Subcommittee on Research Security
National Science and Technology Council
Office of Science and Technology Policy

DRAFT Research Security Programs Standard Requirement

Prepared by the Interagency Working Group on Research Security Programs, Subcommittee on Research Security, National Science and Technology Council

February 2023

Introduction

After more than a year of productive partnership among Federal agencies, together with engagement with the external research community, the National Science and Technology Council of the Office of Science and Technology Policy (OSTP) released Guidance for Implementing National Security Presidential Memorandum 33 (NSPM-33) on National Security Strategy for United States Government-Supported Research and Development, on January 4, 2022. NSPM-33 charges OSTP with "coordina[ting] activities to protect Federally funded R&D from foreign government interference, and outreach to the United States scientific and academic communities to enhance awareness of risks to research security and Federal Government actions to address these risks." A similar charge is captured in the National Defense Authorization Act of 2020.[1]

The Guidance, called for by the Director of the Office of Science and Technology Policy, delivers on three key priorities, consistent with the values of the Biden-Harris Administration, in the areas of research security and integrity: (1) protecting America's security and openness; (2) being clear in our delivery of guidance and information to impacted communities, so that compliance with NSPM-33 is easy, straightforward, and minimally burdensome; and (3) ensuring that our policies do not fuel xenophobia or prejudice.

The Guidance details the implementation of five key NSPM-33 provisions, including disclosure requirements and standardization, digital persistent identifiers, consequences for violating disclosure requirements, agency information sharing, and research security programs. These provisions apply to all federally funded research and development, focused primarily, but not solely, on fundamental research. They also represent best practices that can be extended to federally funded development, demonstration and deployment projects, among other types of science and technology activities.

This Memorandum relates to the last provision, **research security programs**. Specifically, Section 4(g) of NSPM-33 reads as follows:

> ***Risk Identification and Analysis***. *...Heads of funding agencies shall require that research institutions receiving Federal science and engineering support in excess of 50 million dollars per year certify to the funding agency that the institution has established and operates a research security program. Institutional research security programs should include elements of cyber security, foreign travel security, insider threat awareness and identification, and, as appropriate, export control training. Heads of funding agencies*

[1] The language from the 2020 NDAA (Public Law 116-92), captured in Sec. 1746. (a), states: "In general.--The Director of the Office of Science and Technology Policy, acting through the National Science and Technology Council, in consultation with the National Security Advisor, shall establish or designate an interagency working group 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 progression and American leadership in science and technology."

shall consider whether additional research security program requirements are appropriate for institutions receiving Federal funding for R&D in critical and emerging technology areas with implications for United States national and economic security.

To ensure that Federal research agencies move towards upholding this provision in a standardized manner, and aligning with the values of consistency and transparency driving the NSPM-33 implementation, this Memorandum provides further details on appropriate standards for research security programs that would facilitate compliance with NSPM-33. These requirements should be communicated by Federal research agencies to research organizations as part of their funding agreement processes.

Research security program requirements include the research security training requirement described in Sec. 10634 of P.L. 117-167, commonly known as the CHIPS and Science Act. Establishing a research security program that includes, but is not limited to, research security training is a requirement of covered research organizations, per NSPM-33.

Covered Research Organizations

Research organizations that have received at least $50 million per year in Federal science and engineering support for each of the previous two consecutive fiscal years must establish and maintain a research security program containing the elements outlined below. Covered research organizations may decide that elements beyond the standards discussed in this Memorandum are necessary. In addition, Federal research agencies may impose additional requirements beyond these standards, as is expected, for example, for classified and controlled unclassified information (CUI). The baseline requirements for research security programs do not create exceptions to other legal requirements that may apply, and other legal requirements do not waive the required standards.

To assess the amount of science and engineering support that research organizations have received from the Federal Government over the course of a fiscal year, organizations may refer to usaspending.gov, in addition to their own financial records. Research organizations that are non-profit educational institutions or non-profit organizations also may consult the National Science Foundation's data on "Federal Science and Engineering Support to Universities, Colleges, and Nonprofit Institutions."

The requirement outlined in Section 4(g) of NSPM-33 applies to any research organization, such as a university, whose component parts (e.g., departments, affiliated research centers, or schools) receive at least $50 million in Federal science and engineering support annually in the aggregate. If a research organization is part of an interconnected network of research organizations (e.g., a public university system.), the requirement applies only to those individual organizations within the network that individually receive at least $50 million in annual Federal science and engineering support. Subawards must be included in the total award amount considered by each research organization. Should questions or concerns emerge, email: **researchsecurity@ostp.eop.gov**.

Covered research organizations will have one year from the date of this Memorandum to establish a research security program that complies with the standards established herein. Covered research organizations will be required to provide a status update 120 days from the issuance of this Memorandum, by posting it publicly, such as on the website of the research organization.

Overarching Program Requirements and Certification

As a condition for receiving and maintaining Federal science and engineering support, all covered research organizations must certify that they maintain a research security program that meets the requirements for foreign travel security, research security training, cybersecurity, and export control training, detailed below.[2] Self-certification will take place centrally on SAM.gov on an annual basis for covered research organizations Self-certification will begin one year from the issuance of this Memorandum.

Covered research organizations must maintain a description of the finalized research security program, made available on a publicly-accessible website, with descriptions of each item contained in this Memorandum. CUI information attached to areas such as cybersecurity or export controls need not be made public. Covered research organizations also must provide documentation of the maintained research security program within 30 days of a request from a research agency that is funding an R&D (Research and Development) award or considering an application for R&D award funding to that research organization.

As a component of their research security programs, covered research organizations must designate a research security point of contact and provide publicly accessible means to contact that individual, such as a website. Covered research organizations should manage the required elements as an integrated program. Covered research organizations must maintain clear response procedures to address reported allegations of research security non-compliance. They also must report incidents of research security violations to the federal awarding agency or agencies. Covered research organizations should conduct regular self-assessments to ensure that their research security programs are functioning effectively.

Foreign Travel Security

Covered research organizations must establish or maintain international travel policies for covered individuals (see Definitional Appendix) engaged in federally funded R&D who are traveling internationally for organizational business, teaching, conference attendance, research purposes, or who receive offers of sponsored travel for research or professional purposes.

International travel policies and procedures must include:

1. Maintenance of an organizational record of covered international travel by covered individuals engaged in federally funded R&D.
2. A disclosure and authorization requirement in advance of international travel.
3. Mandatory applicable security briefings, and advice regarding electronic device security (e.g., smartphones, laptops) prior to covered international travel, or to travel including electronic devices utilized for federally funded R&D or bought with Federal funding.

Please see the Definitional Appendix for definitions of each of these terms. Best practices for electronic device security that have been developed by the National Counterintelligence and Security Center can be accessed at Travel Tips (dni.gov). For further information on country-specific security precautions, refer to guidance from the Department of State.

[2] NSPM-33 cites "insider threat awareness and identification" as a separate component of research security programs, while the Implementation Guidance does not. This is because, in the Implementation Guidance, insider threat awareness and identification are subsumed into the broader category of "research security training."

Research Security Training

Covered research organizations must implement research security training as a component of research security programs required for qualifying organizations in accordance with NSPM-33. Covered research organizations must incorporate the below elements of research security into existing training programs, such as training on responsible and ethical conduct of research, and must provide training at initial orientation for new personnel as well as regular refresher training. Covered research organizations must maintain the ability to certify that personnel have completed the required training for the purposes of Federal R&D award applications as mandated by the CHIPS and Science Act.

Research security training must be regularly updated and include components such as research security threat awareness, identification, and insider threats. Training should be tailored to appropriate personnel, such as faculty, staff, and students. Covered research organizations must annually certify their training meets requirements. Training programs must include instruction in the following areas:

1. Understanding why research security is important for the U.S. R&D enterprise and what constitutes foreign interference.
2. The importance of non-discrimination as a guiding principle of U.S. research security policy.
3. Disclosure policy and how it is used, particularly with regard to conflicts of interest and conflicts of commitment.
4. Identifying, managing, and mitigating risk, particularly in the context of foreign talent programs and insider threats.
5. Proper use of funds.
6. The value of and challenges with international collaboration
7. Responsible international travel practices.
8. Basic cybersecurity hygiene and data protection practices, including recognition of and response to social engineering threats and cyber breaches.
9. Intellectual property and data protection requirements and best practices.

In the event of a research security breach finding, covered research organizations must conduct tailored training related to the finding as a component of the organization's response, and keep a record of such trainings for affected individuals.

Cybersecurity

Covered research organizations must implement baseline safeguarding protocols and procedures for information systems used to store, transmit, and conduct federally funded R&D. Collectively, these protocols provide protection of scientific data from ransomware and other data integrity attack mechanisms. The following protocols are required:

1. Limit information system access to authorized users and processes acting on behalf of authorized users, or devices (including other information systems), as described in Office of Management and Budget Memorandum M-21-31 on Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents.

2. Limit information system access to the types of transactions and functions that authorized users are permitted to execute.
3. Verify and control/limit connections to, and use of, external information systems.
4. Control any non-public information posted or processed on publicly accessible information systems.
5. Identify information system users and processes acting on behalf of users, or devices.
6. Authenticate (or verify) the identities of those users, processes, and devices, as a prerequisite to allowing access to organizational information systems.
7. Monitor, control, and protect organizational communications (information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.
8. Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.
9. Identify, report, and correct information and information system flaws in a timely manner.
10. Provide protection from malicious code at appropriate locations within organizational information systems.
11. Update malicious code protection mechanisms when new releases are available.
12. Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, and executed.

Covered research organizations must follow applicable cybersecurity requirements and controls beyond these baseline requirements for research involving classified information, controlled unclassified information (CUI), commercially sensitive information, or information that, if inadvertently or intentionally released, may harm US Government rights.

Please refer to the National Institute of Standards and Technology website for further information and updates on cybersecurity standards for research security purposes, which will be guided by Section 10229 of the CHIPS and Science Act.

Export Control Training

Covered research organizations conducting R&D that is subject to export control restrictions must provide training to relevant personnel on requirements and processes for reviewing foreign sponsors, collaborators and partnerships, and for ensuring compliance with Federal export control requirements and restricted entities lists. Areas subject to Federal export control requirements and restricted entities are defined through the International Traffic in Arms Regulations (ITAR) and Export Administration Regulations (EAR). The training must emphasize that the "fundamental research" exception has explicit limitations. For example, federally funded R&D of "applied" energy technologies (i.e., "applied research"), many with dual-uses (civilian and military), fall outside of any exception and are subject to such laws.

Definitional Appendix

Conflict of commitment – 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 and effort, including obligations to dedicate time in excess of organizational or research agency policies or commitments. Other types of conflicting obligations, including obligations to improperly share information with, or to withhold information from, an employer or research agency, can also threaten research security and integrity, and are an element of a broader concept of conflicts of commitment used in this document.

Conflict of interest – A situation in which an individual, or the individual's spouse or dependent children, has a significant financial interest or financial relationship that could directly and significantly affect the design, conduct, reporting, or funding of research.

Controlled unclassified information (CUI) – Information that requires safeguarding or dissemination controls consistent with applicable laws, regulations, and Government-wide policies, but is not classified. For more information, refer to: https://www.archives.gov/cui.

Covered individual or senior/key personnel – 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 personnel 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.

Covered international travel – Covered international travel is international, official business travel that contributes to a substantive, meaningful way to the 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. Covered international travel may include travel by faculty, staff, or students seeking or receiving Federal research and development funding and researchers at Federal agency laboratories and facilities, including Government-owned, contractor operated laboratories and facilities, and other recipient institutions.

Covered Research Organizations – Covered research organizations have received at least $50 million per year in Federal science and engineering support for each of the previous two consecutive fiscal years. Management and Operations (M&O) Contractors are not covered research organizations. Covered research organizations may be single research organizations, such as a university, non-profit educational institutions or non-profit organizations, and are inclusive of the component parts of that research organization (e.g., departments, affiliated research centers, or schools). Covered research organizations do not include interconnected networks of universities (e.g., public university systems).

Current and pending research support – (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 or not 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. This term has the same meaning as the term Other Support as applied to researchers in NSPM-33: As articulated in NSPM-33, Other Support includes 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, services, or employees). This includes 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.

Digital persistent identifier (DPI or digital PID) – A digital identifier that is globally unique, persistent, machine resolvable and processable, and has an associated metadata schema. Consistent with NSPM-33, digital persistent identifiers for individuals are used to disambiguate and identify an individual person.

Federal research agency or research agency – Any Federal department or agency with an annual extramural research expenditure of over $100,000,000. This term has the same meaning as "funding agency" in NSPM-33.

Federal science and engineering support -- Activities that provide support related to scientific research and education. Such projects are generally oriented toward academic departments, institutes, or whole institutions. This term implies a spectrum of varying types of support. At one extreme is support provided without any specification of purpose other than that the funds be used for scientific activities. Another kind of general support is to be found in projects that provide funds for activity within a specified field of S&E (Science and Engineering) but without specifying an explicit purpose. This support may permit a significant measure of freedom as to purpose (e.g., research, faculty support, education, institutional support). Included are: R&D funding including research awards; facilities and equipment for instruction in S&E; fellowship, traineeship, and training grant programs that are directed primarily toward S&E; the development and maintenance of the scientific and technical manpower; facilities and equipment for R&D such as laboratory construction; and general support for S&E, which includes activities that provide nonspecific or general support for activities related to scientific research and education. Organizations may refer to usaspending.gov, in addition to their own financial records, to determine their Federal science and engineering support. Research organizations that are non-profit educational institutions or non-profit organizations may also consult the National Science Foundation's data on "Federal Science and Engineering Support to Universities, Colleges, and Nonprofit Institutions."

Foreign government-sponsored talent recruitment program – An effort organized, managed, or funded by a foreign government, or a foreign government instrumentality or entity, to recruit science and technology professionals or students (regardless of citizenship or national origin, or 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, sometimes through illicit 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 United States research facilities or receipt of Federal research funds while concurrently working at and/or receiving compensation from a foreign institution, and some direct participants not to disclose their participation to United States entities. 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.

Gift – Includes any gratuity, favor, discount, entertainment, hospitality, loan, forbearance, license, special access, equipment time, samples, research data, or other item having monetary value. A gift also includes services as well as gifts of training, transportation, local travel, lodging, meals, research hours, whether provided in-kind, by purchase of a ticket, payment in advance, or reimbursement after the expense has occurred.

Honorarium – A payment of money or anything of value for an appearance, speech, article, or other form of compensation or award.

Insider threat – Insider threat means the threat that an insider will use their authorized access, wittingly or unwittingly, to do harm to the security of the United States. This harm can include damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities. For research organizations, this harm can include malicious, complacent, or unintentional acts that negatively affect the integrity, confidentiality, and availability of the organization, its data, personnel, or facilities.

International Travel – International travel includes any approved travel for official business (whether wholly or partly on official business) from the United States (including the Commonwealths of Puerto Rico and the Northern Mariana Islands, and the territories and possessions of the United States) to a foreign country and return or travel between foreign countries by persons, including foreign nationals, whose salaries or travel expenses or both will ultimately be funded in whole or in part by a Federal research agency from its appropriations. International travel also includes travel funded by non-Department entities for which the traveler represents the Department or conducts business or discusses work performed on behalf of the U.S. Government.

Intramural Researcher – An individual who conducts research supported by the agency in which they are employed.

Research and development (R&D) – Includes basic research, applied research, and experimental development. Basic research is experimental or theoretical work undertaken primarily to acquire new knowledge of the underlying foundations of phenomena and observable facts. Applied research is original investigation undertaken in order to acquire new knowledge, and directed primarily towards a specific practical aim or objective. Experimental development is creative and systematic work, drawing on knowledge gained from research and practical experience, which is directed at producing new products or processes or improving existing products or processes. Like research, experimental development will result in gaining additional knowledge. Experimental development includes the production of materials, devices, and systems or methods, including the design, construction, and testing of experimental prototypes. Experimental development also includes technology demonstrations in cases where a system or component is being demonstrated at scale for the first time, and it is realistic to expect additional refinements to the design (feedback R&D) following the demonstration.

Research and development award – Support provided to an individual or entity by a Federal research agency to carry out R&D activities, which may include support in the form of a grant, contract, cooperative agreement, or other such transaction. The term does not include a grant, award, contract, agreement, or other transaction for the procurement of goods or services to meet the administrative needs of a Federal research agency.

Research integrity – 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.

Research organization – An entity that has applied for or received an R&D award from a Federal research agency. This term has the same meaning as "entity" as defined in Section 223 of the NDAA for 2021.

Research security – Safeguarding 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.

Research security incident – An action regarding Federal science and engineering support, such as failure to disclose information that could pose financial conflicts of interest or conflicts of commitment; misappropriation of research data or knowhow; and diversion of intellectual property; among others, due to improper foreign influence.

Sponsored travel – Sponsored travel refers to any travel offered in an official capacity, i.e., not personal travel, to a researcher due to their professional work, but paid for by a third-party. The third-party can be a Federal Government agency, a private corporation, an international organization, or a foreign government.

Security incident – Security incidents include a range of possible actions, inactions, or events that cause one or more of the following results:

a. Pose threats to national security interests and/or Federal Government or recipient institution assets
b. Create potentially serious or dangerous security situations
c. Have a significant effect on the agency's safeguards and security program's capability to protect its interests
d. Indicate the failure to adhere to security procedures
e. Illustrate the system is not functioning as designed by identifying and/or mitigating potential threats (e.g., detecting suspicious activity, hostile acts, elicitation)
f. Cause adverse effects of loss or compromise of classified or controlled unclassified information.

United States Government supported research and development – Includes R&D projects funded by the U.S. Government, in whole or in part; projects that use U.S. Government equipment, facilities, or data for conducting R&D; and R&D projects in which U.S. Government employee and contractor personnel participate, regardless of the project's funding source.