers with their awards, publications, and research outputs. DPIs offer many benefits, including enhancing research rigor by ensuring that researchers receive credit for publications, data sets, and other scholarly works; simplifying the tracking of funding received and notification about future funding opportunities; and searching for scholarly works and collaborators. They also

[5] DHS/ICE/HSI, Student and Exchange Visitor Program. https://www.ice.gov/sevis

represent a potential means for streamlining grant application processes via pre-population of digital forms.

9. ***Ensure compliance with requirements for reporting foreign gifts and contracts.*** Research organizations should ensure compliance with requirements under Section 117 of the Higher Education Act[6] for reporting of gifts or contracts received from or entered into with foreign sources. This law requires nearly all colleges and universities to report biannually to the Secretary of Education foreign gifts and contracts valued at $250,000 or more and to disclose any foreign ownership or control. Such reporting is important for transparency, accountability, and organizational integrity, and also aids senior leaders in appropriately identifying and managing organizational conflicts of interest. Failure to comply with these statutory requirements may result in audits and other various legal consequences.

Provide and Share Training, Support, and Information

10. ***Provide training to participants in the research enterprise on the responsible conduct of research.*** The 2007 America COMPETES Act mandated training in the responsible and ethical conduct of research (RECR) for undergraduate students, graduate students, and postdoctoral researchers funded by NSF.[7] This requirement was formally implemented in January 2010, and the training is required to occur during the period of the award. Since then, other agencies (e.g., National Institutes of Health, U.S. Department of Agriculture) have required RECR training under some circumstances, or otherwise made training available to research personnel even in circumstances where Federal requirements do not apply.

    RECR training is foundational to educating current and future researchers about the importance of integrity in research and the role of researchers in upholding it. All organizations performing organized research, irrespective of funding source, should offer RECR training to all researchers including new students, visiting scholars, employees, and affiliates and include annual refresher training, where applicable. The training content should include requirements and processes for disclosure of conflicts of interest and commitment, as well as training on upholding core organizational values, protection of IP, and the responsible and ethical conduct of research.

    Since all organizations receiving NSF funding already have RECR programs in place, numerous examples exist of content from which to draw. In addition to those collected by NSF,[8] the U.S. Department of Health and Human Services Office of Research Integrity also provides numerous resources on RECR.[9]

11. ***Provide guidance for those considering participation in foreign government-sponsored talent recruitment programs.*** Some foreign government-sponsored talent programs encourage or direct unethical and criminal behaviors, including some listed in Recommendation 13(a). Transparency and full disclosure are essential to properly assess risks that participation in these programs may pose to the integrity and security of the research enterprise. Therefore, to the extent feasible, research organizations should assist their researchers in reviewing contracts and understanding the implications of commitments individuals might be assuming, and any potential for exploitation.

---

[6] Section 117 of the Higher Education Act of 1965. https://www2.ed.gov/policy/highered/leg/foreign-gifts.html

[7] America Competes Act. https://www.congress.gov/110/plaws/publ69/PLAW-110publ69.pdf

[8] National Science Foundation, America COMPETES Act RECR Training Requirements. https://www.nsf.gov/bfa/dias/policy/rcr.jsp

[9] Health and Human Services Office of Research Integrity. https://ori.hhs.gov/

12. ***Partner with local FBI field offices to strengthen research security.*** Research organizations should partner with their local FBI field offices to help inform and strengthen research security efforts such as insider threat and cybersecurity programs, policies, and awareness training to help recognize suspicious behavior and better protect personnel, facilities, and information. The FBI has engaged, and continues to engage, the research community on the topic of research security, through a range of initiatives and activities. Research organizations that have worked with the FBI to build strong partner relationships have benefited from expertise and resources resident in the Federal law enforcement and security communities. Such trusted relationships are critical for securing America's research enterprise while also maintaining the degree of openness needed for it to thrive.

    The 56 FBI field offices across the United States serve as local points of contact for research organizations and represent an extraordinarily valuable resource for addressing research security.[10] The FBI also has designated a national program office focused on forging and strengthening relationships with research organizations, and can provide briefings upon request. Contact information can be found at the end of this document under Federal Government and Agency Contacts.

13. ***Increase awareness of and protections against circumstances and behaviors that may indicate risk to research security and integrity.*** Over the past several years, the U.S. Government and research organizations have become increasingly aware of concerning behaviors that indicate inappropriate foreign government interference in the U.S. research enterprise. These concerning behaviors are not limited to any one background, ethnicity, nationality, or research field. In many cases, researchers engaged in contractual relationships with terms that directed unethical and in some cases criminal behavior, often without disclosing to their U.S. employer or funder. Greater awareness protects organizations and researchers by helping them recognize potentially problematic circumstances and behaviors. The FBI can provide briefings on these matters upon request, and contact information can be found at the end of this document under Federal Government and Agency Contacts. Research organizations should ensure that all members of the research enterprise share awareness of circumstances and behaviors that may pose a risk to research security and integrity, including the following:

    A. Certain conditions, contract terms, or other obligations associated with participation in foreign government-sponsored programs or entities, including talent recruitment programs, to include:
        1. Contracts withheld or provided without a third-party certified English translation;
        2. Contracts that allow for or encourage continued employment at U.S. research facilities or receipt of Federal research funds while concurrently working at and/or receiving compensation from a foreign organization;
        3. Setting up or relocating a laboratory in a foreign country;
        4. Obligation to file international patents;
        5. Obligation to publish in particular journals, and/or list a foreign organization affiliation in any published paper;
        6. Obligation to share information that is or may be confidential (e.g., grant applications, peer-review information) with unapproved entities;
        7. Obligation to withhold information from the U.S. home organization or funding agency;
        8. Conflicts of time commitment (e.g., sum of all appointments totals more than 100%);

[10] FBI Field Offices. https://www.fbi.gov/contact-us/field-offices

9. Purpose or stated goals of the program that conflict with goals of the U.S. home organization;
10. Obligation to participate in talent-recruitment activities;
11. Obligation to hire or provide career advancement opportunities to other participants in such programs;
12. Obligation to provide pre-publication data or other pre-publication information to the foreign entity; and
13. Obligation to prove loyalty or political fealty to a foreign government.

B. Participation by researchers in any government-sponsored talent recruitment program that has encouraged or directed participants to engage in behaviors that conflict with principles of research security and integrity;
C. Any obligation for researchers to conduct R&D activities on behalf of another research organization or entity without the knowledge and approval of the employing organization;
D. Foreign travel by researchers related to professional R&D activities, particularly when funded by a foreign entity, without justification regarding the benefits;
E. Extended travel by researchers that is inconsistent with funding received and/or the researcher's organizational obligations;
F. Association, affiliation, or collaboration by researchers with foreign entities identified on the U.S. government's Consolidated Screening List;[11] and
G. Gifts that are provided to research enterprise participants with terms and conditions associated with research activities.

14. ***Share information regarding potential violations of disclosure policies.*** Research organizations should share information regarding potential violations of disclosure policies with relevant Federal funding agencies and ensure compliance with any funding agency requirements regarding provision of such information. Sharing information about potential violations of disclosure policies, while appropriately protecting privacy and due process, is important for enabling accurate risk assessments and effective response measures. Research organizations should work with funding and law enforcement agencies to determine appropriate conditions and mechanisms for the provision of such information. Appendix A includes contact information for Federal funding agencies.

Ensure Effective Mechanisms for Compliance with Organizational Policies

15. ***Establish and exercise effective means of discovering violations of disclosure policies and other activities that threaten research security and integrity.*** As discussed in Recommendation 5, disclosure of required information is critical to maintaining the security and integrity of the research enterprise. However, research organizations also need to develop the means to identify instances where disclosures are incomplete or inaccurate, or when disclosure policies are otherwise violated. Documenting and reporting violations to relevant authorities leverages their ability to discover and investigate violations.

    Research organizations should establish and administer clear processes for identifying, documenting, and reporting to relevant authorities applicable instances in which individuals fail to comply with organizational policies regarding conflict of interest and commitment. Research organizations should work together and with law enforcement, Federal funding agencies, and the private sector to develop more effective tools to identify potentially problematic foreign relationships. Where appropriate, research organizations should cooperate and assist with law

[11] Consolidated Screening List. https://legacy.export.gov/csl-search

enforcement investigations and analysis aimed at discovering violations, including sharing disclosure statements to the extent that such sharing is consistent with privacy laws and other legal restrictions, and does not interfere with law enforcement activities.

16. ***Ensure appropriate and effective consequences for violation of disclosure requirements and engagement in other activities that threaten research security and integrity.*** Ensuring appropriate penalties for violating ethical standards, agency and organizational policies, and applicable laws is a vital dimension of ensuring research security and integrity. Such consequences help communicate the importance of research security and integrity and deter behaviors that would harm the research enterprise. In some cases, penalties are appropriately applied by funders or the courts, while in other cases, the most appropriate penalties may be within the purview of the research organization.

    A. Depending on the nature of the violation, research organizations may consider a range of consequences, consistent with law and their governing documents, including but not limited to the following:
        1. Preserving the grant, contract, or agreement, but requiring replacement, with prior Federal agency approval where required, of the individual(s);
        2. Termination of grant funding to individual researcher(s);
        3. Probation;
        4. Revocation of tenure;
        5. Termination of employment or contract; and/or
        6. Expulsion.
    B. In addition to these measures, civil and criminal penalties under U.S. Federal and state laws may apply in some cases, such as when individuals intentionally provide incomplete or incorrect information during the grant funding process, or misappropriate trade secrets.
    C. In order to strengthen the effectiveness of response measures, research organizations should share information about violators with the relevant Federal funding agency to the extent allowed by law. Organizations should be aware of and comply with any legal obligations they may have to share such information with funding agencies or other authorities.

17. ***Include in employment agreements provisions that support research security and integrity.*** Research organizations should include in employment agreements deliberate provisions tailored to research security and integrity. Such agreements also have the benefit of being legally binding and thus provide protection for both the research organization and the employees within it.

    In developing employment agreements, research organizations should consider provisions that:

    A. To the extent permissible by law, establish clear expectations regarding conducting and reporting activities outside the period covered by the employment agreement (e.g., during summer months for academic year appointments).
    B. Establish clear expectations regarding research security training and adherence to codes of conduct regarding responsible and ethical conduct of research.
    C. Allow organizations to take effective actions against individuals who violate research security and integrity principles and policies, including in cases of inappropriate behaviors on the part of individuals serving in Federal merit review processes.

Manage Potential Risks Associated with Collaborations and Data

18. ***Establish a centralized review and approval process for evaluating formal research partnerships.*** Research organizations should establish a centralized review and approval process for evaluating formal research partnerships or contracts with outside entities to assess potential risk to the security or integrity of the research enterprise. Many research organizations have offices of sponsored programs or similar offices, with access to legal counsel, that evaluate terms and conditions of research assistance awards, contracts, and other funding and partnership instruments. Fundamentally, research partnerships involve ceding work of value to another individual, set of individuals, or organization(s); therefore, responsible engagement in research partnerships requires knowing and trusting all parties involved, along with elements of risk assessment and management. A careful assessment of risk, together with the potential for project success and benefit, is critical to protecting individual and organizational interests.

    The following factors should be considered in such a benefit and risk evaluation:

    A. Affiliations and comprehensive ownership (i.e., direct and indirect) of the outside entity or entities;
    B. Potential value of IP resulting from the research;
    C. Planned research activities, including subject areas(s), type of activities, research location(s), publication rights or intents, and information sharing;
    D. Personnel exchanges with the outside entity or entities;
    E. Export control considerations;
    F. Funding sources and how they may affect partners' rights, obligations, and responsibilities;
    G. Regulatory requirements and standards for data sharing and governance; and
    H. Contract terms, including mechanisms for dispute resolution, governing language, and choice of law.

19. ***Establish and operate a risk-based security process for foreign travel review and guidance.*** Travel by researchers is often essential to successful collaboration, but can also provide opportunities for ill-intentioned actors to improperly acquire research information. Consequently, research organizations should implement programs and processes to manage foreign travel while not unduly impeding the conduct of research. This could include programs, created through organizational export control or research compliance offices, for reviewing travel by researchers and administrators for export compliance, software use restrictions, and other safety and security concerns. Program elements could include:

    A. Requiring that individuals notify the organization of foreign travel;
    B. Providing secure, blank, loaner laptops and phones for researchers traveling abroad;
    C. Wiping laptops, tablets, smartphones, and other electronic devices to protect against digital exploitation before, during, and after foreign travel;
    D. Establishing policies and procedures for the protection and safeguarding of research information and materials while on foreign travel, to include discouraging researchers from crossing international borders with devices containing research data or instituting software use restrictions; and
    E. Providing security briefings for individuals prior to traveling internationally, and tailored briefings as needed for destinations considered high-risk.

20. ***Managing potential risks associated with foreign visitors and visiting scholars.*** Principled international collaboration is vitally important to the success of America's research enterprise. However, research organizations should recognize and account for the fact that, like foreign travel

(Recommendation 19), hosting foreign researchers can pose security risks of exploitation. Research organizations should establish and administer policies and processes to help ensure that the organization, its personnel, and its foreign visitors are held to the same high standards of research integrity.

With those objectives in mind, research organizations should develop and deploy requirements for vetting and securely hosting foreign visitors to mitigate potential risks to the security or integrity of the research environment. These requirements could include:

A. Requiring research personnel to alert organization officials, potentially through the organization's export control, research compliance, or international affairs office, when they plan to have foreign visitors come to visit campus and/or tour their laboratories;
B. Requiring research personnel to provide justification to organization officials of the research value of long-term visitors and visiting scholars;
C. Requiring that foreign visitors participate in training on research security and responsible and ethical conduct of research;
D. Screening against available lists of restricted or denied parties, including the Consolidated Screening List;[12] and
E. Taking measures for securely hosting and escorting foreign visitors, including measures to avoid unauthorized information gathering.

21. ***Establish and maintain effective data security measures.*** Data security and cybersecurity are a significant challenge to research security, as they are in many other areas. Research organizations should work continually to identify and implement measures to improve data security, internal breach prevention, and incident response processes, and to maintain compliance with relevant requirements.

    The NIST Cybersecurity Framework[13] serves as a useful resource to help research organizations establish and maintain effective data security measures. The Framework is comprised of five core functions:

    A. Identify - Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.
    B. Protect - Develop and implement appropriate safeguards to ensure delivery of critical services.
    C. Detect - Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
    D. Respond - Develop and implement appropriate activities to take regarding a detected cybersecurity incident.
    E. Recover - Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

    NIST also provides educational resources[14] and examples[15] of how research organizations have successfully used the Framework to improve their cybersecurity risk management.

[12] Consolidated Screening List. https://legacy.export.gov/csl-search
[13] NIST Cybersecurity Framework. https://www.nist.gov/cyberframework
[14] NIST Cybersecurity Framework: Online Learning. https://www.nist.gov/cyberframework/online-learning
[15] NIST Cybersecurity Framework: Success Stories. https://www.nist.gov/cyberframework/success-stories

Conclusion

Implementing the recommendations in this report will help protect the security and integrity of the American and international R&D enterprises, while preserving the open and collaborative nature that has been critical to U.S. leadership in R&D. Our goal is to ensure that scientists and students—both U.S. and foreign national—who follow laws, regulations, policies, and codes of conduct will be welcome and supported within a vibrant and secure enterprise that remains a desirable destination for researchers across the world.

Success in this endeavor will require partnership and cooperation across the R&D enterprise, including the Federal Government, research organizations, private companies, and non-government organizations. Together, we can uphold the principles that bolster the integrity of our research enterprise, strike the right balance between openness and security, and ensure that the United States continues to engage in productive collaboration and remains a global leader in S&T.

Appendix A. Federal Government and Agency Contacts

Agency	Research Security POC
Office of Science and Technology Policy, Executive of the President	JCORE@ostp.eop.gov
National Science Foundation	research-protection@nsf.gov
National Institutes of Health	grantscompliance@od.nih.gov
Department of Agriculture	ocspolicy@usda.gov
Department of Defense	osd.pentagon.ousd-r-e.mbx.dod-grants-policy-office@mail.mil
Department of Education	ForeignSourceReporting@ed.gov
Department of Energy	researchsecurity@science.doe.gov
Department of Homeland Security	ststrategyandpolicy@hq.dhs.gov
Department of Justice	nsd.public@usdoj.gov
Department of State	OES-STC-DG@state.gov
Federal Bureau of Investigation	Academic Institutions: Academia@fbi.gov Other research organizations: HQ-DIV00-OPS-PSC-PROGRAM@ic.fbi.gov
National Institute of Standards and Technology	fnareview@nist.gov