Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

Updated December 4, 2024

Research Security Policies: An Overview

The international scientific community generally views the free and open exchange of information as vital to the process of scientific inquiry, including the vetting of ideas and the verification of research results. The U.S. research ecosystem broadly operates on these principles. U.S. officials and others have raised concerns about various efforts of foreign governments—most notably the People's Republic of China—to influence and exploit the openness of the U.S. research ecosystem. The acquisition of U.S. advances in science and technology, intellectual property, and talent by strategic competitors may pose a risk to U.S. national defense and global economic competitiveness.

Congress and the executive branch have taken several actions intended to maintain the benefits of an open research ecosystem while protecting it from external threats. For example, in 2019, Section 1746 of the National Defense Authorization Act (NDAA) for Fiscal Year 2020 (P.L. 116-92) directed federal agencies, among other things, to develop descriptions of known and potential threats to federally funded research and development (R&D) and to the integrity of the U.S. scientific enterprise. In January 2021, President Trump issued National Security Presidential Memorandum 33 (NSPM-33), which "direct[ed] action to strengthen protections of United States Government-supported [R&D] against foreign government interference and exploitation." And in January 2022, the Biden Administration issued guidance to federal agencies on the implementation of NSPM-33.

This In Focus summarizes key developments in four selected research security policy areas—disclosure requirements; foreign talent recruitment programs; research security training and program requirements; and information sharing and risk assessment—and poses potential oversight questions for Congress to consider.

Disclosure Requirements

Congress and the executive branch have strengthened existing policies and instituted new requirements concerning the information that applicants for federal R&D funding must disclose, especially regarding foreign support.

In January 2021, with the enactment of the NDAA for FY2021 (P.L. 116-283), Congress directed federal agencies to require individuals applying for federal R&D funding to disclose all current and pending research support. Congress also charged the Office of Science and Technology Policy (OSTP) with ensuring that disclosure requirements are consistent across federal agencies.

Section 4(b)(vi) of NSPM-33 listed specific types of information that agencies should require funding applicants to disclose and reaffirmed the need for agency coordination. The 2022 NSPM-33 implementation guidance further elaborated that funding applicants should disclose "all resources made available, or expected to be made available, in support of the individual's [R&D] efforts," including both domestic and foreign support, both monetary and in kind. In November 2023, the National Science Foundation (NSF) released two common disclosure forms to assist agency collection of such disclosures: the Biographical Sketch Common Form and the Current and Pending (Other) Support Common Form. In February 2024, OSTP directed all federal agencies with annual extramural research expenditures over $100 million to require grant and cooperative agreement applications to include the forms.

P.L. 116-283 also directed agencies to require that covered individuals, as defined in the NSPM-33 implementation guidance, update their disclosure information during the term of the award, as determined by the agency. Though the NSPM-33 implementation guidance also directed agencies to require certified updates to disclosure reporting during the term of the award, the common disclosure form defers to individual agency policies on the frequency and timing of post-award disclosure requirements.

Foreign Talent Recruitment Programs

In addition to requiring the disclosure of foreign support, the executive branch and Congress have issued specific policies governing both federal employee and grantee participation in *foreign talent recruitment programs*. For example, Section 10631 of P.L. 117-167, known as the CHIPS and Science Act, directs agencies to establish policies to (1) require covered individuals (e.g., principal investigators) to disclose if they are party to a foreign talent recruitment program contract and, (2) to the extent practicable, require federal R&D funding recipients (e.g., universities) to prohibit covered individuals participating in *malign* foreign talent recruitment programs from working on projects supported by federal R&D awards. Section 10631 also prohibits all personnel of federal research agencies from participating in foreign talent recruitment programs.

Section 10632 specified that, not later than August 9, 2024, federal research agencies should establish policies requiring an R&D award proposal to include (1) certification from covered individuals that they are not a party to a malign foreign talent recruitment program, as part of the initial submission and annually for the duration of the award, and (2) certification from an institution of higher education or other organization applying for the award that each covered individual employed by the entity has been made aware of and is in compliance with the malign foreign talent recruitment program disclosure requirements.

The Biographical Sketch Common Form currently requires applicants to certify that, "at the time of submission," they are not party to a malign foreign talent recruitment program. It also includes the institutional certification required by statute.

In accordance with Section 10631(b) of the CHIPS and Science Act, in February 2024, OSTP issued uniform guidance to inform agency implementation of statutory prohibitions on foreign talent recruitment program participation. For example, the guidance indicates that, though statutory prohibitions pertain to current and/or ongoing program participation, agencies may "apply mitigation and management measures to address past participation."

Research Security Training and Program Requirements

To build awareness and strengthen compliance with research security policies, the executive branch and Congress have issued research security training and program requirements. For example, Section 4(g) of NSPM-33 directed agencies to require research institutions receiving more than $50 million per year in federal science and engineering support to certify that they have established and operate a research security program. The provision directed institutional research security programs to include "elements of cyber security, foreign travel security, insider threat awareness and identification, and, as appropriate, export control training."

Additionally, Section 10634 of the CHIPS and Science Act directs agencies to require specified individuals applying for R&D awards to complete research security training annually. It also requires OSTP to coordinate with relevant research agencies to develop research security training modules and to issue guidelines for institutions in developing research security training programs. In January 2024, in coordination with OSTP and other federal agencies, NSF released four interactive online research security training modules to be used by U.S. researchers and institutions.

In July 2024, OSTP issued guidance for federal agencies on implementing the research security program requirements established by NSPM-33 and the CHIPS and Science Act. The guidance established "as a standardized requirement" that federal agencies require covered institutions to certify that their research security programs include specific elements relating to "(1) cybersecurity; (2) foreign travel security; (3) research security training; and (4) export control training, as appropriate." In addition to defining *covered institution*, the guidance directs federal agencies to clearly communicate program requirements with covered institutions and ensure access to trainings, materials, and other resources needed to fulfill such requirements.

OSTP's July 2024 guidance also established related implementation deadlines. In implementing the new, standardized research security program requirements, OSTP requires each agency to submit a plan detailing how it will update its policies to reflect the new guidance and requirements by January 9, 2025. It also directs agencies to require covered institutions to implement research security programs no later than 18 months after the date that they submitted their plan to OSTP.

Information Sharing and Risk Assessment

To improve the ability of federal agencies to identify and respond to potential research security threats, Section 4(e) of NSPM-33 directed agencies to share information about individuals and institutions that violate disclosure policies. Similarly, as required by the CHIPS and Science Act, on July 24, 2024, NSF announced the establishment of the Safeguarding the Entire Community of the U.S. Research Ecosystem (SECURE) Center to "serve as a clearinghouse for information to empower the research community to identify and mitigate foreign interference that poses risks to the U.S. research enterprise."

Congress has also directed individual agencies to develop risk assessment tools and frameworks to manage and mitigate security risks. For example, the Consolidated Appropriations Act, 2023 (P.L. 117-328), required the Department of Health and Human Services to develop a set of strategies and frameworks to protect federally funded biomedical R&D from national security and other risks.

Potential Issues for Congress

As Congress oversees the implementation of current research security provisions and the potential development of new measures, the following topics could be considered:

- Should the disclosure information associated with covered individuals and research institutions be made publicly available and, if so, how?
- How frequently should post-award disclosure reporting occur? To what extent, if at all, should agencies harmonize such requirements?
- What mechanisms exist to ensure effective and consistent monitoring and enforcement of research security provisions?
- To what extent are research security roles and responsibilities clearly and appropriately allocated between federal agencies and research institutions?
- How sufficiently are research security efforts, including monitoring and enforcement activities, staffed and funded at federal agencies and research institutions?
- How, if at all, should risk assessments vary among federal agencies (e.g., defense or civilian), stage of research (e.g., basic or applied), or area of research (e.g., critical or emerging technology)?
- To what extent, if at all, should agencies review current and pending support disclosures for security risks, in addition to conflicts of commitment?
- To what extent, if at all, should research security policies aim to equally address concerns about security and maintaining scientific collaboration?

Emily G. Blevins, Acting Section Research Manager
Marcy E. Gallo, Analyst in Science and Technology Policy

Disclaimer