EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF SCIENCE AND TECHNOLOGY POLICY
WASHINGTON, D.C. 20502

July 9, 2024

MEMORANDUM FOR THE HEADS OF FEDERAL RESEARCH AGENCIES

FROM: Arati Prabhakar
Assistant to the President for Science and Technology
Director of the Office of Science and Technology Policy

SUBJECT: Guidelines for Research Security Programs at Covered Institutions

---

To address risks posed by strategic competitors to the U.S. research and development (R&D) enterprise, the Biden-Harris Administration is implementing several measures to improve research security while preserving the openness that has long enabled U.S. R&D leadership throughout the world and without exacerbating xenophobia, prejudice, or discrimination.

This memorandum provides federal research agencies with guidelines for implementing a certification requirement imposed by National Security Presidential Memorandum-33 (NSPM-33).[1] Specifically, federal research agencies must require certain research institutions ("covered institutions") to certify to the funding agency that the institution has established and operates a research security program, including several specific elements described in detail below.

These guidelines are issued in accordance with NSPM-33 and certain provisions of Public Law 117-167 (the CHIPS and Science Act).[2] The White House Office of Science and Technology Policy (OSTP)—in consultation with National Science and Technology Council (NSTC) Subcommittee on Research Security, the Office of Management and Budget (OMB), and stakeholders—is responsible for developing a "standardized requirement" for "uniform implementation" across federal research agencies.[3] This memorandum describes and sets forth that standardized requirement.[4] It reflects the significant work of the NSTC Subcommittee on

---

[1] "Presidential Memorandum on United States Government-Supported Research and Development National Security Policy." The White House (January 14, 2021) §4(g). https://trumpwhitehouse.archives.gov/presidential-actions/presidential-memorandum-united-states-government-supported-research-development-national-security-policy/

[2] Pub. L. 117-167 §10634, 42 U.S.C. §19234. https://www.congress.gov/bill/117th-congress/house-bill/4346/text

[3] "Guidance for Implementing National Security Presidential Memorandum 33 (NSPM-33) on National Security Strategy for United States Government-Supported Research and Development." National Science and Technology Council (NSTC). January 2022. pp.18-21. https://www.whitehouse.gov/wp-content/uploads/2022/01/010422-NSPM-33-Implementation-Guidance.pdf

[4] This guidance is intended to be consistent with NSPM-33 and relevant portions of the CHIPS and Science Act. It supersedes, in full, the portions of the NSTC Implementation Guidance describing Research Security Programs (see, in particular, pp. 18-21). With respect to section 4(g) of NSPM-33, the guidance in this memorandum sets forth the "standardized requirement" for "uniform implementation" across federal agencies, as contemplated by the NSTC

Research Security, OMB, experts, and feedback from the public on a published draft memorandum.[5]

(I) Background

Science, technology, and innovation have been integral to U.S. leadership in the world for many decades, supported by the strength of the U.S. research community. Today, the global strategic environment is characterized by fierce military and economic competition among many actors. This marks a significant change from the global environment 10 years ago. In particular, the People's Republic of China (PRC) intends to reshape the international order and increasingly has the military and economic power to advance that objective.[6] Technology and R&D are central to this strategic competition, and the PRC has exploited international research collaboration by undermining values – such as transparency, accountability, and reciprocity – in order to advance its strategic objectives and military modernization.

To address risks to research security, the Biden-Harris Administration is implementing NSPM-33 and research security provisions of the CHIPS and Science Act[7] to align with American values. NSPM-33 recognizes that the open and collaborative nature of the U.S. R&D enterprise underpins America's science and technology leadership, economic competitiveness, and national security.[8] It is crucial that we preserve this open and collaborative environment to compete effectively.[9] This includes prioritizing attracting global talent to the United States to conduct R&D.

Importantly, federal research agencies should implement research security policies in a way that treats everyone equally under law, without xenophobia, prejudice, or discrimination, a principle reinforced by the CHIPS and Science Act. The law also requires that research security activities

---

Implementation Guidance describing Research Security Programs (p. 19). With respect to section 10634(a) of the CHIPS and Science Act (42 U.S.C. §19234), the guidance in this memorandum sets forth training requirements for "consistent" implementation across federal agencies, but only for entities that qualify as "covered institutions." Implementation of section 10634(a) for entities that do not qualify as "covered institutions" is outside the scope of this memorandum.

[5] "Request for Information; NSPM 33 Research Security Programs Standard Requirement" (88 Fed Reg 14187) Office of Science and Technology Policy (March 7, 2023). https://www.federalregister.gov/documents/2023/03/07/2023-04660/request-for-information-nspm-33-research-security-programs-standard-requirement

[6] "National Security Strategy." The White House (October 2022), 23. https://whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf

[7] CHIPS and Science Act §10634, 42 U.S.C. §19234.

[8] NSPM-33 §1.

[9] "Readout of Dr. Alondra Nelson's Participation in the G7 Science Ministerial: Progress Toward a More Open and Equitable World." The White House (June 2022). https://www.whitehouse.gov/ostp/news-updates/2022/06/21/readout-of-dr-alondra-nelsons-participation-in-the-g7-science-ministerial-progress-toward-a-more-open-and-equitable-world/

be carried out in a manner that does not target, stigmatize, or discriminate against individuals on the basis of race, ethnicity, or national origin.[10]

The purpose of the Administration's research security efforts is to make sure that institutions of higher education and other research institutions recognize the altered global landscape and fulfill their responsibilities as the first line of defense against improper or illicit activity. Unlike proprietary R&D, most academic research is intended for publication or to be shared, and it thrives in a global exchange of ideas. But some research can lie close to applications with national security implications. We know that members of the R&D community are still acclimating to the changes in geopolitics. Many of the actions that researchers were encouraged to undertake only a decade ago, including collaborations with the PRC, are now being recognized for the risks they may present. This is why we must be clear with the research community about how the world has changed; how the policies and practices of foreign countries of concern differ from those of the U.S. R&D enterprise and the values that sustain our system; and the ways that some of the results from U.S. R&D can contribute to human rights abuses, surveillance, and military aggression.

It is vital that research security programs increase awareness of research security threats and enable researchers, other participants in the U.S. R&D enterprise, and federal research agencies to respond appropriately while maintaining openness and ensuring fairness. Federal research agencies should be attentive to and study how research security programs are implemented by covered institutions, as well as the impact of research security programs on (A) covered institutions and participants in the U.S. R&D enterprise; (B) covered individuals and the researcher community; (C) and U.S. government-supported R&D and U.S. R&D. Federal research agencies should use the NSTC Subcommittee on Research Security as a forum for sharing feedback on implementation of research security programs. OSTP will consider amendments to this policy as informed by this feedback.

(II) Research Security Program Requirements

This section describes the "standardized requirement" for federal research agencies when requiring covered institutions to certify pursuant to NSPM-33 about their research security programs. This section includes substantive elements as well as a standardized definition of "covered institution."[11]

Definition of Covered Institution

NSPM-33 directs federal research agencies to require that participants in the U.S. R&D enterprise receiving federal science and engineering support "in excess of $50 million per year" certify to the funding agency that the institution has established and operates a research security program.[12] For purposes of this guidance, a participant in the U.S. R&D

[10] CHIPS and Science Act §10637, 42 U.S.C. §19236.

[11] Additional standardized terms and definitions are set forth in Section (IV).

[12] NSPM-33 §4(g).

enterprise is a "covered institution" if and only if (A) it is an institution of higher education,[13] a federally funded research and development center (FFRDC), or a nonprofit research institution; and (B) it receives in excess of $50 million per year, in fiscal year 2022 constant dollars, under (1) the three-year average of federal R&D obligations provided to participants in the U.S. R&D enterprise as reported in the most recent version of the Survey of Federal Science and Engineering Support to Universities, Colleges, and Nonprofit Institutions;[14] or (2) the three-year average of federal R&D obligations to FFRDCs as provided in the most recent versions of the Survey of Federal Funds for Research and Development[15].

As required by NSPM-33[16] federal research agencies shall require covered institutions to certify that they have implemented their own research security programs, including research security training as required by the CHIPS and Science Act,[17] to address their unique needs, challenges, and risk profiles. Federal research agencies are encouraged to adopt research security requirements similar to those in this memorandum for non-covered institutions that meet the funding threshold described in part (B) of the definition of covered institution.

As a standardized requirement, federal research agencies shall require covered institutions to certify that their research security programs include elements relating to (1) cybersecurity; (2) foreign travel security; (3) research security training; and (4) export control training, as appropriate. These elements are described in more detail below.

(1) Cybersecurity

As the first element of the standardized requirement, federal research agencies shall require institutions of higher education to certify that the institution will implement a cybersecurity program consistent with the cybersecurity resource for research institutions described in the CHIPS and Science Act,[18] within one year after the National Institute of Standards and Technology (NIST) of the Department of Commerce publishes that resource. For covered institutions that are not institutions of higher education, federal research agencies shall require covered institutions to certify that the institution will implement a cybersecurity program

[13] For the purposes of part (A) of this definition, a University Affiliated Research Center (UARC) should be considered part of its affiliated university. For the purposes of part (B) of this definition, any federal funding received by a UARC should be considered part of the funding of its affiliated university.

[14] https://ncses.nsf.gov/surveys/federal-support-survey/. For non-academic nonprofit institutions, the three-year average of federal R&D and R&D plant obligations as provided in the most recent versions of the Survey.

[15] https://ncses.nsf.gov/surveys/federal-funds-research-development

[16] NSPM-33 §4(g).

[17] CHIPS and Science Act §10634, 42 U.S.C. §19234.

[18] CHIPS and Science Act §10229, 42 U.S.C. §18935. The National Institute of Standards and Technology (NIST) has published an initial public draft of the cybersecurity resource: "NIST IR 8481: Cybersecurity for Research: Findings and Possible Paths Forward." NIST (August 31, 2023). https://csrc.nist.gov/pubs/ir/8481/ipd

consistent with another relevant cybersecurity resource maintained by NIST or another federal research agency.

(2) Foreign Travel Security

As the second element of the standardized requirement, federal research agencies shall require covered institutions to:

(A) certify that the institution (1) will implement periodic training on foreign travel security to covered individuals engaged in international travel, including sponsored international travel, for organization business, teaching, conference attendance, or research purposes, within one year after a foreign travel security training resource is made available by a federal research agency,[19] and (2) ensures that all such covered individuals take this training at least once every six years; and

(B) implement a travel reporting program, to include an organizational record of international travel, including sponsored international travel, for organization business, teaching, conference attendance, and research purposes by covered individuals, for covered individuals participating in R&D awards when a federal research agency has determined that security risks warrant travel reporting in accordance with the terms of an R&D award.

(3) Research Security Training

As the third element of the standardized requirement, federal research agencies shall require covered institutions to certify that the institution has implemented a research security training program for all covered individuals to address the unique needs, challenges, and risk profiles of covered individuals and to certify that the institution ensures that each such covered individual completes such training.

Federal research agencies must allow covered institutions to meet this requirement in either of the following ways:

(A) The covered institution may certify that (1) the institution requires covered individuals to complete training modules made available by the National Science Foundation (NSF)[20] (or successor trainings developed by the federal government designed to satisfy the

[19] One type of resource that meets the training requirement (i.e., part (A)) is a training module made available by a federal research agency. Through coordination of the NSTC Subcommittee on Research Security, the National Science Foundation (NSF)—in coordination with the National Institutes of Health, the Department of Energy, the Department of Defense, the Department of State, and OSTP—intends to enter into an agreement or contract with a qualified entity for the development of a foreign travel security training module.

[20] "Research Security Training Modules." https://rst.nsf.gov

relevant requirements of the CHIPS and Science Act[21] and NSPM-33[22]) and (2) each such covered individual has completed such trainings; or

(B) The covered institution may certify that the institution requires covered individuals to complete research security training and each such covered individual has completed the research security training program. The research security training program shall (1) provide covered individuals with explicit examples of behaviors that have resulted in a known improper or illegal transfer of U.S. government-supported R&D in the context of the research environment, as described to the covered institution by federal research agencies; and (2) communicate to covered individuals the importance of U.S. researcher participation in global discoveries, including attracting foreign talent to U.S. research institutions, as a core principle of maintaining international leadership and national security.

(4) Export Control Training

As the fourth element of the standardized requirement, federal research agencies shall require covered institutions to certify that the institution requires covered individuals who perform R&D involving export-controlled technologies, to complete training on U.S. export control and compliance requirements.

Federal research agencies must allow covered institutions to meet this requirement in either of the following ways:

(A) The covered institution may certify that the institution requires covered individuals who perform R&D involving export-controlled technologies to complete relevant trainings administered by the Bureau of Industry and Security of the Department of Commerce and that each relevant covered individual has completed such training. Additionally, the Directorate of Defense Trade Controls at the Department of State has publicly available resources to assist an institution in developing its own individually tailored and robust compliance programs; [23]or

(B) The covered institution may certify that the institution requires covered individuals who perform R&D involving export-controlled technologies to complete training and that each such covered individual has completed training on complying with (1) U.S. export control and compliance requirements to relevant covered individuals; and (2) requirements and processes for reviewing foreign sponsors, collaborators, and partnerships.

[21] CHIPS and Science Act §10634, 42 U.S.C. §19234.

[22] NSPM-33 §4(g).

[23] "Directorate of Defense Trade Controls." https://www.pmddtc.state.gov/ddtc_public/ddtc_public

(III) Agency Responsibilities and Principles for Implementing this Memorandum

This section articulates additional principles and requirements related to federal research agencies implementing research security requirements. In developing research security program requirements, federal research agencies should communicate clear expectations of covered institutions; institute policies that maximize transparency with covered institutions, covered individuals, and the public; require additional risk mitigation measures at the level of specific R&D awards, when practicable, that may require heightened security measures; and ensure covered institutions have access to trainings, materials, and other resources required to fulfill research security program requirements.

(1) Non-Discrimination

Consistent with the CHIPS and Science Act,[24] federal research agencies shall ensure that the research security program requirements they impose on covered institutions do not result in targeting, stigmatization, or discrimination against individuals on the basis of race, color, ethnicity, religion, sex (including pregnancy, sexual orientation, or gender identity), national origin, age (40 or older), disability, or genetic information (including family medical history). Federal research agencies shall require covered institutions to certify that they have implemented safeguards to protect the rights of researchers, students, and research support staff or otherwise comply with such requirements.[25]

(2) Flexibility

Federal research agencies should provide covered institutions with flexibility to structure their research security program to best serve the institution's particular needs and to leverage existing programs and activities where relevant, provided that the institution implements all required program components. This includes the flexibility to integrate research security program requirements into existing programs—such as existing cybersecurity programs or trainings—to maximize efficiency.

(3) Mechanism for Certifications by Covered Institutions

NSPM-33 directs federal research agencies to require covered institutions to "certify to the funding agency that the institution has established and operates a research security program."[26] The CHIPS and Science Act directs federal research agencies to require covered individuals as part of an R&D award application to certify that they have completed research security training and requires R&D award applicants to certify that covered individuals have completed relevant

[24] CHIPS and Science Act §10637, 42 U.S.C. §19236.

[25] Similar statutory and regulatory non-discrimination requirements may exist for covered institutions, including under Title VI of the Civil Rights Act of 1964 (42 U.S.C. §§ 2000d et seq.), Title IX of the Education Amendments of 1972 (20 U.S.C. §§ 1681 et seq.), the Rehabilitation Act of 1973 (29 U.S.C. §794), and the Age Discrimination Act of 1975 (42 U.S.C. §§ 6101 et seq.).

[26] NSPM-33 §4(g).

trainings.[27] For the purposes of this memorandum, a covered institution's certification requirement is met when the covered institution provides a written or electronic attestation to a federal research agency that the covered institution has met relevant research security program requirements.[28]

(4) Reducing Administrative Burden

Consistent with the CHIPS and Science Act[29] and NSPM-33,[30] in developing research security program requirements, federal research agencies should minimize administrative burden on covered institutions and covered individuals. Federal research agencies should also encourage covered institutions to minimize administrative burden on covered individuals.

Federal research agencies should be especially cognizant of administrative burden for institutions that may be less resourced, including research institutions in Established Program to Stimulate Competitive Research (EPSCoR) jurisdictions, historically black colleges and universities (HBCUs), and other minority serving institutions (MSIs).

Federal research agencies should be available to provide technical assistance and other resources necessary for covered institutions to comply with research security program requirements and other related research security requirements.

(5) Minimizing Impact to Smaller Institutions

Federal research agencies should avoid disadvantaging non-covered institutions during the award process in order to facilitate broad participation in the federal R&D enterprise.

(6) Additional Research Security Program Requirements

NSPM-33 permits federal research agencies to develop additional requirements for the research security programs of covered institutions beyond the four elements described in this memorandum.[31] Requirements in addition to those listed here should be limited to cases where (A) policies are required by statute, regulation, or executive order or other executive action; (B) more stringent protections are necessary for protection of R&D that includes classified information, technologies subject to Export Administration Regulations, or otherwise legally protected matters; or (C) there are other compelling agency-specific reasons consistent with legal

[27] CHIPS and Science Act §10634(a)(1), 42 U.S.C. §19234(a)(1).

[28] Within 90 days of the issuance of this memorandum, the NSTC Subcommittee on Research Security will provide agencies with additional details on a system for U.S. government collection of certifications from covered institutions.

[29] CHIPS and Science Act §10634(c)(2), 42 U.S.C. §19234(c)(2).

[30] NSPM-33 §3(b)(iv).

[31] NSPM-33 §4(g).

authorities and missions of an individual federal research agency and in coordination with the Director of OSTP.

When considering whether a covered institution will be subject to additional requirements not described in this memorandum as a part of their broader research security program, federal research agencies should first consider if:

- addressing a specific research security concern could be accomplished at the level of an R&D award;
- the additional requirement addresses a clear and describable risk related to an observed or known improper or illegal transfer of U.S. government-supported R&D to foreign countries of concern;
- the additional requirement is relevant to all fields of R&D conducted at the covered institution, including those that present minimal or no risk of U.S. government-supported R&D or technology transfer to foreign countries of concern;
- implementing the requirement would be substantially burdensome to the covered institution, particularly the least well-resourced covered institutions; and
- providing supplemental funds to the covered institution is necessary in order for them to satisfy the additional requirements.

As a reminder of current federal policies, additional research security program requirements are subject to review and approval by the Office of Information and Regulatory Affairs (OIRA) of OMB. A federal research agency may not conduct or sponsor, and a covered individual is not required to respond to, an information collection subject to the requirements of the Paperwork Reduction Act (PRA) unless it displays a valid OMB control number. Guidance for federal research agencies on obtaining approval from OIRA may be obtained from agency PRA officers.

(IV) Implementation Timeline

Within six months of the issuance of this memorandum, federal research agencies shall submit to OSTP and OMB plans for updating policies to ensure this guidance is reflected in the Research Security Programs Standard Requirements of each federal research agency. Updated policies of federal research agencies shall take effect no later than six months after finalized plans have been submitted to OSTP and OMB.

Federal research agencies shall ensure that covered institutions have adequate time, but not more than 18 months after the effective date of their plans, to implement the requirements of this memorandum. Agencies should ensure that covered institutions have maximum flexibility and the least burden possible in meeting their expectations under this memorandum.

(V) Definitions

For the purposes of this memorandum, the following definitions apply:

(1) ***Classified information*** – The term "classified information" has the meaning given such term in Section 10339(b)(1) of the CHIPS and Science Act (42 U.S.C. 19038(b)(1)).

(2) ***Covered individual*** – The term "covered individual" has the meaning given such term in Section 10638(1) of the CHIPS and Science Act (42 U.S.C. 19237(1)).

(3) ***Covered institution*** – The term "covered institution" is defined in section (II) of this memorandum.

(4) ***Federal research agency*** – The term "federal research agency" has the meaning given the term "Federal research agency" in Section 10002(10) of the CHIPS and Science Act (42 U.S.C. 18901(10)).

(5) ***Foreign country of concern*** – The term "foreign country of concern" has the meaning given such term in Section 10638(2) of the CHIPS and Science Act (42 U.S.C. 19237(2)).

(6) ***Institution of higher education –*** The term "institution of higher education" has the meaning given such term in Section 101(a) of the Higher Education Act of 1965 (20 U.S.C. 1001(a)).

(7) ***Non-covered institution*** – The term "non-covered institution" means a participant in the U.S. R&D enterprise that is not a covered institution.

(8) ***Participants in the U.S. R&D enterprise*** – The term "participants in the U.S. R&D enterprise" has the meaning given the term "participants in the United States R&D enterprise" in section 2(a) of NSPM-33.

(9) ***R&D award*** – The term "R&D award" has the meaning given the term "research and development award" in section 10002(25) of the CHIPS and Science Act (42 U.S.C. 18901(25)).

(10) ***Research and development*** and ***R&D*** – The terms "research and development" and "R&D" have the meaning given such terms in 2 C.F.R. §200.1.

(11) ***U.S. government-supported R&D*** – The term "U.S. government-supported R&D" has the meaning given the term "United States Government-supported R&D" in Section 2(b) of NSPM–33.