Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

February 8, 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. Sources have documented a variety of mechanisms employed on behalf 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 to try to maintain the benefits of an open research ecosystem while attempting to protect it from external threats. For example, in 2019, Section 1746 of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2020 (P.L. 116-92) directed federal agencies to, among other things, develop descriptions of known and potential threats to federally funded research and development (R&D) and 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 Research and Development (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.

To help all federal agencies require applicants to disclose such information, the National Science Foundation (NSF) released two common forms in November 2023 expected to be included in all applications for federal research awards: the Biographical Sketch Common Form and the Current and Pending (Other) Support Common Form. OSTP must review any potential modifications to the common forms that agencies may wish to make.

P.L. 116-283 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 4(c)(ii) of NSPM-33 directed agency heads to establish or clarify existing policies that prohibit federal employee participants in the U.S. R&D enterprise from participating in foreign government-sponsored talent recruitment programs. It also indicated that agency heads may consider establishing agency-specific policies that would extend the prohibition to "some or all agency contractor personnel."

Congress, however, mandated more restrictive measures on foreign talent recruitment program participation. Section 10631 of P.L. 117-167, known as the CHIPS and Science Act, specified that agency guidelines should (a) require covered individuals to disclose if they are party to a foreign talent recruitment program contract, and (b) to the extent practicable, require federal R&D funding recipients to prohibit covered individuals participating in *malign* foreign talent recruitment programs from working on projects supported by federal R&D awards.

Section 10632 also 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.

## Research Security Training and Program Requirements

To build awareness and strengthen compliance with research security policies, NSPM-33 issued new requirements related to research security training.

Section 4(f) directed funding agencies to ensure that federal personnel involved in the conduct of R&D or allocation of R&D funding receive training to include "risks to the United States R&D enterprise, individuals' responsibilities related to research security and integrity, and circumstances and behaviors that may indicate risk to research security and integrity."

Section 4(g) directed agencies to require research institutions receiving more than $50 million in federal science and engineering support per year to certify that the institution has established and operates 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 handling."

In February 2023, OSTP released a "Draft Research Security Programs Standard Requirement" to facilitate implementation of Section 4(g) of NSPM-33 as well as research security training requirements mandated by Section 10634 of P.L. 117-167. The draft guidance provided additional details on covered organizations, foreign travel security, research security training, cybersecurity, and export control training. It also specified that federal agencies should communicate the required training components and standards to research organizations as part of their funding agreement processes.

In August 2023, the National Institute of Standards and Technology (NIST) released the *Safeguarding International Science: Research Security Framework*, through which NIST intended to establish

> a uniform Research Security implementation methodology designed to safeguard America's science and research community from undue foreign interference while safeguarding the benefits of international science, thus ensuring the integrity of the U.S. innovation ecosystem.

NIST's framework included a range of guidance for federal agencies, institutions of higher education, and other entities, in developing research security programs, acquiring research security personnel, and conducting research security risk analysis, among other elements.

On January 20, 2024, as directed by P.L. 117-167, NSF released four interactive online research security training modules to be used by U.S. researchers and institutions.

## 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, P.L. 117-167 directed NSF to establish an independent research security and integrity information-sharing analysis organization. The organization is to, among other duties, serve as a clearinghouse of information for the research community, provide timely reports on research security risks, and develop risk assessment best practices.

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?
- How frequently should post-award disclosure reporting occur and should agencies be required to harmonize such requirements?
- What mechanisms exist to ensure effective and consistent monitoring and enforcement of research security provisions?
- Are research security roles and responsibilities clearly and appropriately allocated between federal agencies and research institutions?
- Are research security efforts, including monitoring and enforcement activities, sufficiently staffed and funded?
- Should agencies be required to use disclosed information in performing security risk assessments?
- 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)?

**Emily G. Blevins**, Analyst in Science and Technology Policy

IF12589

**Marcy E. Gallo**, Analyst in Science and Technology Policy

## Disclaimer