



October 2026

RESEARCH SECURITY

NIH Action Needed to Strengthen Foreign Interference Risk Management



NIH Action Needed to Strengthen Foreign Interference Risk Management

GAO-27-107848

October 2026

A report to congressional requesters

For more information, contact: Candice N. Wright at WrightC@gao.gov

What GAO Found

The National Institutes of Health (NIH) funds extramural research through awards to universities and other institutions. Implementation of federal research security requirements helps safeguard this research from foreign interference, including misappropriation and unauthorized access by foreign countries and entities.

NIH implemented 14 of the 15 federal research security requirements GAO reviewed that address: (1) disclosure, (2) malign foreign talent recruitment programs, (3) research security training and programs, and (4) collaboration and information sharing. These requirements apply across federal research agencies and include actions NIH must take, as well as requirements it must impose on grant applicants, recipients, and specified individuals. For the remaining requirement concerning certification by certain recipient institutions that they have established and operate research security programs, NIH is working with an interagency group to implement the requirement.

NIH relies heavily on self-reported information disclosed by researchers and institutions to identify and manage foreign interference risks and generally does not verify such disclosures using sources outside those required during pre-award risk assessments unless it receives a foreign interference allegation. Additionally, NIH does not require disclosure of all past affiliations, and foreign component disclosures are only required when the collaboration involves the performance of a significant element or segment of the NIH-funded project outside of the United States. As a result, NIH may not identify risks when relevant information is not required to be disclosed or is left out.

From 2017 through 2025, NIH received 697 allegations of potential foreign interference involving personnel on NIH awards. NIH identified disclosure violations in 264 cases, and NIH or recipient institutions took one or more actions in most of those cases, such as prohibiting individuals from participating on awards.

NIH Allegations of Potential Foreign Interference and Outcomes, 2017–2025

Total number of allegations (697)	Violations found (264)	Action taken by NIH or recipient institution (223)
	No violations found (433)	No actions taken (41)
		Action taken by NIH or recipient institution (45)
		No actions taken (388)

Source: GAO analysis of National Institutes of Health data. | GAO-27-107848

In seven nongeneralizable case studies, GAO used outside sources to identify publicly available information about foreign affiliations and coauthored publications that did not appear in the award documentation. These cases do not establish the prevalence of undisclosed information or foreign interference across NIH awards but illustrate potential limitations of NIH's disclosure-based process.

NIH's risk management program is fully aligned with GAO's enterprise risk management practices but not fully aligned with GAO's Fraud Risk Framework. Although NIH's annual risk inventory considers fraud, it is not a documented extramural-program-specific assessment of fraud schemes, controls, and residual risks. Without such an assessment, NIH lacks a documented basis for determining whether its controls and monitoring activities address the most significant fraud risks and are adjusted as those risks evolve.

Why GAO Did This Study

The U.S. has long promoted an open and collaborative research environment, but policymakers have raised concerns that foreign countries and entities may exploit the openness of the federally funded research enterprise to undermine national security and economic competitiveness. In fiscal year 2025 alone, NIH awarded about \$35 billion in extramural funding.

GAO was asked to review NIH's efforts to safeguard extramural research from foreign interference and related ethical concerns. This report examines, among other things: (1) NIH's implementation of selected federal research security requirements, (2) the extent to which NIH identifies and manages foreign interference risks in its extramural research program, and (3) the alignment of NIH's risk management policies and practices with GAO risk management practices.

GAO reviewed relevant legal authorities, policies, and NIH documentation; analyzed NIH foreign interference allegation data from 2017 through 2025; conducted seven nongeneralizable case studies of NIH awards selected based on their potential for heightened foreign interference risk; compared NIH practices with GAO risk management frameworks; and interviewed NIH and Department of Health and Human Services officials.

What GAO Recommends

GAO recommends that NIH regularly conduct and document a fraud risk assessment tailored to NIH's extramural research program that considers foreign interference risks. NIH concurred with the recommendation.

Contents

Letter		1
	Background	4
	NIH Has Implemented Most Selected Research Security Requirements	10
	NIH Uses a Disclosure-Based Process to Identify Foreign Interference Risks, but the Process Has Potential Limitations	18
	NIH Aligns with GAO's Enterprise Risk Management Practices but Has Not Conducted a Fraud Risk Assessment Tailored to Its Extramural Research Program	36
	HHS's Office for Human Research Protections Has Limited Visibility Into International Institutions Involved in HHS-Supported Human Subjects Research	49
	Conclusions	51
	Recommendations for Executive Action	52
	Agency Comments	52
Appendix I	Objectives, Scope, and Methodology	54
Appendix II	Case Studies of NIH's Implementation of Foreign-Interference-Related Requirements and Identification of Risks	58
Appendix III	Alignment Between NIH's Risk Management Program and Selected GAO Fraud Risk Framework Overarching Concepts	65
Appendix IV	Comments from the Department of Health and Human Services	72
Appendix V	GAO Contact and Staff Acknowledgments	74
Tables		
	Table 1: NIH Implementation of Selected Federal Research Security Requirements, by Research Security Area	10
	Table 2: Outcomes of National Institutes of Health (NIH) Foreign Interference Allegations, 2017 through 2025	30

Table 3: NIH Risk Management Program’s Alignment with Leading Practices by GAO Fraud Risk Framework Overarching Concept	39
Table 4: National Institutes of Health (NIH) Risk Management Program Alignment with Leading Practices of Selected GAO Fraud Risk Framework Overarching Concepts	65

Figures

Figure 1: Federal Government Enterprise Risk Management Practices	8
Figure 2: The GAO Fraud Risk Framework	9
Figure 3: National Institutes of Health Pre-Award Review Process and Actions to Address Foreign Interference Risks	21
Figure 4: National Institutes of Health Award Process and Actions to Address Foreign Interference Risks	22
Figure 5: National Institutes of Health Post-Award Monitoring Process and Actions to Address Foreign Interference Risks	26
Figure 6: Number of Allegations of Potential Foreign Interference Received by the National Institutes of Health, 2017–2025	27
Figure 7: Sources of Allegations of Potential Foreign Interference Received by the National Institutes of Health, 2017–2025	28

Abbreviations

DOD	Department of Defense
DOD list	<i>Fiscal Year 2023 Lists Published in Response to Section 1286 of the National Defense Authorization Act for Fiscal Year 2019, as amended</i>
DOJ	Department of Justice
eRA	Electronic Research Administration
ERM	enterprise risk management
FACTS	Foreign Award and Component Tracking System
FBI	Federal Bureau of Investigation
HHS	Department of Health and Human Services
IRB	institutional review board
NDAA	National Defense Authorization Act
NIH	National Institutes of Health
NNSFC	National Natural Science Foundation of China
NSPM-33	National Security Presidential Memorandum-33
OER	Office of Extramural Research
OER-RI	Office of Extramural Research-Research Integrity
OHRP	Office for Human Research Protections
OIG	Office of Inspector General
OMA	Office of Management Assessment
ONS	Office of National Security
OPERA	Office of Policy for Extramural Research Administration
OSTP	Office of Science and Technology Policy
PI	principal investigator
R&D	research and development
SAM.gov	System for Award Management

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



October 5, 2026

The Honorable Brett Guthrie
Chairman
Committee on Energy and Commerce
House of Representatives

The Honorable H. Morgan Griffith
Chairman
Subcommittee on Health
Committee on Energy and Commerce
House of Representatives

The Honorable John Joyce, M.D.
Chairman
Subcommittee on Oversight and Investigations
Committee on Energy and Commerce
House of Representatives

The Honorable Earl L. "Buddy" Carter
House of Representatives

The Honorable Gary Palmer
House of Representatives

The United States has long promoted an open and collaborative research environment. In recent years, however, policymakers have raised concerns that foreign countries and entities may exploit this openness to gain access to federally funded research in ways that could undermine U.S. national security and economic competitiveness. Such foreign interference may include efforts to misappropriate or gain unauthorized access to federally funded research, including through undisclosed affiliations, sources of financial support, or participation in foreign talent recruitment programs.

In response to these concerns, Congress and the executive branch have established a federal research security framework through legal authorities including (1) provisions in the William M. Thornberry National Defense Authorization Act for Fiscal Year 2021 (FY 2021 NDAA), (2) National Security Presidential Memorandum-33 (NSPM-33), and (3) provisions in the Research and Development, Competition, and Innovation Act, contained in what is commonly referred to as the CHIPS

and Science Act.¹ These authorities require federal research agencies² to strengthen disclosure requirements for applicants and recipients of federal research awards, prohibit covered individuals³ from participating in malign foreign talent recruitment programs,⁴ enhance information sharing, and generally authorize consequences for violations of these requirements. These authorities rely heavily on the use of self-reported information disclosed by researchers and institutions to identify risks related to foreign interference.

The National Institutes of Health (NIH), within the Department of Health and Human Services (HHS), is the world's largest public funder of biomedical research. Most of this funding supports extramural research conducted at universities, hospitals, and other institutions.⁵ Given NIH's scale, its implementation of federal research security requirements is

¹William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, § 223, 134 Stat. 3388, 3470-72; The White House, *Presidential Memorandum on United States Government Supported Research and Development National Security Policy*, National Security Presidential Memorandum 33 (NSPM-33) (Jan. 14, 2021); and Research and Development, Competition, and Innovation Act, Pub. L. No. 117-167, §§ 10631, 10632, 10634, 136 Stat. 1399, 1664–66, 1667-68 (2022).

²Under Section 223 of the FY 2021 NDAA and NSPM-33, a “federal research agency” is a federal department or agency with an annual extramural research expenditure of over \$100 million. See Pub. L. No. 116-283, § 223(d)(4), 134 Stat. 3471-72, National Science and Technology Council, *Guidance for Implementing National Security Presidential Memorandum 33 (NSPM-33) on National Security Strategy for United States Government-Supported Research and Development* (January 2022). Under the CHIPS and Science Act, a “federal research agency” is “any agency with an annual extramural research expenditure over \$100 million in fiscal year 2022 constant dollars.” Pub. L. No. 117-167, § 10002(10), 136 Stat. 1399, 1406.

³Under the CHIPS and Science Act, a “covered individual” is “an individual who 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 is designated as a covered individual by the federal research agency concerned.” Pub. L. No. 117-167, § 10638(1), 136 Stat. 1399, 1669-70 (2022). This is the same definition for “covered individual” as found in section 223 of the FY 2021 NDAA.

⁴A “malign foreign talent recruitment program” is broadly described as a program, position, or activity that includes compensation (cash or in-kind) provided by a foreign country or affiliated entity to an individual in exchange for actions such as unauthorized transfer of intellectual property or nonpublic information from the United States to a foreign country, establishing labs or employment abroad in violation of federal award terms, or conducting work that substantially overlaps or duplicates federally funded research. For the full definition of “malign foreign talent recruitment program” see Pub. L. No. 117-167, § 10638(4), 136 Stat. 1399, 1670 (2022).

⁵Extramural research is research conducted by any institution or entity other than the federal agency to which supporting funds were appropriated.

important to safeguarding the integrity of the federally funded research enterprise.

You asked us to examine NIH's efforts to safeguard extramural research from national security and ethical concerns arising from relationships between researchers funded through NIH awards and entities in foreign countries. This report examines (1) NIH's implementation of selected federal research security requirements, (2) the extent to which NIH identifies and manages foreign interference risks for its extramural research program, (3) the extent to which NIH's risk management policies and practices align with GAO's enterprise risk management and Fraud Risk Framework practices, and (4) HHS's oversight of human subjects research conducted outside the United States.

To evaluate NIH's implementation of selected federal research security requirements, we reviewed relevant legal authorities and NIH documentation, including NIH policy manuals, grants guidance, guide notices, and internal guidance for staff, and we compared NIH's efforts with selected requirements from the FY 2021 NDAA, NSPM-33, and the CHIPS and Science Act. To examine the extent to which NIH identifies and manages foreign interference risks for its extramural research program, we conducted seven nongeneralizable case studies of NIH awards. We selected five awards from research articles published between January 2024 and May 2025 that acknowledged NIH funding and included coauthors affiliated with institutions the Department of Defense has identified as engaging in activity that may pose heightened foreign interference risk.⁶ We supplemented these with two NIH-identified awards for which NIH had imposed mitigations in response to foreign interference concerns. We selected these cases to examine how NIH's processes operated in circumstances that may present heightened foreign interference risk, not to estimate the prevalence of such risks across NIH awards. We also analyzed NIH Office of Extramural Research (OER) data on allegations of potential foreign interference from 2017 through 2025.

To determine the extent to which NIH's risk management policies and practices align with selected GAO enterprise risk management (ERM) and Fraud Risk Framework practices, we compared NIH's risk management documentation and practices with all six GAO ERM

⁶Department of Defense, *Lists Published in Response to Section 1286 of the National Defense Authorization Act for Fiscal Year 2019 (Public Law 115-232), as amended*.

practices and with leading practices for the nine GAO Fraud Risk Framework overarching concepts we determined most relevant to our review. For this comparison, we reviewed documentation describing NIH's risk management program, including NIH's Policy Manual and NIH's Enterprise Risk Management Guidebook.⁷ We also reviewed supporting documentation, interviewed NIH officials, and analyzed responses to our written questions. To describe HHS's oversight of foreign human subjects research, we reviewed relevant laws and regulations governing human subjects protections and reviewed documents and interviewed officials from the HHS Office for Human Research Protections. Appendix I provides further information about our objectives, scope, and methodology.

We conducted this performance audit from September 2024 to September 2026 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

NIH is the largest public funder of biomedical research in the world. In fiscal year 2025, NIH awarded about \$35.3 billion in extramural funding, representing about 73 percent of its total funding. NIH awards this funding through its institutes and centers, such as the National Cancer Institute and the National Institute of Allergy and Infectious Diseases, each of which has a specific research focus. NIH's extramural awards support research conducted at universities, hospitals, and other institutions. Much of this research is fundamental scientific work intended to expand knowledge and be broadly disseminated. To identify and manage risks associated with this open research environment, including foreign interference risks, NIH relies primarily on disclosure requirements and institutional oversight.

NIH has reported that many instances of foreign interference involve undisclosed conflicts of interest or commitment associated with foreign institutions. NSPM-33 broadly defines conflicts of interest as financial interests or financial relationships of an individual or the individual's

⁷National Institutes of Health, *NIH Policy Manual*, 1750 - NIH Risk Management Program (Oct. 23, 2023; technical rev. Apr. 22, 2026), <https://policymanual.nih.gov/1750>; National Institutes of Health, *NIH Risk Management Program Guidebook for ICs and OD Offices* (Oct. 2023).

spouse or dependent children that could significantly affect the design, conduct, reporting, or funding of research, and conflicts of commitment as conflicting obligations between or among multiple employers or other entities, including competing commitments of time or obligations to improperly share or withhold information from an employer or funding agency.⁸ Such conflicts may involve overlapping research activities, competing professional commitments, or relationships with foreign institutions. NIH permits foreign collaborations, awards, and employment that are unrelated to work funded through an NIH award and do not present concerns about scientific, budgetary, or commitment overlap, financial conflict of interest, or undisclosed foreign components.

Specified individuals may not participate in malign foreign talent recruitment programs and must disclose all domestic and foreign research activities, including relevant foreign agreements and contracts, among other things, to NIH.⁹ Failure to disclose required information may prevent NIH from identifying conflicts of interest or commitment and violates federal requirements and NIH grant policy. In some circumstances, nondisclosure may also be investigated as potential grant fraud. Undisclosed or unmanaged conflicts may deprive NIH of information needed to make award and oversight decisions and, when they involve foreign entities, may increase the risk that federally funded research or related knowledge is inappropriately transferred outside the United States. GAO reported in January 2026 that improper foreign influence cases led to some researchers losing their funding, experiencing other administrative outcomes, or receiving criminal convictions, underscoring the importance of identifying such risks to prevent fraud, waste, and abuse of taxpayer-funded research.¹⁰

Research Security Requirements

NIH implements multiple federal research security requirements, including those established through the FY 2021 NDAA, NSPM-33, and the CHIPS and Science Act. The following authorities establish requirements

⁸See *NSPM-33*, § 2(c)-(d) for the full definitions of conflict of interest and conflict of commitment.

⁹For the purposes of this report, a specified individual is a “covered individual” as defined by the FY 2021 NDAA and the CHIPS and Science Act, or a principal investigator or senior or key personnel pursuant to NSPM-33.

¹⁰GAO, *Research Security Agencies Should Assess Safeguards Against Discrimination*, [GAO-26-107544](#) (Washington, D.C.: Jan. 21, 2026).

intended to reduce the risk that foreign actors could gain improper access to federally funded research:

- **FY 2021 NDAA:** Section 223 of the FY 2021 NDAA directs federal research agencies to require that covered individuals listed on applications for research and development awards disclose all sources of current and pending research support; certify that such disclosures are current, accurate, and complete; and agree to update those disclosures prior to and during the life of an award. It also directs federal agencies to require applicants to certify that covered individuals employed by the applicant and listed on the application are made aware of disclosure requirements, and authorizes agencies to take actions such as rejecting applications, or suspending or terminating awards, in response to violations.
- **NSPM-33:** Among other things, NSPM-33 and implementing guidance include provisions that direct federal research agencies to standardize disclosure processes to the extent practicable. They also direct agencies to require principal investigators and other senior and key personnel seeking or receiving federal extramural funding to disclose (1) their organizational affiliations and employment; (2) other support; (3) current or pending participation in, or applications to, programs sponsored by foreign governments, instrumentalities, or entities, including foreign government-sponsored talent recruitment programs; and (4) positions and appointments, both domestic and foreign, including affiliations with foreign entities or governments.¹¹ NSPM-33 and implementing guidance also direct federal research agencies to require certain institutions receiving federal research funding to certify that they have established and operate a research security program;¹² identify disclosures that have the potential to negatively impact research funding, security, or integrity; and share information about

¹¹For researchers, “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 institution, 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 includes resource and 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. NSPM-33 § 4(b)(ii)(2).

¹²Implementation guidance issued by OSTP includes guidance for determining which institutions are considered covered institutions and are required to certify that they have a research security program. See the Office of Science and Technology Policy, *Guidelines for Research Security Programs at Covered Institutions* (July 9, 2024) for the full definition of a “covered institution.”

individuals who violate policies implementing NSPM-33 or whose activities clearly demonstrate an intent to threaten research security and integrity with specified agencies, consistent with applicable law and other restrictions. These agencies include federal law enforcement agencies, the Department of Homeland Security, and the Department of State.

- **CHIPS and Science Act:** The CHIPS and Science Act and implementing guidance include requirements for covered individuals to disclose participation in foreign talent recruitment programs, prohibit participation in malign foreign talent recruitment programs by covered individuals, require covered individuals to certify that they are not a party to a malign foreign talent recruitment program, and direct federal research agencies to require research security training for covered individuals and related certification, among other things.¹³

Enterprise Risk Management Practices

Managing risks related to foreign interference requires NIH to identify potential risk indicators, such as undisclosed affiliations, and design controls to mitigate those risks. GAO's risk management frameworks provide criteria for assessing these efforts. GAO's enterprise risk management (ERM) practices help agencies identify, assess, and respond to risks that could affect mission achievement, while GAO's Fraud Risk Framework provides more detailed guidance for identifying, assessing, and mitigating fraud risks in specific programs, such as nondisclosure in extramural research programs.¹⁴ Although ERM and fraud risk management are related, they serve different purposes and require distinct processes. An agency may have an effective ERM program while still having gaps in its fraud risk management approach.

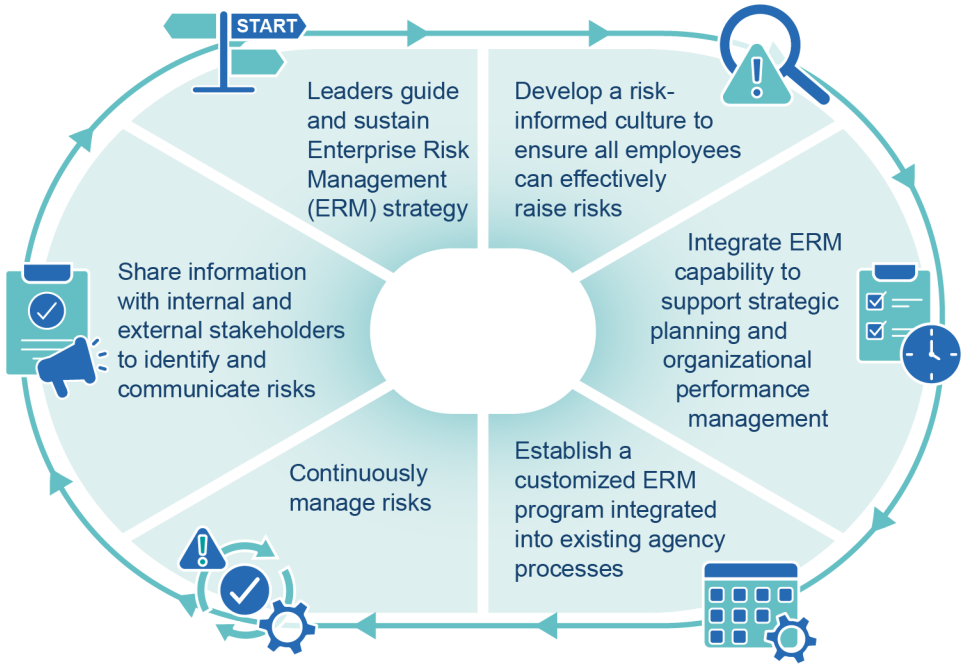
GAO has identified six essential practices that support effective ERM in federal agencies, including leadership commitment, a risk-informed culture, integration with strategic planning, and continuous monitoring of

¹³Section 10631 of the CHIPS and Science Act directs OSTP, in coordination with others, to issue guidelines for federal research agencies regarding foreign talent recruitment programs, to include requiring covered individuals to disclose participation in a foreign talent recruitment program. It further directs federal research agencies to issue a policy using these guidelines. Pub. L. No. 117-167, 10631, 136 Stat. 1399, 1664-65 (2022); Office of Science and Technology Policy, *Guidelines for Federal Research Agencies Regarding Foreign Talent Recruitment Programs* (Feb. 14, 2024).

¹⁴GAO, *Enterprise Risk Management: Selected Agencies' Experiences Illustrate Good Practices in Managing Risk*, [GAO-17-63](#) (Washington, D.C.: Dec. 1, 2016). GAO, *A Framework for Managing Fraud Risks in Federal Programs*, [GAO-15-593SP](#) (Washington, D.C.: July 28, 2015).

risks (see fig. 1). NIH identified foreign interference as a risk in its February 2024 Enterprise Risk Management Profile.

Figure 1: Federal Government Enterprise Risk Management Practices



Source: GAO (data); Hazha/stock.adobe.com (icons). | GAO-27-107848

GAO's Fraud Risk Framework identifies leading practices for managing fraud risks in federal programs and provides guidance for strategically mitigating the likelihood and impact of fraud. The framework consists of four components, each containing two to four overarching concepts (see fig. 2). Each overarching concept includes multiple leading practices. Agencies can use these practices to assess program fraud risks, such as intentional nondisclosure in grant programs, and to design controls to help ensure program integrity.

Figure 2: The GAO Fraud Risk Framework



Source: GAO. | GAO-27-107848

NIH Has Implemented Most Selected Research Security Requirements

In our review of NIH's policies and procedures, we found that NIH has implemented 14 of the 15 selected federal research security requirements established by the FY 2021 NDAA, NSPM-33, and the CHIPS and Science Act. The selected requirements are grouped into four research security areas: (1) disclosure, (2) malign foreign talent recruitment programs, (3) research security training and programs, and (4) collaboration and information sharing. These requirements apply across federal research agencies and include actions NIH must take, as well as requirements it must impose on grant applicants, recipients, and specified individuals. For the remaining requirement, concerning certification that certain recipient institutions have established and operate research security programs, NIH has not fully implemented the requirement but is working with an interagency group to do so. Table 1 summarizes NIH's implementation status for the selected requirements in each research security area.

Table 1: NIH Implementation of Selected Federal Research Security Requirements, by Research Security Area

Research security area	Implementation
Disclosure	
Require specified individuals on grant applications to disclose and update disclosure of certain information to help identify potential conflicts of interest and commitment ^{a,b}	●
Require covered individuals on grant applications to certify that disclosures of specified information are current, accurate, and complete, and require applicants to certify that covered individuals listed on the application and employed by the applicant institution are made aware of disclosure requirements ^a	●
Identify disclosures that have the potential to negatively impact research funding, security, and integrity, in cooperation with inspectors general and law enforcement as appropriate ^b	●
Ensure the availability of consequences for violations of disclosure policies and engagement in activities that threaten the security and integrity of federally funded research ^b	●
Implement standardized disclosure processes, definitions, and forms across agencies to the extent practicable ^b	●
Require specified individuals to disclose participation in foreign talent recruitment programs ^{a,b,c}	●
Malign foreign talent recruitment programs	
Prohibit awards from being made for proposals in which covered individuals are participating in a malign foreign talent recruitment program ^c	●
Require covered individuals to certify they are not party to a malign foreign talent recruitment program and require institutions to certify that covered individuals have been made aware of the requirement ^c	●

Research security training and programs	
Require covered individuals to certify they have completed research security training and require applicant institutions to certify that covered individuals employed by the institution and listed on the application have completed the training ^c	●
Ensure that recipient institutions provide training on the risks of malign foreign talent recruitment programs to covered individuals ^c	●
Require institutions receiving federal science and engineering support exceeding \$50 million per year to certify that they have a research security program ^{b,d}	○
Collaboration and information sharing	
Cooperate with recipient institutions to ensure they have established and administer policies and processes to identify and manage risks to research security and integrity, including potential conflicts of interest and commitment ^b	●
Cooperate with agency inspectors general and law enforcement, as appropriate, in investigation of suspected instances of failure to comply with disclosure requirements ^b	●
Work with inspectors general, law enforcement, university program offices, and the private sector, as appropriate, to strengthen mechanisms and capabilities to identify and investigate potential violations of disclosure requirements ^b	●
Share information regarding violators of specified research security requirements with other federal research agencies, law enforcement, the Department of Homeland Security, and the Department of State ^b	●

● Implemented: NIH has implemented the federal research security requirement.

○ Not implemented: NIH has not implemented the federal research security requirement. Requirements were considered not implemented if they were in progress but not fully implemented.

Source: GAO analysis of federal research security requirements and National Institutes of Health information. | GAO-27-107848

Notes: The federal research security requirements in this table apply to all federal research agencies with an annual extramural research expenditure of over \$100 million.

This table uses the term “specified individuals” to include both “covered individuals” as defined in the FY 2021 NDAA and CHIPS and Science Act and principal investigators and other senior and key personnel pursuant to NSPM-33. The full definition of a covered individual can be found in section 223 of the FY 2021 NDAA and section 10638 of the CHIPS and Science Act. Pub. L. No. 116-283, § 223, 134 Stat. 3388, 3470-72, Pub. L. No. 117-167, § 10638(1), 136 Stat. 1399, 1669-70 (2022).

^aSection 223 of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (FY 2021 NDAA) and

^bNational Security Presidential Memorandum-33 (NSPM-33) and implementing guidance

^cResearch and Development, Competition, and Innovation Act (CHIPS and Science Act) and implementing guidance

^dNSPM-33 implementation guidance for research security programs defines a “covered institution”—an institution required to certify that it has established and operates a research security program—as an institution of higher education, a federally funded research and development center, or a nonprofit research institution that receives in excess of \$50 million per year, in fiscal year 2022 constant dollars under either the 3-year average of federal research and development obligations as reported in the most recent version of the Survey of Federal Science and Engineering Support to Universities, Colleges and Nonprofit Institutions, or the 3-year average of federal R&D obligations to federally funded research and development centers as provided in the most recent versions of the Survey of Federal Funds for Research and Development. Office of Science and Technology Policy, Guidelines for Research Security Programs at Covered Institutions (July 9, 2024).

Disclosure. Federal requirements establish disclosure and certification requirements. In addition, NSPM-33 directs research agencies to standardize disclosure processes, definitions and forms across research agencies, to the extent practicable. The information collected through required disclosures is used to identify potential conflicts of interest and commitment. NIH's Grants Policy Statement requires specified individuals to disclose required information including affiliations, research support, and participation in foreign talent recruitment programs and to update this information throughout the life of the award.¹⁵

NIH requires covered individuals to certify, at the time of application, that disclosures of current and pending (other) support are current, accurate, and complete.¹⁶ According to NIH officials, applicants must also certify that covered individuals have been made aware of the disclosure and certification requirements.¹⁷ According to NIH documentation and officials, disclosed information helps NIH identify potential conflicts of interest and commitment and make informed award decisions during application review and award monitoring. NIH officials told us they have worked, as appropriate, with HHS's Office of Inspector General (OIG), law enforcement, and recipient institutions to investigate potential violations of disclosure requirements. NIH's Grants Policy Statement also identifies potential consequences for violations, including disallowing costs, withholding payments, and suspending grants.¹⁸

NIH has also implemented the NSPM-33 requirement to standardize disclosure processes and forms across federal research agencies. In December 2025, NIH announced that it would require use of common forms for biographical sketches and current and pending (other) support

¹⁵NIH also requires updates to required disclosures as part of annual progress reports. National Institutes of Health, Grants Policy Statement, 8.4.1.9 at p. IIA-156 (Mar. 2026).

¹⁶NIH, Grants Policy Statement, 2.5.1 at p. I-82, 8.4.1.9 at p. IIA-156 (Mar. 2026).

¹⁷NIH, Grants Policy Statement, 8.4.1.11 at p. IIA-156 (Mar. 2026). While not a separate certification, NIH requires applicants to certify that covered individuals have completed research security training, which includes training on disclosures.

¹⁸NIH, Grants Policy Statement 8.4.1.9 at p. IIA-56 (Mar. 2026). The FY 2021 NDAA authorizes NIH to reject grant applications if information disclosed violates federal law or agency terms and conditions. It also authorizes NIH to take action, such as rejecting an application or suspending or terminating an ongoing award, should covered individuals knowingly fail to disclose information. Similarly, NSPM-33 allows for appropriate and effective consequences for violations of disclosure requirements.

in January 2026.¹⁹ These forms are harmonized disclosure forms for use by federal research agencies to collect required information.²⁰ After extending its initial implementation period, NIH began requiring use of the common forms in May 2026.²¹

The CHIPS and Science Act also mandates that federal research agencies issue a policy requiring covered individuals to disclose if they are participating in foreign talent recruitment programs.²² NIH has established requirements for covered individuals to disclose, in grant applications and in annual progress reports, current or pending participation in programs sponsored by foreign governments or entities, including foreign government-sponsored talent recruitment programs.

Malign foreign talent recruitment program. The CHIPS and Science Act and its implementing guidance prohibit federal research agencies from making research and development awards for applications that include covered individuals participating in malign foreign talent recruitment programs and require related certifications. NIH has implemented these requirements. In December 2025, NIH announced that individuals participating in malign foreign talent recruitment programs would be ineligible to serve as senior or key personnel on NIH grants or

¹⁹National Institutes of Health, *NIH's Implementation of Common Forms for Biographical Sketch and Current and Pending (Other) Support for Due Dates on or after January 25, 2026*, NOT-OD-26-018 (Dec. 2, 2025).

²⁰In February 2024, OSTP issued NSPM-33 implementing guidance for federal research agencies to use harmonized common disclosure forms for the biographical sketch and current and pending (other) support portions of grant and cooperative agreement applications across federal research agencies. Executive Office of the President, Office of Science and Technology Policy, *Policy Regarding Use of Common Disclosure Forms for the "Biographical Sketch" and the "Current and Pending (Other) Support" Sections of Applications by Federal Research Funding Agencies*, Memorandum for the Heads of Federal Research Agencies (Feb. 14, 2024).

²¹National Institutes of Health, *Adjusted Timeline for NIH's Implementation of Common Forms*, NOT-OD-26-033 (Feb. 4, 2026).

²²Section 10631 of the CHIPS and Science Act directs OSTP, in cooperation with others, to issue a uniform set of guidelines for federal research agencies regarding foreign talent recruitment programs, to include requiring covered individuals to disclose participation in a foreign talent recruitment program. Federal research agencies are required to issue policies using these guidelines. Pub. L. No. 117-167, 10631, 136 Stat. 1399, 1664-65 (2022); Office of Science and Technology Policy, *Guidelines for Federal Research Agencies Regarding Foreign Talent Recruitment Programs* (Feb. 14, 2024). NSPM-33 also requires principal investigators and senior or key personnel to disclose participation in foreign talent recruitment programs.

cooperative agreements beginning in January 2026.²³ NIH also requires, as part of its implementation of common forms, individuals identified as senior and key personnel to certify, at the time of application and in annual progress reports, that they are not parties to malign foreign talent recruitment programs. Applicants must certify that senior and key personnel have been made aware of and have complied with this certification requirement. NIH officials told us that the prohibition becomes a term and condition of an award.

Research security training and program. The CHIPS and Science Act directs federal research agencies to require that covered individuals on applications for research and development awards certify they have completed research security training covering specified areas within one year of the application.²⁴ Applicant institutions are to certify that the covered individuals employed by the institution and listed on the application have completed the required research security training. Federal research agencies were to implement this requirement no later than 12 months after enactment, in August 2022. NIH's Grants Policy Statement states that each individual identified as senior or key personnel on an NIH grant application must certify that they have completed research security training within 12 months of the date of application submission. The Statement also establishes requirements for the recipient institution's authorized representative to certify, through signature on the application, that covered individuals employed by the institution and listed on the application have completed the research security training.²⁵ This requirement was communicated to the extramural community in NIH's December 2025 guide notice, and the notice included information on the types of training that could be used to satisfy research security training requirements.²⁶ The guide notice also referred to four online research security training modules provided in partnership with the U.S. National Science Foundation and other research agencies,²⁷ as well

²³National Institutes of Health, *NIH's Implementation of Common Forms for Biographical Sketch and Current and Pending (Other) Support for Due Dates on or after January 25, 2026*, NOT-OD-26-018 (Dec. 2, 2025).

²⁴Pub. L. No. 117-167, § 10634, 136 Stat. 1399, 1667-68 (2022).

²⁵NIH, Grants Policy Statement, 8.4.1.11 at p. IIA-156 (Mar. 2026).

²⁶National Institutes of Health, *Research Security Training Requirements for NIH*, NOT-OD-26-017 (Dec. 2, 2025). This notice also states that a covered individual for NIH is defined as senior or key personnel.

²⁷"Research Security Training," National Science Foundation, accessed Aug. 6, 2026, <https://www.nsf.gov/research-security/training>.

as a condensed research security training module that can be completed to become compliant with requirements.²⁸ NIH stated in its Grants Policy Statement and guide notice that it would begin collecting these certifications at the time of application submission beginning May 25, 2026.

Separately, the CHIPS and Science Act requires federal research agencies to ensure, as a condition of award, that recipient institutions provide covered individuals with training on the risks of malign foreign talent recruitment programs. NIH officials told us that the agency satisfies this requirement through the research security training requirements announced in its December 2025 guide notice. Although NIH-approved research security training modules address these risks, the guide notice permits institutions to use alternative training that covers specified topics—cybersecurity, international collaboration, foreign interference, proper use of funds, disclosure, conflicts of commitment, and conflicts of interest.²⁹ The guide notice does not expressly require such alternative training to address the risks of malign foreign talent recruitment programs. However, NIH added information to its Grants & Funding website in August 2026 clarifying that institution-provided research security training must address the risks of malign foreign talent recruitment programs.

NSPM-33 and implementing guidance also establish research security program certification requirements for federal research agencies, under which NIH is to require covered institutions to certify that they have established and operate a research security program.³⁰ NIH issued a guide notice in September 2025 establishing such requirements but later

²⁸“Consolidated Training Module,” National Science Foundation SECURE Center, accessed Aug. 6, 2026, <https://www.secure-center.org/training>.

²⁹The guide notice referred to four online research security training modules provided in partnership with the U.S. National Science Foundation and other research agencies, as well as the National Science Foundation’s SECURE Center Consolidated Training Module, which include training on the risks of malign foreign talent recruitment programs.

³⁰NSPM-33 implementation guidance for research security programs defines a “covered institution” as an institution of higher education, a federally funded research and development center, or a nonprofit research institution that receives in excess of \$50 million per year, in fiscal year 2022 constant dollars under either the 3-year average of federal research and development obligations as reported in the most recent version of the Survey of Federal Science and Engineering Support to Universities, Colleges and Nonprofit Institutions, or the 3-year average of federal R&D obligations to federally funded research and development centers as provided in the most recent versions of the Survey of Federal Funds for Research and Development. Office of Science and Technology Policy, *Guidelines for Research Security Programs at Covered Institutions* (July 9, 2024).

rescinded that guide notice and had not established a new implementation date as of our review.³¹ NIH officials told us that the National Science Foundation is expected to collect institutional certifications through a centralized process, but the relevant interagency agreement has not been finalized. NIH officials also told us they are working with the interagency group responsible for implementing this requirement and that implementation has been delayed while the interagency group works with the Office of Science and Technology Policy (OSTP) to establish the necessary agreements. Because NIH's implementation of the requirement depends on completion of an ongoing interagency process, we are not making a recommendation to NIH at this time.

Collaboration and information sharing. NSPM-33 requires federal research agencies to cooperate with recipient institutions to ensure they have policies and processes to identify and manage risks to research security and integrity, including conflicts of interest and commitment. As a resource to institutions, NIH has issued guide notices, a policy checklist, and other guidance containing information on requirements for applicants to disclose information, which can reveal potential conflicts of interest and commitment. For example, NIH's Grants Policy Statement describes Just-In-Time procedures that include disclosure requirements, and NIH has issued a guide notice stating that institutions must maintain internal controls for disclosure.³²

NSPM-33 also requires federal research agencies to cooperate, as appropriate, with inspectors general and law enforcement agencies in investigating suspected violations of disclosure requirements and to, as appropriate, work with these entities and others to strengthen their ability to identify and investigate such violations.

NIH has established referral and coordination processes to implement these requirements. Its Grants Policy Statement provides that potentially criminal disclosure violations will be referred to NIH's Office of Management Assessment (OMA) for consultation with the HHS OIG, the Department of Justice (DOJ), or other law enforcement agencies, as

³¹National Institutes of Health, *Implementation of NIH Research Security Policies*, NOT-OD-25-154 (Sept. 11, 2025). This guide notice was rescinded and replaced on September 29, 2025. National Institutes of Health, *Update: Recission Notice re: Implementation of NIH Research Security Policies*, NOT-OD-25-161 (Sept. 29, 2025).

³²NIH, *NIH's Implementation of Common Forms*, NOT-OD-26-018.

appropriate. NIH officials also told us that OER may refer suspected disclosure violations to HHS OIG, DOJ, or the Federal Bureau of Investigation (FBI) for investigation. They also said they meet monthly with the HHS OIG to discuss cases that may involve civil or criminal violations and to coordinate on matters in which HHS OIG, DOJ, or the FBI may have an interest. In addition, OER officials told us they collaborate with HHS's Office of National Security (ONS)—the department's primary liaison to the broader intelligence community—to discuss research security developments, trends, and foreign interference concerns, including through classified briefings on cases that may have a national security connection. An HHS OIG official told us that their Office of Investigations routinely receives referrals and information on potential violations of disclosure requirements from NIH, and they use that information strictly for law enforcement purposes as part of their broader grant fraud investigations. The official said they work closely with NIH on criminal and civil investigations involving failures to disclose required information, including foreign talent recruitment programs, foreign affiliations, and other support.

NSPM-33 separately requires federal research agencies to share information regarding violators of specified research security requirements with other federal research agencies, law enforcement agencies, the Department of Homeland Security, and the Department of State, as appropriate. NSPM-33 implementation guidance provides guidance to federal research agencies regarding when they should share information about disclosure violations, including when a covered individual has an undisclosed affiliation with a foreign research institution and also receives funding from other research agencies.³³ In addition to NIH sharing information on disclosure violations with law enforcement, as described above, NIH officials also told us that they will share information on disclosure violations with other agencies, such as in cases when a violator is also funded by another research agency. NIH also records suspension and debarment enforcement actions taken on violators of disclosure policies in the System for Award Management (SAM.gov), the information sharing mechanism for government-wide exclusions. Based on these activities, we determined that NIH has implemented the selected collaboration and information sharing requirements within NSPM-33.

³³Research agencies are to share this information consistent with due process, privacy considerations, and all other applicable laws. National Science and Technology Council, *Guidance for Implementing NSPM-33* (Jan. 2022).

As our analysis shows, NIH has implemented all but one of the selected federal requirements, but several of these requirements rely substantially on information disclosed by applicants, recipients, and covered individuals.

NIH Uses a Disclosure-Based Process to Identify Foreign Interference Risks, but the Process Has Potential Limitations

NIH's process for identifying and managing foreign interference risks is based largely on compliance with the disclosure requirements discussed above, and its assessment of foreign interference risk may be limited because it relies primarily on information that applicants and recipients disclose unless it receives allegations of foreign interference. NIH compliance reviews in response to such allegations identified violations of disclosure requirements, but NIH has not identified instances of confirmed foreign interference (i.e., instances where those violations resulted in confirmed theft, transfer, or misappropriation of research funded through NIH awards). In addition, in our seven nongeneralizable case studies, we identified foreign affiliations and coauthored publications that did not appear in the NIH grant applications we reviewed.

NIH Primarily Relies on Disclosure Compliance to Identify Potential Foreign Interference Risks

NIH's process for assessing foreign interference risks primarily relies on compliance with policies requiring disclosure of foreign activities and affiliations by individuals who are privy to information about federally funded biomedical research and can be targets of foreign entities seeking to exploit such access. This includes individuals who serve as peer reviewers of research proposals as well as specified individuals who participate in awarded research projects. NIH does not routinely assess foreign interference risks using indicators beyond required disclosures throughout the award life cycle.

Applications first undergo review by independent experts, known as peer reviewers, to determine their scientific merit. Peer reviewers have access to detailed information about proposed projects and therefore could expose research funded through NIH awards to foreign interference risks. NIH policy requires that these reviewers disclose all conflicts of interest and apparent conflicts of interest, including those involving foreign parties, and certify that they have not participated in reviews for which they have such conflicts.³⁴

NIH regulations also require applications to undergo pre-award risk assessments, in which NIH staff evaluate applicants' ability to

³⁴Reviewers with either conflicts or apparent conflicts of interest with an application may not participate as reviewers on that application unless a waiver is granted.

successfully meet the programmatic and administrative requirements associated with the award.³⁵ NIH implements the disclosure requirements discussed above, in part, by requiring all applications to include biographical sketches for all senior and key personnel describing their education and current professional affiliations. Under NIH policy, grant applications must also disclose whether the proposed research project will include any “foreign components,” which NIH defines as “the performance of any significant element or segment of a project outside the United States either by the recipient or by a researcher employed by a foreign organization, whether or not grant funds are expended.”³⁶ For applications that receive favorable peer reviews, applicants are required to disclose all sources of research support, including financial and in-kind support, for senior and key personnel on the award.

For applications that include disclosure of a foreign component, NIH guidance directs institute and center staff to enter information about the component in the Foreign Award and Component Tracking System (FACTS) within the NIH awards management system. For some awards, NIH uses FACTS to submit information about the foreign component to the Department of State.³⁷ Once State receives the information, it generally has 14 days to determine whether the foreign component poses a risk to U.S. foreign policy interests. If State identifies no risks, or does not respond, NIH may proceed with the award.³⁸

³⁵NIH requires pre-award risk assessments in accordance with 2 C.F.R. § 200.206. HHS adopted the Office of Management and Budget guidance found in 2 C.F.R. part 200 with additions in 2 C.F.R. part 300 and 2 C.F.R. part 376. 2 C.F.R. § 300.106.

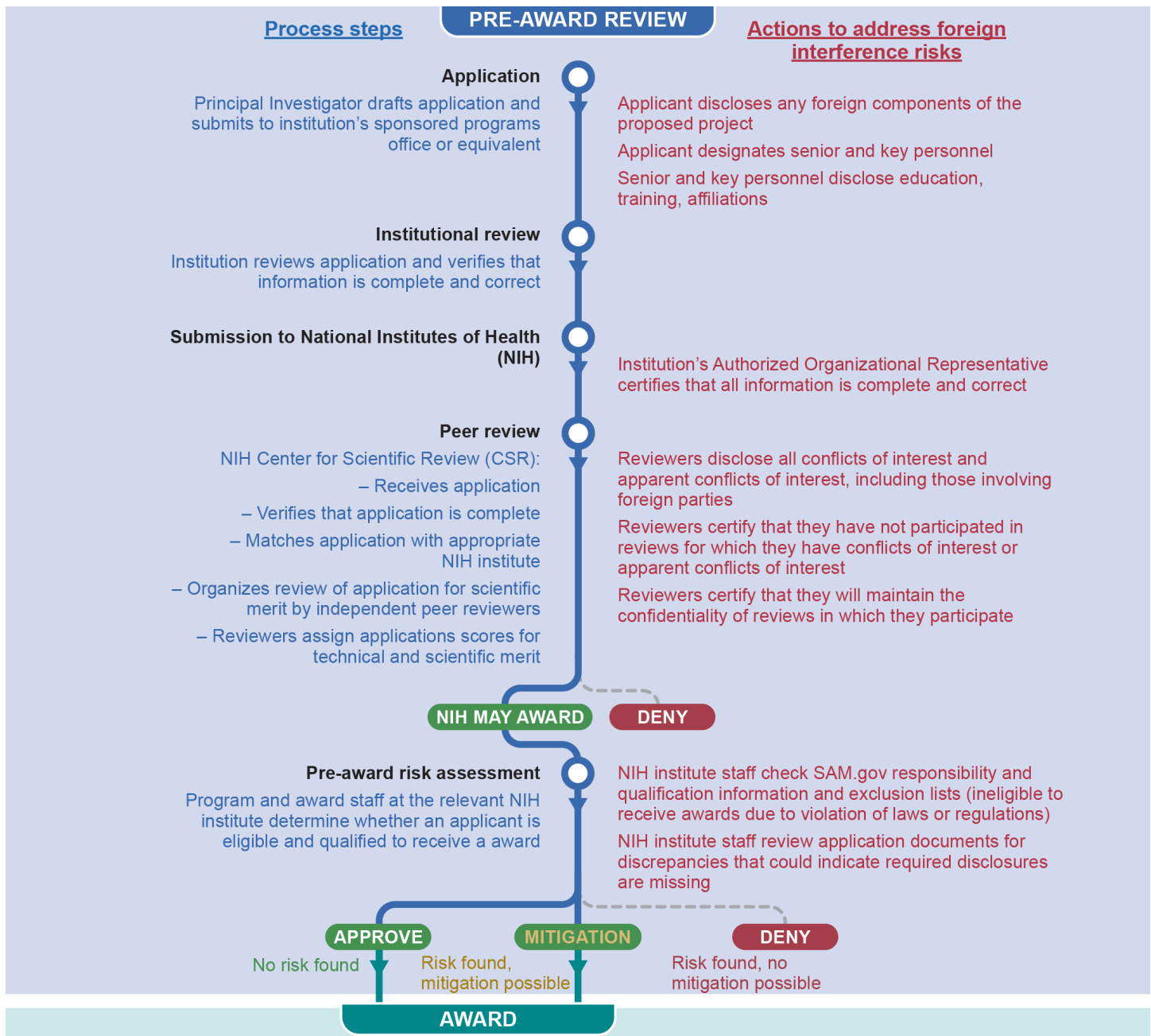
³⁶NIH, Grants Policy Statement, 1.2 at p. I-23 (Mar. 2026). Examples of activities that may be significant enough to be considered foreign components include the receipt of financial support from a foreign entity, the use of instrumentation or equipment at a foreign site, and collaboration with researchers at a foreign site that is expected to result in a coauthored publication.

³⁷Specifically, NIH uses FACTS to submit information about foreign components where human or animal subjects are involved; those that propose extensive foreign travel by recipient project staff for the purpose of data collection, surveying, sampling, and similar activities; those that include involvement in the affairs or environment of a foreign country and may have an impact on U.S. foreign policy; and those that include a substantial monetary commitment at the foreign site (>\$50,000; what is considered “substantial” is determined by NIH program or grants management staff).

³⁸Components in India, Brazil, and China do not default to “approved” status in the Foreign Award and Component Tracking System after 14 days but require review by the applicable foreign government and/or the appropriate U.S. official.

NIH officials told us that, during pre-award risk assessments, staff examine disclosures to determine whether they indicate potential foreign conflicts of interest or commitment. Officials also said that staff look for discrepancies between foreign disclosures and other parts of the application, such as research plans and letters of support, which provide additional details about how, where, and by whom the proposed project will be conducted. According to these officials, such discrepancies could indicate undisclosed foreign components or undisclosed foreign conflicts of interest or commitment. For example, officials at one NIH institute told us they may question whether disclosures are incomplete if a support letter originated from a foreign institution and no foreign affiliations or activities are mentioned elsewhere in the application. Figure 3 shows NIH's pre-award review process steps and actions to address foreign interference risks, which rely largely on disclosures by institutions and award personnel.

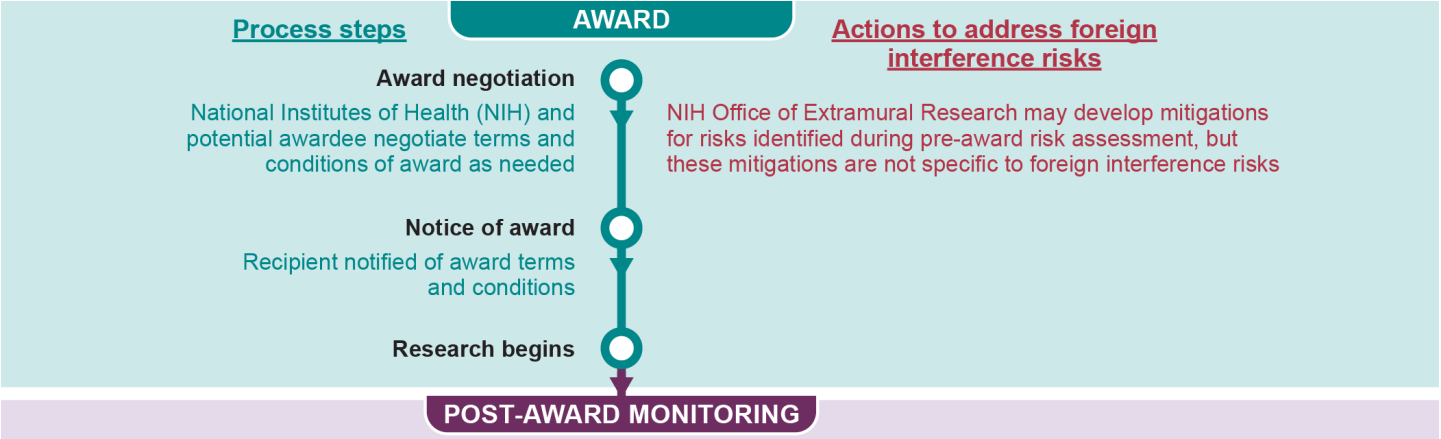
Figure 3: National Institutes of Health Pre-Award Review Process and Actions to Address Foreign Interference Risks



Source: GAO analysis of National Institutes of Health information. | GAO-27-107848

If NIH identifies potential risks before making an award, it may take steps during award negotiations to mitigate those risks, such as imposing award-specific terms and conditions. NIH officials told us they review application documents for indications of missing disclosures that could signal foreign interference, but they also said that conditions imposed during award negotiations are not specific to foreign interference risk. They further told us that NIH does not keep data on how many possible foreign risk indicators staff identify before making awards or on how many new awards have conditions imposed to mitigate foreign interference risk. NIH officials told us that the reason they do not track this information is that risk indicators identified in reviewing applications are not specific to foreign interference. Instead, they concern potential integrity violations such as duplicative funding or overcommitment of research time, which would be treated identically, whether or not foreign parties were involved. Figure 4 shows NIH’s award negotiation process steps and actions to address foreign interference risks.

Figure 4: National Institutes of Health Award Process and Actions to Address Foreign Interference Risks



Source: GAO analysis of National Institutes of Health information. | GAO-27-107848

NIH staff continue to monitor foreign interference risks after awards are made. NIH policy requires award recipients, as part of their progress reports for ongoing projects, to include any new foreign components on an award, and to update disclosures of foreign activities and affiliations

for personnel.³⁹ As with applications, NIH staff told us they also look for discrepancies in annual progress reports that could indicate undisclosed foreign activities and affiliations. For example, they said that if a progress report mentions a foreign research site that was not mentioned in previous documents, they may question whether the recipient failed to disclose a foreign component.

NIH staff told us they use a checklist to guide their review of those progress reports, including whether any changes, such as the addition of a foreign component, require evaluation through information available in the awards management system. Officials provided us with a sample checklist and a completed example demonstrating that their routine reviews include verifying that information on any new foreign components has been entered into the FACTS system. The checklist also includes determining whether there is new evidence of conflicts of interest or commitment, which could indicate foreign interference risk.

NIH officials told us that during the award monitoring process they rely on recipients to certify that disclosed information in progress reports is accurate and complete. They said NIH does not routinely verify disclosures using sources outside those required during pre-award risk assessments, such as online databases of scientific publications that may show researchers' affiliations and collaborations, unless it receives a foreign interference allegation. NIH officials told us they do not routinely verify disclosures using outside sources because institutions are responsible for ensuring that documents are complete and accurate.

NIH officials said that if institute staff identify information suggesting that an applicant failed to disclose foreign affiliations or activities, they generally contact the applicant or recipient institution for an explanation. If the applicant or recipient institution cannot provide a valid explanation, such as accidental omission, staff refer the matter to NIH's OER. The officials told us that OER then determines whether the concern is credible enough to open a compliance review (also referred to as a "compliance case").

NIH has developed a decision matrix for assessing potential foreign interference for covered individuals, whom NIH refers to as senior or key

³⁹The NIH Grants Policy Statement requires prior approval for the addition of a non-monetary foreign component to a grant to a domestic or foreign organization. NIH will not accept or approve requests to add a foreign subaward to an ongoing project. NIH, Grants Policy Statement, 8.1.2.10 at p.IIA-122 (Mar. 2026).

personnel.⁴⁰ This matrix outlines three main indicators of potential foreign interference risk: (1) undisclosed participation in a foreign talent recruitment program, (2) undisclosed foreign funding, and (3) undisclosed affiliation with a foreign institution. In compliance cases, OER officials told us, they work with staff at recipient institutions and use tools such as online databases to search for information indicating that senior or key personnel may have undisclosed foreign funding or affiliations or may participate in a malign foreign talent recruitment program.

To mitigate risk while compliance reviews are ongoing, OER officials told us, they may impose conditions on awards associated with personnel involved in those cases. Such conditions may include requiring the recipient institution to withhold salary funded through an NIH award from the individuals involved. Recipient institutions may also impose mitigations such as prohibiting individuals involved in compliance reviews from participating in research funded through an NIH award at the institution. Officials also said they may place a “bar” in NIH’s awards management system on individuals involved in compliance cases. This bar alerts institute and center staff to contact OER before making additional awards on which those individuals are listed as senior or key personnel.

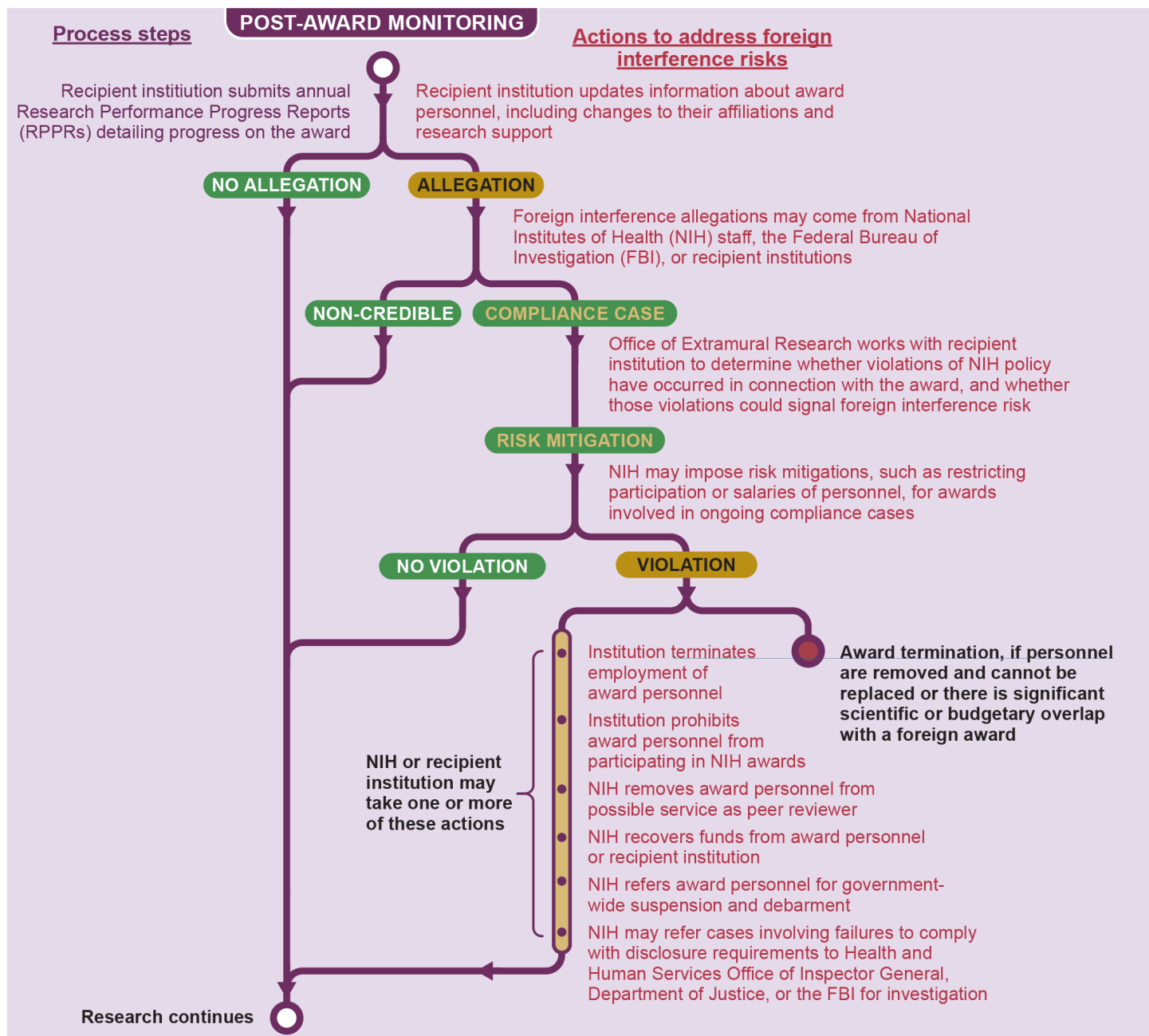
Compliance Reviews May Identify Disclosure Violations but Provide Limited Insight into the Extent of Foreign Interference

An allegation or compliance review involving potential foreign interference does not establish that foreign interference occurred. Such reviews may identify disclosure or other policy violations without establishing intentional concealment, fraud, or misappropriation of research. NIH officials told us that missing disclosures may result from oversight or a lack of understanding of disclosure requirements by award recipients and personnel, rather than intentional concealment. The officials also said that in cases where they have strong reasons to believe foreign interference is occurring, they also typically see failures to disclose foreign activities or affiliations. NIH officials further told us that criminal diversion of research, such as intellectual property theft, can be difficult to establish. In the open and collaborative research environment the United States fosters, researchers may generally share information that is not protected by intellectual property restrictions or confidentiality agreements. As a result, NIH primarily addresses foreign interference risk by responding to disclosure and other policy violations. It generally responds to those violations through administrative actions, such as removing personnel

⁴⁰National Institutes of Health, *Decision Matrix for Assessing Potential Foreign Interference for Covered Individuals or Senior/Key Personnel*. (Bethesda, MD, 2025).

from possible service as peer reviewers rather than through civil or criminal prosecution. Figure 5 shows NIH's post-award monitoring process steps and actions to address foreign interference risks.

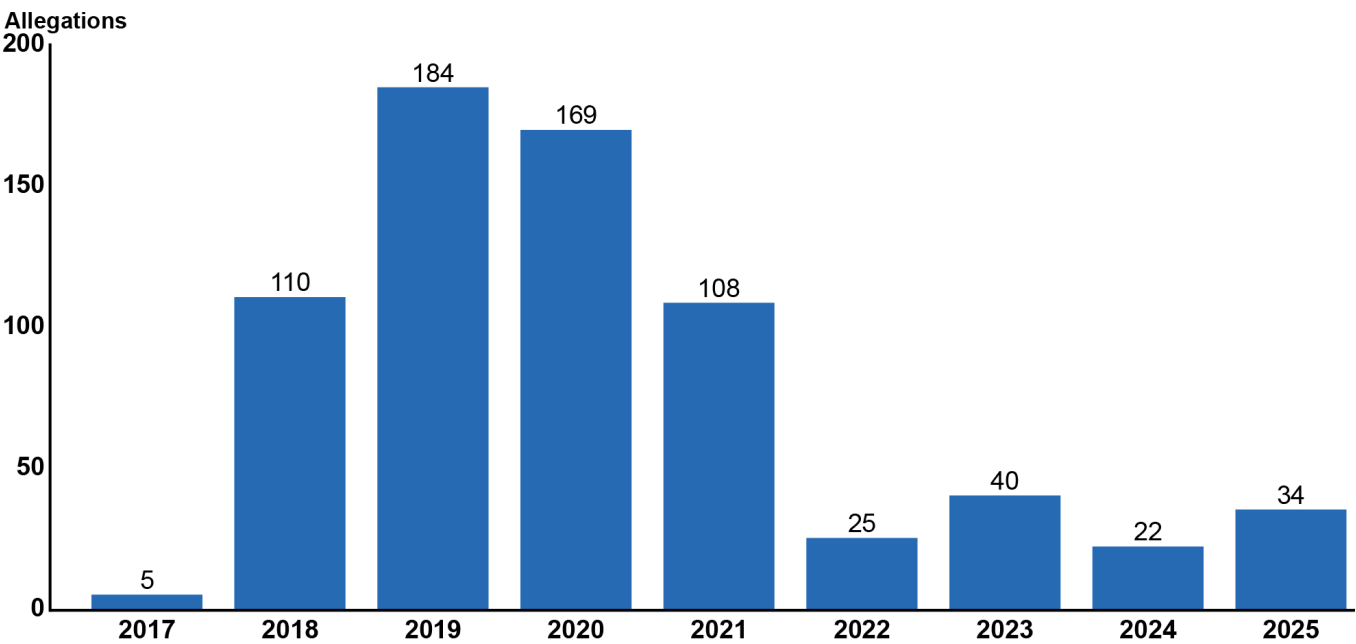
Figure 5: National Institutes of Health Post-Award Monitoring Process and Actions to Address Foreign Interference Risks



Source: GAO analysis of National Institutes of Health information. | GAO-27-107848

According to our analysis of NIH data, OER received 697 allegations of potential foreign interference involving personnel on NIH awards from 2017 through 2025. Figure 6 shows the number of allegations NIH received each year from 2017 through 2025. NIH officials said the distribution of allegations may reflect, in part, an initial surge of allegations involving prior-year conduct when NIH began addressing foreign interference more systematically. They also said that, over time, institutions may have improved compliance with institutional and NIH requirements related to foreign interference, resulting in the general decline in allegations.

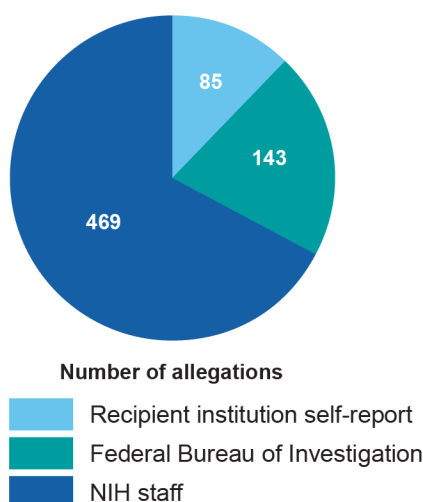
Figure 6: Number of Allegations of Potential Foreign Interference Received by the National Institutes of Health, 2017–2025



Source: GAO analysis of National Institutes of Health data. | GAO-27-107848

As figure 7 shows, most allegations originated from NIH staff, with the remainder originating from the FBI or recipient institution self-reports.

Figure 7: Sources of Allegations of Potential Foreign Interference Received by the National Institutes of Health, 2017–2025



Source: GAO analysis of National Institutes of Health data. | GAO-27-107848

Of the 697 allegations of potential foreign interference, NIH data show that OER officials determined that for 264, at least one violation of NIH's disclosure policies related to potential foreign interference had occurred. Those data also show that NIH tracks three types of violations that may indicate a risk of foreign interference: undisclosed participation in a foreign talent recruitment program, undisclosed foreign funding, and undisclosed foreign affiliations. According to its data, NIH considers undisclosed participation in a foreign talent recruitment program and undisclosed foreign funding to be serious violations but does not consider undisclosed foreign affiliations to be serious violations. Table 2 shows that of the 264 allegations where NIH found violations, 238 involved serious violations, while 26 involved no serious violation (i.e., undisclosed foreign affiliation without any other violation). NIH found no violation of its disclosure policies related to foreign interference for the remaining 433 allegations.

Table 2 also shows the NIH actions and recipient institution actions taken because of these allegations. Specifically, NIH or another federal agency referred 18 personnel with serious violations to HHS's Office of Recipient Integrity Coordination, which issued a government-wide suspension or debarment for 15 personnel, prohibiting them from participating in

federally funded research.⁴¹ For allegations where it found serious violations, NIH received repayment of funds from 48 institutions or personnel. NIH also removed 199 personnel from possible service as peer reviewers.⁴² Our analysis shows that recipient institutions also took actions against personnel for serious violations. Specifically, institutions terminated employment of 114 personnel, or they resigned, and institutions prohibited 52 personnel from participating in NIH awards to the institution.

NIH's data show that some personnel faced actions in cases where NIH did not identify serious disclosure violations. Specifically, as table 2 shows, one individual was referred for government-wide suspension or debarment, and NIH received repayment of awarded funds from five institutions and removed 14 personnel from possible service as peer reviewers. Our analysis shows that institutions also took actions against personnel in the absence of serious violations. Specifically, institutions terminated the employment of six personnel, or they resigned, and institutions prohibited four personnel from participating in NIH awards to the institution in the absence of serious violations.⁴³

Moreover, individuals faced actions in 45 of the 433 instances where NIH did not find disclosure violations. As table 2 also shows, one individual was referred for government-wide suspension or debarment. NIH also removed 44 personnel from possible service as peer reviewers, and, in the case of one individual, either the recipient institution terminated their employment or they resigned from their position.⁴⁴

⁴¹Those other agencies are the Department of Justice, National Science Foundation, Department of Agriculture, and HHS OIG.

⁴²Overall, NIH received about \$39.6 million in repayments from 55 individuals and institutions in connection with foreign interference allegations.

⁴³A single individual or institution may be subject to multiple actions, so the total number of actions is greater than the total number of allegations.

⁴⁴NIH data did not specify which outcome applied to this individual.

Table 2: Outcomes of National Institutes of Health (NIH) Foreign Interference Allegations, 2017 through 2025

Outcome of allegation	Source of action	Type of action	Number of instances
One or more serious violations found (238)	NIH	Removal from possible service as peer reviewer	199
		Receipt of repaid funds	48
	NIH or other federal agency	Referral for government-wide suspension or debarment	18
	Recipient institution	Termination of employment or individual resigned	114
		Prohibition from participating in NIH awards at the institution	52
Violation found, not serious (26)	NIH	Removal from possible service as peer reviewer	14
		Receipt of repaid funds	5
	NIH or other federal agency	Referral for government-wide suspension or debarment	1
	Recipient institution	Termination of employment or individual resigned	6
		Prohibition from participating in NIH awards at the institution	4
No violation found (433)	NIH	Removal from possible service as peer reviewer	44
		Receipt of repaid funds	0
	Federal Bureau of Investigation	Referral for government-wide suspension or debarment	1
	Recipient institution	Termination of employment or individual resigned	1
		Prohibition from participating in NIH awards at the institution	0

Source: GAO analysis of National Institutes of Health data. | GAO-27-107848

Note: Each allegation corresponds to an individual researcher. NIH and recipient institutions may take more than one action against a researcher alleged to have engaged in foreign interference.

NIH officials stated that some actions taken in cases without serious disclosure violations, or where NIH’s data did not identify a disclosure violation, reflected other integrity or enforcement concerns not captured in NIH’s foreign interference violation categories. According to these officials, these concerns included active institutional or law enforcement investigations, peer review integrity issues, research misconduct, harassment, misrepresentation, and other compliance matters. The officials added that some individuals were also removed from peer review due to evidence of recent participation in a malign foreign talent recruitment program.

Some disclosure violations did not result in actions by NIH or recipient institutions. We found 41 personnel for whom NIH identified disclosure violations—31 of which NIH considered to be serious—but neither NIH

nor the institution had taken actions as of December 2025. NIH officials told us that in these instances, either

- the case remained ongoing;
- the violation was not associated with a conflict of interest or commitment and therefore no action was necessary;
- an individual had been approached by a foreign talent recruitment program but had not accepted an offer; or
- the institution had taken action, such as requiring additional training or increasing disclosure oversight, not reflected in NIH's data.

In addition to administrative actions, some allegations of potential foreign interference have led to civil or criminal proceedings, although NIH has reported that such outcomes are rare. Overall, as of December 2025, NIH reported working with the Department of Justice to secure three civil settlements against two recipient institutions and criminal convictions against three individuals. In each of those instances, the judgment or conviction involved charges of fraud rather than the misappropriation of funded research to the benefit of foreign parties.

OER officials estimated that about 1 percent of individuals who receive NIH-awarded funds may be involved in foreign interference. However, according to our analysis, the greatest number of allegations of potential foreign interference OER has received in a single calendar year was 184 in 2019, across an average of about 50,000 active grants each fiscal year from 2017 through 2025.⁴⁵ NIH data provide limited insight into the prevalence of foreign interference in research the agency supports because the agency's data track allegations it received and the outcomes of compliance reviews but are not designed to estimate the prevalence across NIH's award portfolio. In addition, NIH generally addresses allegations through compliance with disclosure policies rather than separately determining whether awarded research was misappropriated.

NIH Uses Pre-Award Screening and System Access Controls

In addition to relying on disclosure requirements, NIH officials told us they use certain pre-award screening steps and system access controls to help safeguard federally funded research. Before making awards, NIH institute and center officials are required to review, through the System for Extramural Award Risk (SEAR) tool in eRA, entity information from

⁴⁵NIH tracks foreign interference allegations at the individual-investigator level rather than by the awarded project, and each individual may be associated with between one and 10 NIH awards each year.

SAM.gov, including responsibility and qualification information and exclusions related to suspensions and debarments, as part of pre-award risk assessments. These reports indicate whether institutions are ineligible to receive federal awards or face restrictions on awards because of findings in past civil, criminal, or administrative proceedings. NIH officials told us they consider these pre-award screening steps and system access controls to be safeguards against foreign interference, although they are not specific to foreign interference risk. Violations of laws, regulations, or policies related to foreign interference are among the reasons an individual or institution could appear as prohibited or restricted in SAM.gov.⁴⁶

Outside the grant review and monitoring process, NIH officials told us they safeguard funded research by controlling access to the agency's Electronic Research Administration (eRA) system, a set of web-based systems used to manage research awards throughout the award life cycle. According to the officials, NIH's Office of eRA monitors access by users in certain foreign countries—Burma, China, Cuba, Eritrea, Hong Kong, India, Iran, Nicaragua, Nigeria, North Korea, Pakistan, Russia, Saudi Arabia, Syria, Tajikistan, and Turkmenistan. They also said the office reviews registration attempts from institutions in countries of concern twice each year, including checking whether institutions appear on any of several lists of entities that may pose foreign interference concerns. These lists are published by U.S. and foreign governments, as well as certain nongovernmental organizations, and include:

- U.S. Food and Drug Administration – Listing of Significantly Regulated Organizations
- U.S. Department of the Treasury – Specially Designated Nationals and Blocked Persons list
- U.S. Department of Defense (DOD) – Lists Published in Response to Section 1286 of the National Defense Authorization Act for Fiscal Year 2019 (Public Law 115-232), as amended
- U.S. Department of Commerce – Consolidated Screening List
- Government of Canada – Named Research Organizations list

⁴⁶GAO has previously reported on challenges agencies face in using SAM.gov exclusion and responsibility/qualification information, GAO, *Research Security: Strengthening Interagency Collaboration Could Help Agencies Safeguard Federal Funding from Foreign Threats*, [GAO-24-106227](#) (Washington, D.C.: Jan. 11, 2024).

-
- Australian Strategic Policy Institute – China Defence Universities Tracker
 - International Coalition to End Transplant Abuse in China – Chinese Transplant Institutions list

Officials told us that if the Office of eRA identifies concerns about an institution, it contacts NIH's Office of Defensive Counterintelligence and Personnel Security to assess whether the institution poses a significant risk. If that office determines the institution poses such a risk, the Office of eRA blocks accounts associated with that institution from accessing eRA systems. According to NIH officials, as of April 2025, the Office of eRA had blocked 25 institutions and hundreds of individuals from accessing eRA.

Although these steps may help safeguard NIH systems and prevent awards to ineligible entities, they are not designed to routinely verify whether grant applicants and personnel have fully disclosed foreign affiliations, foreign financial interests, or foreign collaborations in connection with specific projects funded through NIH awards.

Case Studies Illustrate Potential Limitations of NIH's Disclosure Requirements

We reviewed seven NIH awards to illustrate how NIH's process for identifying and managing foreign interference risks operates in circumstances that may present heightened risk. Our review suggests that NIH's primarily disclosure-based application review and award monitoring efforts may not identify all potential indicators of elevated foreign interference risk. That is, in our seven nongeneralizable case studies, we identified foreign affiliations and coauthored publications that did not appear in the NIH grant applications we reviewed. These observations do not demonstrate policy violations or establish how frequently such information is omitted across NIH's research portfolio, but they illustrate issues that may arise when a process generally does not verify disclosures against external sources absent an allegation.

We selected five awards acknowledged in publications that were coauthored by NIH-supported researchers and researchers affiliated with institutions included on the DOD's *Fiscal Year 2023 Lists Published in Response to Section 1286 of the National Defense Authorization Act for Fiscal Year 2019* (Public Law 115-232), as amended (DOD list). According to DOD, institutions on the list engaged in activities that increased the likelihood that U.S.-funded research and development efforts could be misappropriated to the detriment of U.S. national security and economic competitiveness. Collaborations involving researchers

affiliated with these institutions may therefore present elevated foreign interference risks.

NIH does not use the DOD list to assess foreign interference risks in the research it funds. We did not identify a requirement that NIH do so, and coauthoring a publication with a researcher on the DOD list does not, by itself, indicate that foreign interference occurred. For each award, we reviewed publicly available sources for information about potential foreign components and foreign affiliations that did not appear in the documents NIH reviewed.⁴⁷ The absence of such information does not necessarily indicate a violation of NIH policies or requirements. We provided the information to NIH.

NIH officials told us that their prior reviews had not raised concerns about the five awards and that NIH had received no foreign interference allegations involving those awards. However, they also told us that some of the information we provided, including information indicating that researchers may have had foreign affiliations or activities that were not reflected in the NIH records we reviewed, was potentially concerning. They said they would conduct additional reviews to determine whether opening compliance cases was warranted.

We selected two additional awards that NIH identified as examples in which it had imposed mitigations in response to foreign interference concerns.⁴⁸ For both awards, NIH had received foreign interference allegations involving personnel at the recipient institutions and required

⁴⁷NIH began enhanced efforts to address foreign interference in 2016, and its policies have evolved over time as federal requirements have evolved with, for example, the issuance of NSPM-33 and the passage of statutory provisions discussed above. For our case studies, the five awards we identified based on coauthored publications were active between 2020 and 2025. The policies and requirements that would have been applicable at any given point in the life cycle of each of these grants may have evolved over the period of performance. However, requirements throughout that period consistently included the disclosure of foreign components, foreign financial interests, and certain foreign affiliations. For that reason, we looked at whether publicly available sources revealed undisclosed information in these areas for the awards and progress reports during this time in these five case studies.

⁴⁸Both awards were active between 2020 and 2025, the period during which NIH requirements consistently included the disclosure of foreign components, foreign financial interests, and certain foreign affiliations. For that reason, we looked at whether publicly available sources revealed undisclosed information in these areas for the awards and progress reports during this time in these two case studies.

the institutions to withhold the portion of the individuals' salaries funded through NIH awards while compliance cases were ongoing.

The case studies show that there are potential limitations to NIH requirements for the disclosure of foreign activities and affiliations. For three of the five awards we identified, researchers had foreign affiliations that were not disclosed to NIH. For example, the principal investigator (PI) on one award held five honorary professorships at Chinese universities that were not disclosed in the application or progress reports. For these awards, because the active dates of those affiliations were unclear, it was not possible to determine whether disclosure was required.

NIH policy requires applicants to disclose foreign components of awards and gives, as an example of an activity that may constitute a foreign component, collaboration with investigators at a foreign site expected to result in coauthorship. Only one of the five awards we selected based on coauthored publications disclosed a foreign component corresponding with the publication we identified. However, not all foreign collaborations constitute foreign components. Activities, including foreign collaborations, are considered a foreign component and must be disclosed when a significant element or segment of a project funded through an NIH award is conducted outside the United States, and some collaborations resulting in coauthored publications may not meet this criterion. Moreover, NIH officials told us that in two of our case studies, the NIH award was unrelated to the publication that acknowledged it and may have been listed in the publication to inflate the number of publications resulting from the award. For those awards, disclosure of a foreign component would not have been required.

The two case studies based on awards NIH identified show that NIH may impose conditions on awards to mitigate risks when compliance cases are ongoing. They also show that NIH may determine, after reviewing the facts of the individual case, that policy violations such as undisclosed funding or affiliations do not indicate a risk of foreign interference. In one of these two case studies, NIH required the individual to stop collaborating with colleagues in China in connection with the NIH award. In the other, NIH determined that the individual was not required to disclose the Chinese funding that had led to the allegation. In both cases, the individuals resumed receiving NIH-awarded funds once the compliance cases ended. Both individuals also continued to coauthor publications with affiliates of multiple institutions on the DOD list.

The nature of some biomedical research may increase the potential consequences of foreign interference because such research can have both beneficial and harmful applications. NIH assesses certain awarded research involving pathogens and toxins for dual-use potential, but none of the seven awards we reviewed met the applicable criteria for dual-use research of concern or research involving pathogens with enhanced pandemic potential. According to NIH officials, NIH does not assess research that does not involve pathogens or toxins for dual-use potential because the agency lacks the resources and is not required to do so. A recent National Academies workshop noted that biosecurity and biosafety policies and risk assessment frameworks have focused largely on pathogens and toxins, even though other biotechnology applications may also present security and safety risks.⁴⁹ Appendix II provides our detailed analysis of these cases.

NIH Aligns with GAO's Enterprise Risk Management Practices but Has Not Conducted a Fraud Risk Assessment Tailored to Its Extramural Research Program

NIH's Enterprise Risk Management Profile identifies foreign interference as a component of an enterprise risk area, and NIH's fraud risk profile identifies foreign influence as a top fraud risk.⁵⁰ NIH uses fraud indicators, including nondisclosure of foreign affiliations or funding and participation in foreign talent recruitment programs, to identify possible foreign interference during the application and review process. We found that NIH's risk management program was fully aligned with GAO's ERM practices but not fully aligned with all of GAO's Fraud Risk Framework overarching concepts. The following details our findings for each of the six practices:

NIH's Risk Management Program Fully Aligns with GAO's Enterprise Risk Management Framework

GAO's Enterprise Risk Management framework includes six practices and 15 key considerations.⁵¹ Our review found that NIH's risk

⁴⁹National Academies of Sciences, Engineering, and Medicine, *Biological Threats in the Age of Emerging Biotechnology: Proceedings of a Workshop Series* (Washington, D.C.: The National Academies Press, 2026), doi: 10.17226/27767.

⁵⁰NIH, *NIH Risk Management Program Guidebook for ICs and OD Offices*; NIH, *NIH Policy Manual*, 1750 - NIH Risk Management Program.

⁵¹GAO, *Enterprise Risk Management: Selected Agencies' Experiences Illustrate Good Practices in Managing Risk*, [GAO-17-63](#) (Washington, D.C.: Dec. 1, 2016).

management program aligned with all 15 key considerations under the six ERM practices.⁵²

Leaders guide and sustain ERM strategy. NIH's risk management program aligns with all three key considerations for this practice: designating ERM leaders, committing organization resources to support ERM, and setting organizational risk appetite. NIH has designated a risk management officer and risk management champions for each of its units with responsibilities for implementing and maintaining risk management programs. NIH also incorporated ERM into its strategic plan and resource allocations, and NIH's Policy Manual states that institutes and centers should identify and score risks that could impact their mission, goals, and objectives.

Develop a risk-informed culture to ensure all employees can effectively raise risks. NIH's risk management program aligns with all four key considerations for this practice: encouraging employees to discuss risks openly, training employees on ERM approach, engaging employees in ERM efforts, and customizing ERM tools for NIH's mission and culture. NIH's Policy Manual states that NIH employees will embrace the NIH risk management culture that promotes open and candid risk identification and management. NIH also provided documentation showing it trained employees in its ERM approach. Furthermore, NIH's Policy Manual indicates that risk management officers, risk management champions, and others involved in the process are assigned specific roles in supporting this culture. And NIH officials told us that the Management and Budget Working Group monitors risks and discusses mitigation strategies.

Integrate ERM capability to support strategic planning and organizational performance management. NIH's risk management program aligns with both key considerations for this practice: incorporating ERM into strategic planning and using ERM to improve agency decision-making. In executing NIH's risk management methodology, institutes and centers are to review mission-related strategic plans and consider constraints when planning risk management activities. NIH's Policy Manual also states that institutes and centers are

⁵²For the purposes of this report, we assessed whether NIH's risk management program aligns with the key considerations of GAO's enterprise risk management practices. Alignment indicates that NIH's risk management program addresses the key considerations of the ERM practice.

to monitor the effectiveness of internal controls and integrate periodic internal assessments into their continuous monitoring activities.

Establish a customized ERM program integrated into existing agency processes. NIH's risk management program aligns with all three key considerations for this practice: designing an ERM program that fits the agency, developing a consistent and routinized ERM program, and using a maturity model approach to build the program. NIH's Policy Manual states that institutes and centers are to develop and document appropriate risk responses to enterprise risks, and NIH officials told us that the Management and Budget Working Group is responsible for monitoring risks and discussing mitigation strategies. NIH also uses an ERM capability maturity model survey to assess the maturity of its risk management programs.

Continuously manage risks. NIH's risk management program aligns with the key consideration for this practice: tracking and monitoring current and emerging risks. NIH's Policy Manual directs institutes and centers to routinely monitor their risk environments, identify and score new risks, review existing risks for continued applicability, and rescore risks based on current circumstances. It also directs them to monitor the status of risk responses. NIH officials told us that their annual risk inventory assessment process incorporates assessment of the likelihood, impact, controls, and risk response decisions. For example, NIH officials told us that OER's fiscal year 2025 risk inventory assessment identified and assessed risks related to foreign influence and peer review integrity. The assessment also included an impact and likelihood score related to the impact on the integrity of NIH-awarded research by undue outside and foreign involvement if researchers do not fully disclose foreign affiliations and funding information.

Share information with internal and external stakeholders to identify and communicate risks. NIH's risk management program aligns with both key considerations for this practice: incorporating stakeholder feedback to better manage risks and sharing risk information across the enterprise. NIH's Policy Manual states that, when requested by NIH senior leadership, OMA is to collaborate with key stakeholders to monitor and report completion of corrective actions. NIH officials also told us they engage with the broader research community to share best practices and lessons learned from fraud incidents.

NIH’s Risk Management Program Does Not Fully Align with GAO’s Fraud Risk Framework

NIH has multiple controls and oversight processes that address foreign-interference-related risks, including disclosure requirements, pre-award screening, post-award monitoring, program integrity activities, internal controls, and referrals to HHS OIG and DOJ, as discussed above. However, according to NIH officials, these activities are not based on a documented fraud risk assessment tailored to the extramural research program. Although NIH’s annual risk inventory considers fraud, it is not a documented, program-specific assessment of fraud schemes, controls, and residual risks in the extramural research program. A fraud risk assessment is foundational to the GAO Fraud Risk Framework because it helps agencies identify and prioritize the fraud risks facing a program, assess their likelihood and impact, and use that assessment to guide prevention, detection, response, monitoring, and evaluation activities. Without such an assessment, an agency may have fraud-related controls and response processes in place but lack assurance that those activities are strategically targeted to the program’s most significant fraud risks.

GAO’s Fraud Risk Framework includes multiple overarching concepts, each consisting of leading practices for identifying, assessing, and responding to fraud risks in federal programs. NIH does not align with several of the leading practices under the GAO Fraud Risk Framework overarching concepts we reviewed.⁵³ Table 3 shows the results of our assessment of NIH’s alignment with the leading practices for nine selected overarching concepts. Appendix III provides additional information for this assessment.

Table 3: NIH Risk Management Program’s Alignment with Leading Practices by GAO Fraud Risk Framework Overarching Concept

Overarching concept	Number of aligned leading practices
2.1. Plan regular fraud risk assessments that are tailored to the program	
2.2. Identify and assess risks to determine the program’s fraud risk profile	
3.1. Determine risk responses and document an antifraud strategy based on the fraud risk profile	
3.2. Design and implement specific control activities to prevent and detect fraud	

⁵³[GAO-15-593SP](#).

3.3. Develop a plan outlining how the program will respond to identified instances of fraud	 
3.4. Establish collaborative relationships with stakeholders and create incentives to help ensure effective implementation of the antifraud strategy	   
4.1. Conduct risk-based monitoring and evaluate all components of the fraud risk management framework	   
4.2. Monitor and evaluate fraud risk management activities with a focus on measuring outcomes	 
4.3. Adapt fraud risk management activities and communicate the results of monitoring and evaluations	   

 Aligned with GAO Fraud Risk Framework leading practice

 Not aligned with GAO Fraud Risk Framework leading practice

Source: GAO analysis of National Institutes of Health (NIH) information. GAO (icons). | GAO-27-107848

The following details our assessment of NIH's alignment with the leading practices for the nine overarching concepts.

2.1 Plan regular fraud risk assessments that are tailored to the program. NIH's risk management program aligns with two of the four leading practices for this concept: involve relevant stakeholders in the assessment process, and identify tools, methods, and sources for gathering information about fraud risks. It does not align with the other two: conduct a fraud risk assessment tailored to its extramural research program, and plan to conduct such assessments at regular intervals. NIH officials told us they hold biweekly and ad hoc research integrity meetings to review procedures in their research security review process and involve relevant internal and external stakeholders, including institute and center leadership, awards management staff, enterprise risk management officials, and recipient institutions. NIH officials also told us that they use multiple sources of information to identify and assess fraud-related risks, including annual risk inventory assessments, oversight reviews, investigative and allegation trends, internal control assessments, and subject-matter expertise from program integrity and grants oversight officials.

NIH officials told us that the agency's institutes and centers submit risk inventories through an annual process that considers risks related to fraud, waste, abuse, foreign influence, and research integrity as appropriate to their individual operational environments. NIH's annual risk inventory assessment process identifies and scores risks across NIH components. However, NIH did not demonstrate that this process

systematically identifies how fraud could occur in the extramural research program, assesses the likelihood and impact of specific fraud schemes, evaluates the suitability of existing controls, or prioritizes residual fraud risks. Those program-specific steps are central to a fraud risk assessment under GAO's Fraud Risk Framework. NIH also did not demonstrate that it uses the annual risk inventory to determine whether its safeguards against foreign interference are appropriately aligned with the identified fraud risks.

NIH collects data on the results of compliance cases stemming from allegations of potential foreign interference. However, as discussed earlier, these data provide limited insight into the prevalence of foreign interference in NIH-supported research because they track allegations received and compliance review outcomes, rather than estimate the prevalence of foreign interference across NIH's award portfolio.

Regarding the two remaining leading practices for this overarching concept, NIH officials told us that NIH has not conducted a fraud risk assessment tailored to its extramural research program and has not planned to conduct such assessments at regular intervals. NIH officials told us the agency conducted a fraud risk assessment for its National Center for Advancing Translational Sciences Clinical and Translational Science Awards program. Although that assessment identified unauthorized foreign interference as a fraud risk, it did not assess the likelihood and impact of that risk across NIH's extramural research program more broadly. NIH officials also told us the agency has no stand-alone fraud risk assessment. As discussed above, while NIH conducts annual risk inventory assessments that consider fraud, they are not a documented, extramural-program-specific assessment of fraud schemes, controls, and residual risks.

Without a documented fraud risk assessment tailored to its extramural research program, NIH does not have a systematic basis for determining whether its safeguards and oversight processes address the program's most significant fraud risks and adapting those processes as fraud schemes and foreign interference risks evolve.

2.2 Identify and assess risks to determine the program's fraud risk profile. NIH's risk management program aligns with three of the five leading practices of this concept: identify inherent fraud risks affecting the program, assess the likelihood and impact of inherent fraud risks, and document the program's fraud risk profile. NIH officials told us that the agency's institutes and centers submit risk inventories during their annual

risk inventory assessment process, and that this process includes consideration of risks related to fraud, waste, abuse, foreign influence, and research integrity as appropriate to their individual operational environments.

NIH officials told us that their annual risk inventory assessment incorporates assessment of the likelihood, impact, existing controls, and risk response decisions, including fraud risks. For example, NIH officials told us that OER's fiscal year 2025 risk inventory assessment identified and assessed risks related to foreign influence and peer review integrity. NIH officials also said the assessment included an impact and likelihood score related to the impact on the integrity of NIH-awarded research by undue outside and foreign involvement if researchers do not fully disclose foreign affiliations and funding information. NIH also provided documentation of a fraud risk profile that identifies NIH's top fraud risks, including foreign influence, and assigns them priority and risk levels based on the likelihood and impact. NIH officials told us that the fraud risk profile was informed by various sources of information such as consultations with subject matter experts, results from internal control reviews, the fraud risk assessment for NIH's National Center for Advancing Translational Sciences Clinical and Translational Science Awards program discussed above, and lessons learned from compliance cases. However, NIH officials did not state that the fraud risk profile was informed by NIH's annual risk inventory assessment process.

NIH officials told us they have a low tolerance for foreign interference risk, but NIH's fraud risk profile does not document the extramural research program's fraud risk tolerance or assess the suitability of existing controls and prioritize residual fraud risks for the extramural research program. As discussed above, because NIH has not conducted and documented a fraud risk assessment tailored to the extramural research program, it lacks a basis for determining whether its existing controls, monitoring activities, and response processes are effective in addressing fraud risks, including risks related to foreign interference. Conducting a fraud risk assessment would help NIH make such determinations.

3.1 Determine risk responses and document an antifraud strategy based on the fraud risk profile. NIH's risk management program aligns with four of the six leading practices for this concept. NIH has established roles and responsibilities for fraud risk management activities, including responsibilities for OMA, risk management officers, risk management champions, and the Management and Budget Working Group. NIH officials also described timelines for certain risk management activities,

such as annual risk inventory assessments and continuous monitoring of internal controls.

NIH's fraud risk profile identifies major fraud risks and summarizes controls in the application and management process, and NIH links antifraud efforts to its broader application and monitoring activities. Although NIH's fraud risk profile states that information from the profile can inform operations dedicated to preventing, detecting, and responding to fraud, NIH did not demonstrate alignment with the remaining two leading practices for this concept: use the fraud risk profile to help decide how to allocate resources to respond to residual fraud risks and develop, document, and communicate an antifraud strategy. NIH officials told us that NIH leadership uses the fraud risk profile as a data source for formulating risk-based budget analyses and defending resource allocations, but they did not tell us how fraud risks related to foreign interference inform resource allocation decisions to respond to that risk.

NIH has not developed, documented, or communicated an antifraud strategy, based on a fraud risk assessment, for the extramural research program that describes the program's activities for preventing, detecting, and responding to fraud risks identified, as well as monitoring and evaluation. NIH officials told us that instead of an antifraud strategy, they have a layered operational approach to fraud prevention, detection, response, monitoring, and evaluation through their internal controls, disclosure requirements, award screening and monitoring, program integrity activities, and coordination with HHS OIG and DOJ. According to GAO's Fraud Risk Framework, antifraud strategies identify who is responsible for fraud risk management, what the program is doing to manage fraud risk, when the program implements fraud risk management activities, where the program focuses its fraud risk management activities, and why fraud risk management is important. Conducting a fraud risk assessment of its extramural research program in accordance with GAO's Fraud Risk Framework could help NIH identify the fraud risks that it could address through an antifraud strategy.

3.2 Design and implement specific control activities to prevent and detect fraud. NIH's risk management program aligns with one of three leading practices for this concept: focus on fraud prevention over detection. While NIH has not developed or documented an antifraud strategy based on a fraud risk assessment that would provide a basis for designing and evaluating specific control activities for the extramural research program, NIH has implemented some control activities intended to prevent and detect fraud. NIH control activities include conducting pre-

award risk assessments, fraud awareness initiatives, reporting mechanisms, and employee integrity activities. NIH officials said they conduct pre-award risk assessments for all awards, confirm compliance with NIH policies and standard terms and conditions before awarding funds, and communicate with external recipients to resolve or mitigate foreign interference risks before awards are made.

As discussed earlier, in the section of this report on NIH's disclosure-based assessment process, NIH officials told us that, during pre-award risk assessments, staff examine disclosures to determine whether there are discrepancies that may indicate potential foreign conflicts of interest or commitment. NIH officials told us they do not keep data on how many possible foreign risk indicators staff identify before making awards or on how many new awards have conditions imposed to mitigate foreign interference risk. NIH officials also stated that its pre-award risk assessments include checking applicants against qualification and exclusion information in SAM.gov and reviewing foreign components through the Department of State process. In addition, NIH officials provided documentation showing that NIH conducts fraud awareness training for award staff and program staff and maintains reporting mechanisms for fraud, waste, and abuse through OMA's public website and the HHS OIG referral process. The NIH Grants Policy Statement describes avenues for reporting fraud, waste, or abuse.⁵⁴ NIH officials also told us that the agency follows federal and HHS-wide personnel and ethics frameworks for employee integrity and screening.

While NIH has designed and implemented some control activities related to GAO's leading practice to design and implement control activities to prevent and detect fraud, including fraud-awareness initiatives, reporting mechanisms, and employee integrity activities, NIH has not provided evidence that it conducted data analytics activities called for in this leading practice. As discussed in the section above on NIH compliance reviews, NIH collects data on the results of compliance cases stemming from allegations of potential foreign interference. However, these data provide limited insight into the prevalence of foreign interference in research supported by NIH. While NIH tracks allegations received and compliance review outcomes, it does not estimate the prevalence of foreign interference across its award portfolio. NIH officials also told us

⁵⁴NIH, Grants Policy Statement, 2.3.10 at pp. I-70-71 (Mar. 2026).

they do not have data on foreign interference risk indicators identified prior to awards being made.

NIH also did not show that it considered the benefits and costs of control activities in light of assessed residual fraud risks. Although NIH provided written descriptions of the benefits and costs associated with its activities to address fraud risks, these descriptions were not grounded in a documented assessment of the prevalence or potential impact of fraud risks, including foreign interference. Conducting a fraud risk assessment of its extramural research program in accordance with GAO's Fraud Risk Framework could help NIH identify the fraud risks for which control activities could be developed to prevent and detect and the costs and benefits of which could be assessed.

3.3 Develop a plan outlining how the program will respond to identified instances of fraud. NIH has certain processes in place that align with the two leading practices supporting this concept. NIH's Enterprise Risk Management Guidebook states that the agency is committed to responding promptly to instances of fraud, including working with appropriate parties to take proper disciplinary actions and implementing remedial measures to prevent recurrence. NIH's fraud risk profile identifies foreign influence as a fraud risk, and NIH's foreign interference website describes the agency's process for responding to allegations, including referring cases that may rise to the level of civil or criminal fraud to HHS's OIG. NIH officials also told us that OMA's Division of Program Integrity reviews allegations of fraud, waste, and abuse in cooperation with the HHS OIG and that NIH refers cases of potential foreign interference, such as those involving undisclosed foreign affiliations, to the HHS OIG and, when appropriate, to DOJ. As discussed in the section above on NIH's implementation of research security requirements, an HHS OIG official told us their Office of Investigations routinely receives referrals and information on potential violations of disclosure requirements from NIH, and they use that information strictly for law enforcement purposes as part of their broader grant fraud investigations.

3.4 Establish collaborative relationships with stakeholders and create incentives to help ensure effective implementation of the antifraud strategy. NIH's risk management program aligns with three of the four leading practices for this overarching concept. NIH officials told us they have collaborative relationships with internal and external stakeholders to share information on fraud risks and emerging fraud schemes, and that they work with the HHS OIG and other federal

agencies, such as DOJ and FBI, to investigate and address potential cases of fraud and foreign interference. NIH officials also said they engage with the broader research community to share best practices and lessons learned from fraud incidents and that they provide training and outreach to award recipients on fraud risks, red flags, and preventive measures. These activities help support awareness of fraud risk and compliance responsibilities.

A leading practice for this overarching concept holds that agencies should create incentives for employees to manage risks and report fraud, including creating performance metrics that assess fraud risk management efforts and employee integrity, and balance these metrics with those that measure employees' performance related to other duties. While NIH officials told us they integrate fraud-related responsibilities into broader grants oversight, management, compliance, internal control, and operational functions, they do not integrate fraud-related responsibilities into incentive structures or performance metrics for the extramural research program. NIH officials told us that managers are expected to identify and mitigate fraud risks within the ERM cycle. Implementing performance metrics can reinforce the objectives of fraud risk management activities and strike a balance with other activities that serve the program's mission, as called for in GAO's Fraud Risk Framework.

4.1 Conduct risk-based monitoring and evaluate all components of the fraud risk management framework. NIH's risk management program aligns with two of the four leading practices for this concept: engage stakeholders responsible for specific fraud risk management activities in monitoring and evaluation, and collect and analyze data, including data from reporting mechanisms and instances of detected fraud. NIH officials told us that OER and NIH's Office of Policy for Extramural Research Administration (OPERA) monitor emerging foreign interference risks and communicate status and resolution to NIH program and grants staff through the NIH Alert Module, the Research Misconduct Allegation Review System, and direct e-mail communication. NIH officials also said they hold monthly meetings with the HHS OIG to discuss ongoing cases and biweekly research integrity meetings to review research security procedures.

NIH officials also told us they collect information on instances of fraud, including those related to foreign interference, and perform trend analysis. NIH officials told us they revise their policies and procedures based on the insights from those data to close gaps that have been exploited, such as updating their pre- and post-award disclosures relating to the

biographical sketch and other support. NIH officials also stated that they implement stronger internal controls and safeguards in areas identified as high risk, which may include more rigorous vetting, enhanced monitoring, and stricter enforcement of compliance requirements.

However, NIH did not demonstrate alignment with the two remaining leading practices for this concept. NIH has not monitored and evaluated the effectiveness of existing fraud prevention activities and controls or applied a risk-based monitoring approach that accounts for internal and external factors affecting the control environment. As discussed previously, NIH has not conducted a fraud risk assessment tailored to the extramural research program or developed an antifraud strategy against which it can assess the effectiveness of the fraud prevention and response activities. Additionally, while NIH tracks foreign interference allegations received and compliance review outcomes, it does not estimate the prevalence of foreign interference across NIH's award portfolio. Conducting a fraud risk assessment tailored to the extramural research program would help NIH determine whether its existing fraud prevention activities and controls are appropriate. Such an assessment would guide a risk-based monitoring approach for foreign interference and related fraud risks.

4.2 Monitor and evaluate fraud risk management activities with a focus on measuring outcomes. NIH's risk management program does not align with either leading practice for this concept—measure outcomes, in addition to outputs, of fraud risk management activities, and assess how well managers follow recommended leading practices for designing fraud risk management activities. As discussed in the section above on NIH compliance reviews, NIH provided data on the number of allegations of potential foreign interference that had at least one violation of NIH disclosure policies related to potential foreign interference. However, those data do not show how often NIH found actual conflicts of interest or commitment, scientific overlap, or misappropriation of federally funded research to the detriment of U.S. national security or economic competitiveness. As discussed in the section above on NIH's reliance on disclosure compliance to identify potential foreign interference risks, NIH does not keep data on how many possible foreign risk indicators staff identify before making awards or on how many new awards have conditions imposed to mitigate foreign interference risk.

NIH also does not demonstrate that it measures the outcomes of its fraud risk management activities, as distinct from outputs such as allegations received, compliance cases opened, or actions taken. NIH officials told us

that managers are expected to identify and mitigate fraud risks within the ERM cycle, but NIH did not provide examples showing how managers are assessed against leading practices specific to fraud risk management, including the risk of foreign interference. As noted above, conducting a fraud risk assessment tailored to the extramural research program would help NIH determine whether its fraud risk management activities are appropriately designed, evaluate their effectiveness, and adapt them as appropriate.

4.3 Adapt fraud risk management activities and communicate the results of monitoring and evaluations. NIH's risk management program aligns with two of the four leading practices for this concept: use results of investigations and prosecutions to enhance fraud prevention and detection and use analysis of identified instances of fraud and fraud trends to improve fraud risk management activities. NIH officials said they incorporate lessons learned from investigations, enforcement actions, and publicly reported prosecutions related to foreign interference into policy updates and operational safeguards. According to NIH officials, patterns identified through investigations and allegations, such as undisclosed foreign affiliations, overlapping foreign funding, inappropriate data access, and disclosure failures, informed enhancements in several areas. Such enhancements include strengthened disclosure requirements, enhanced pre-award screening, prohibition on data access from countries of concern, enhanced monitoring requirements for data access, improved incident reporting and escalation, and incorporation of fraud risk drivers and residual risk prioritization insights from foreign interference cases into the fraud risk profile.

As discussed in overarching concept 4.1 above, NIH officials told us they collect information on instances of fraud, including those related to foreign interference, and perform trend analysis. NIH officials told us they revise their policies and procedures based on insights from those data to close gaps that have been exploited and implement stronger internal controls and safeguards in areas identified as high risk.

However, NIH did not demonstrate alignment with the two remaining leading practices for this concept. NIH does not monitor and evaluate the effectiveness of its fraud prevention activities and use those results to improve the design and implementation of fraud risk management activities. Because NIH does not conduct such monitoring and evaluations, it also does not have results, including corrective actions, to communicate with relevant stakeholders. Conducting a fraud risk assessment tailored to the extramural research program would help NIH

HHS's Office for Human Research Protections Has Limited Visibility Into International Institutions Involved in HHS-Supported Human Subjects Research

determine whether its fraud risk management activities are appropriately designed, evaluate their effectiveness, and adapt them as appropriate.

In addition to research integrity risks related to foreign interference, NIH-awarded research conducted with researchers at foreign institutions may present oversight considerations related to the protection of human subjects. All non-exempt NIH-awarded human subjects research, including research conducted abroad, is subject to HHS regulations for the protection of human subjects at 45 C.F.R. part 46.⁵⁵ These regulations include requirements related to institutional review boards (IRB), informed consent, assurances of compliance, and additional protections for certain populations, including prisoners and children.⁵⁶

As with NIH's oversight of research security, oversight of human subjects protections relies primarily on institutional compliance mechanisms. According to NIH officials, recipient institutions, including universities, hospitals, and other research organizations, often implement these protections through human research protection programs. When applicable, an IRB reviews and monitors human subjects research in accordance with HHS regulations. Institutions engaged in HHS-supported non-exempt human subjects research must generally hold or rely on a Federalwide Assurance with HHS's Office for Human Research Protections (OHRP), through which the institution commits to comply with HHS human subjects protection regulations when applicable. Unless the research is exempt, HHS regulations require institutions to certify that an IRB has reviewed and approved research involving human subjects.⁵⁷

As part of its approval, the IRB must determine that the research complies with specified regulatory requirements, including requirements

⁵⁵45 C.F.R. part 46, subpart A, titled Basic HHS Policy for the Protection of Human Research Subjects and known as the Common Rule, covers federally funded or conducted research involving human subjects, requiring protections such as Institutional Review Board (IRB) oversight, informed consent, and assurances of compliance. All NIH-awarded human subjects research, unless exempt under 45 CFR § 46.104, is subject to the Common Rule.

⁵⁶Additional protections for pregnant women, fetuses, neonates, prisoners, and children that apply to HHS-awarded research are covered in 45 C.F.R. part 46, subparts B, C, and D.

⁵⁷45 C.F.R. § 46.103(d). The NIH Grants Policy Statement implements this requirement at 4.1.16.2.

related to informed consent.⁵⁸ For certain types of research, IRBs are also responsible for reviewing ongoing research activities covered by the Common Rule and for requiring submission of reports of noncompliance and unanticipated problems involving risks to subjects or others, with few specified exceptions.⁵⁹ In addition, scientific journals that publish results of such research generally impose ethical standards related to human subjects protections as a condition for publication and have issued retractions for violations.

OHRP helps ensure that human subjects research supported by HHS complies with the Common Rule at 45 C.F.R. Part 46, including requirements governing IRB review. According to OHRP officials, the office has not conducted routine inspections of international institutions or assessed the extent to which violations of human subjects protections in foreign research may go unreported. OHRP's last routine, not-for-cause inspection of an international institution was initiated in 2009, and its last for-cause inspection of an international institution was initiated in 2012. Officials attributed the lack of more recent international inspections largely to budgetary constraints. As a result, OHRP has limited visibility into whether oversight mechanisms for HHS-supported foreign human subjects research are functioning as intended.

OHRP has work underway that may strengthen its oversight approach. In January 2023, we recommended that OHRP conduct an annual risk assessment to determine whether it conducts an adequate number of routine IRB inspections and to optimize the use of IRB inspections in the oversight of IRBs and protection of research participants.⁶⁰ HHS agreed with the recommendation. As of May 2026, HHS reported that OHRP was developing a risk assessment framework, identifying relevant available data, exploring the feasibility of integrating data, identifying threshold questions, and considering how to leverage technology systems to facilitate implementation. It is too soon to assess the results of these efforts, and we are not making any additional recommendations at this time. As OHRP develops its risk assessment framework, HHS could use the findings of this report as an opportunity to better understand the risks

⁵⁸45 C.F.R. § 46.111. The purpose of informed consent is to inform potential participants about the study's purpose, potential harms, risks, benefits, and other information that allows the person to make an informed decision about participation.

⁵⁹45 C.F.R. § 46.109(e)-(f).

⁶⁰GAO, *Institutional Review Boards: Actions Needed to Improve Federal Oversight and Examine Effectiveness*, [GAO-23-104721](#) (Washington, D.C.: Jan. 17, 2023).

that violations in foreign human subjects research may go undetected. Implementing GAO's recommendation would help provide HHS greater assurance that OHRP is effectively overseeing IRBs and their activities to protect human research subjects.

OHRP officials told us that, as of January 2025, they were not aware of allegations during the prior 5 years related to unethical conduct in HHS-awarded human subjects research conducted outside the United States. OHRP officials noted, however, that before February 2025, its compliance database did not include a data field that allowed it to readily identify whether complaints involved domestic or international research. OHRP may take appropriate action in response to noncompliance, such as requiring corrective action; restricting or attaching conditions to an institution's Federalwide Assurance; or recommending that HHS take further action such as to suspend or terminate funding.

Conclusions

NIH has taken important steps to implement most federal research security requirements and safeguard its extramural research portfolio. However, NIH has not fully implemented one of the 15 selected requirements we reviewed. NIH has not implemented the requirement that institutions receiving more than \$50 million annually in federal science and engineering support certify that they have established and operate a research security program. Because NIH's implementation of this requirement depends on completion of an ongoing interagency process, we are not making a recommendation to NIH on this matter.

NIH's approach to identifying and managing foreign interference risks relies heavily on information disclosed by applicants, recipients, and researchers. Consequently, NIH may not identify elevated foreign interference risks when relevant affiliations, support, or activities are incomplete, undisclosed, or not otherwise brought to the agency's attention. This limitation does not mean that NIH should independently verify every disclosure. Rather, it underscores the importance of identifying the circumstances in which additional verification, monitoring, or other controls may be warranted. Such risk-informed safeguards are particularly important given the size and openness of NIH's extramural research enterprise and the potential for undisclosed foreign affiliations, support, or collaborations to affect NIH's award and oversight decisions.

NIH's Enterprise Risk Management Profile identifies foreign interference as part of an enterprise risk area, while NIH's fraud risk profile identifies what it terms "foreign influence" as a top fraud risk. However, NIH has not conducted a fraud risk assessment tailored to its extramural research

program. Without such an assessment, NIH lacks a documented basis for determining whether its disclosure requirements, monitoring activities, verification procedures, and response processes address the program's most significant fraud risks. Conducting and documenting such an assessment at regular intervals would help NIH identify and prioritize fraud risks as they evolve and determine whether its safeguards are appropriately designed, targeted, and adjusted accordingly.

Recommendations for Executive Action

We are making one recommendation to NIH:

The Director of NIH should conduct and document, at regular intervals and in accordance with GAO's Fraud Risk Framework, a fraud risk assessment tailored to NIH's extramural research program that considers risks related to foreign interference. (Recommendation 1)

Agency Comments

We provided a draft of this report to the Department of Health and Human Services (HHS) for review and comment. In its comments, reproduced in appendix IV, HHS stated that NIH concurred with our recommendation. HHS also provided technical comments, which we incorporated as appropriate.

Regarding our recommendation, HHS stated that NIH plans to incorporate applicable elements of GAO's Fraud Risk Framework into its existing risk management and internal control processes, strengthen consideration of fraud risk in its annual risk inventory assessments, and periodically conduct and document a fraud risk assessment tailored to its extramural research program that considers foreign interference. If implemented as described, these actions would address our recommendation.

In our draft report, we also recommended that NIH should ensure that the risks of malign foreign talent recruitment programs are included as a topic to be covered in institution-provided training for covered individuals used to address research security training requirements in the Research and Development, Competition, and Innovation Act. During the agency comment period, HHS stated that NIH agreed with the draft recommendation and took action to address it. Specifically, NIH added information to its Grants & Funding website in August 2026 clarifying that institution-provided research security training must address the risks of malign foreign talent recruitment programs, including the prohibition on NIH senior/key personnel participating in such programs. We reviewed NIH's action and determined that it addressed our draft recommendation. Accordingly, we removed the recommendation from our report. Clarifying

that alternative training must address these risks should provide NIH assurance that covered individuals are receiving required training.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 11 days from the report date. At that time, we will send copies to the appropriate congressional committees, the Secretary of Health and Human Services, the Director of the National Institutes of Health, and other interested parties. In addition, the report is available at no charge on the GAO website at <https://www.gao.gov>.

If you or your staff have any questions about this report, please contact me at WrightC@gao.gov. Contact points for our Offices of Congressional Relations and Media Relations may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix V.

//SIGNED//

Candice N. Wright
Director, Science, Technology Assessment, and Analytics

Appendix I: Objectives, Scope, and Methodology

This report examines (1) the National Institutes of Health's (NIH) implementation of selected federal research security requirements; (2) the extent to which NIH identifies and manages foreign interference risks for its extramural research program; (3) the extent to which NIH's risk management policies and practices align with GAO's enterprise risk management and Fraud Risk Framework practices; and (4) the Department of Health and Human Services' (HHS) oversight of human subjects research conducted outside the United States.

First, to evaluate NIH's implementation of selected federal research security requirements, we reviewed requirements established in (1) Section 223 of the William M. Thornberry National Defense Authorization Act for Fiscal Year 2021 (FY 2021 NDAA), (2) National Security Presidential Memorandum-33 (NSPM-33), and (3) the Research and Development, Competition, and Innovation Act, contained in what is commonly referred to as the CHIPS and Science Act. We then reviewed NIH policies, procedures, and practices to determine the extent to which NIH had implemented those selected requirements. We categorized NIH's implementation of the requirements as either Implemented—NIH has implemented the federal research security requirement—or Not implemented—NIH has not implemented the federal research security requirement. Requirements were considered not implemented if they were in progress but not fully implemented.

Second, to assess the extent to which NIH identifies and manages foreign interference risks for its extramural research program, we reviewed NIH documentation and data on allegations of potential foreign interference, interviewed NIH and other HHS officials, and conducted seven nongeneralizable case studies of NIH awards. Specifically, we reviewed public-facing and internal NIH policy documents, including the Grants Policy Statement, Policy Manual, Grants Policy and Administration Manual, and guide notices, as well as guidance documents for NIH staff to understand NIH's documented processes for assessing, monitoring, and enforcing compliance with foreign-interference-related policies. We interviewed officials from NIH's Office of Extramural Research (OER), HHS's Office of National Security, and three NIH institutes to obtain information on how NIH implements these processes. We also analyzed OER data from 2017 through 2025 to understand the sources and outcomes of allegations of potential foreign interference. To assess the reliability of these data, we performed electronic testing and reviewed relevant documentation, including written responses from NIH officials describing how the data were compiled. We determined that the data

were sufficiently reliable for the purpose of providing information about the volume and source of allegations and corresponding actions taken.

For the seven case studies, we judgmentally selected awards to illustrate how NIH's foreign interference policies operated in circumstances that could present elevated foreign interference risk. Of the approximately 141,000 scientific publications we identified that acknowledged NIH awards between January 1, 2024, and May 5, 2025, 634 (0.4 percent) had at least one coauthor affiliated with an institution on the Department of Defense (DOD) Fiscal Year 2023 Lists in Response to Section 1286 of the National Defense Authorization Act for Fiscal Year 2019 (Public Law 115-232), as amended (DOD list). According to DOD, institutions on the list engaged in activities that increased the likelihood that U.S.-funded research and development efforts could be misappropriated to the detriment of U.S. national security and economic competitiveness. Collaborations involving researchers affiliated with these institutions may therefore present elevated foreign interference risks.

We used this universe to judgmentally select five case study awards that were most recently active in fiscal year 2024 or 2025. We structured this selection to include awards administered by NIH institutes and centers of different sizes and to include publications associated with institutions in both China and Russia. We also added two awards identified by NIH to ensure that our review included awards for which NIH had imposed mitigations in response to foreign interference concerns. Both NIH-identified awards met our general selection criteria. This resulted in a final sample of seven awards. Although limited in scope, the case studies were selected to examine how NIH's processes operate under circumstances that may present heightened foreign interference risk, rather than to estimate the prevalence of such risks across NIH research awards.

For each of the seven case studies, we reviewed award documentation and progress reports and searched for publicly available information on

individuals identified as senior and key personnel.¹ We also used an online research security tool to identify current and past institutional affiliations reported in publications. We compared this information with disclosures contained in NIH award documentation and progress reports. In addition, we discussed each case with staff from the NIH institute that awarded the grant and with officials from NIH's Office of Policy for Extramural Research Administration (OPERA).

Third, to evaluate the degree of alignment between NIH's risk management program and GAO's enterprise risk management (ERM) practices and Fraud Risk Framework leading practices, we compared NIH's risk management documentation and practices with all six GAO ERM practices and with leading practices for the nine GAO Fraud Risk Framework overarching concepts we determined most relevant to our review.² We reviewed documentation describing NIH's risk management program, including NIH's Policy Manual and NIH's Enterprise Risk Management Guidebook. We also reviewed supporting documentation, interviewed NIH officials, and analyzed responses to our written questions. We assessed whether NIH's risk management program addressed the 15 key considerations of GAO's six ERM practices. We also assessed NIH's risk management program's alignment with leading practices for the nine GAO Fraud Risk Framework overarching concepts we determined most relevant to review. Alignment indicates that NIH's risk management program addresses, as applicable, the ERM key considerations and Fraud Risk Framework leading practices.

Fourth, to describe HHS's oversight of foreign human subjects research, we reviewed relevant regulations governing human subjects protections

¹NIH began enhanced efforts to address foreign interference in 2016, and its policies have evolved over time as federal requirements have evolved with, for example, the issuance of NSPM-33 and the passage of statutory provisions discussed above. For our case studies, the seven awards were active between 2020 and 2025. The policies and requirements that would have been applicable at any given point in the lifecycle of each of these grants may have evolved over the period of performance. However, requirements throughout that period consistently included the disclosure of foreign components, foreign financial interests, and certain foreign affiliations. For that reason, we looked at whether publicly available sources revealed undisclosed information in these areas for the awards and progress reports during this time in these case studies.

²GAO, *Enterprise Risk Management: Selected Agencies' Experiences Illustrate Good Practices in Managing Risk*, [GAO-17-63](#) (Washington, D.C.: Dec. 1, 2016). GAO, *A Framework for Managing Fraud Risks in Federal Programs*, [GAO-15-593SP](#) (Washington, D.C.: July 28, 2015).

and reviewed documents and interviewed officials from HHS's Office for Human Research Protections.

We conducted this performance audit from September 2024 to September 2026 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Case Studies of NIH's Implementation of Foreign-Interference-Related Requirements and Identification of Risks

We conducted case studies by reviewing seven National Institutes of Health (NIH) awards to illustrate how NIH's process for identifying and managing foreign interference risks operates in circumstances that may present heightened risk.¹ These case studies are illustrative and are not intended to be representative of NIH's award portfolio or the prevalence of foreign interference across research funded through NIH awards. We did not identify any clear violations of NIH regulations or policies. However, NIH officials told us that, based on the information GAO provided, they would likely initiate reviews for some of the personnel involved in these case studies.

For each case study below, we describe the potential indicators of foreign interference risk that GAO identified, including whether NIH's foreign interference risk review process identified those same indicators, and what NIH officials told us about why they did or did not think those risk indicators pointed to real risks associated with foreign interference in the award.

Case Study 1: Principal Investigator with Undisclosed Honorary Professorships

Background: A principal investigator (PI) at a U.S. university coauthored an article with a professor at a Chinese laboratory linked to a foreign talent recruitment program. The article acknowledged funding through an NIH award. Although the two individuals did not work together directly on the award acknowledged in the article, the professor at the Chinese laboratory had previously been a postdoctoral researcher in the PI's U.S. laboratory. After the former postdoctoral researcher left the U.S. laboratory, he and the U.S.-based PI collaborated on research related to the award acknowledged in the article.

Potential risk indicators: In its grant application, the U.S. university included a foreign component disclosure indicating that the U.S.-based PI and the former postdoctoral researcher would collaborate on work related to the award acknowledged in the coauthored article. However, the disclosure only listed the parent university of the laboratory linked to the

¹NIH began enhanced efforts to address foreign interference in 2016, and its policies have evolved over time as federal requirements have evolved with, for example, the issuance of NSPM-33 and the passage of statutory provisions discussed above. For our case studies, the seven awards were active between 2020 and 2025. The policies and requirements that would have been applicable at any given point in the life cycle of each of these grants may have evolved over the period of performance. However, requirements throughout that period consistently included the disclosure of foreign components, foreign financial interests, and certain foreign affiliations. For that reason, we looked at whether publicly available sources revealed undisclosed information in these areas for the awards and progress reports during this time in these case studies.

foreign talent recruitment program as the former postdoctoral researcher's affiliation.

In addition, publicly available information indicates that the U.S.-based PI held five honorary professorships that were not disclosed in the application submitted to NIH. Four of these professorships were at universities in China. One of the professorships was at the parent university of the laboratory where the former postdoctoral researcher worked. At the time when we selected our case studies, the university was not on the Department of Defense (DOD) Fiscal Year 2023 Lists Published in Response to Section 1286 of the National Defense Authorization Act for Fiscal Year 2019 (Public Law 115-232), as amended (DOD list).² However, the university was added to the updated version of the DOD list released in fiscal year 2024.

NIH risk review: NIH institute officials submitted the collaboration between the two researchers to the Department of State as a foreign component of the award and received clearance for it. The officials told us they also performed the required checks in NIH's awards management system and reviewed required application documents and annual progress reports for discrepancies that could indicate undisclosed foreign components or conflicts of interest or commitment.³ The institute officials said they found nothing concerning. NIH officials told us that, because they do not verify disclosures using sources other than required documents, they were not aware of the PI's honorary professorships or the incomplete disclosure of the former student's institutional affiliation. However, they noted that if the honorary professorships were no longer

²According to DOD, institutions on this list engaged in activities that increased the likelihood that U.S.-funded research and development efforts could be misappropriated to the detriment of U.S. national security and economic competitiveness.

³Conflicts of interest are situations "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." Conflicts of commitment are situations "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...." National Science and Technology Council, *Guidance for Implementing National Security Presidential Memorandum 33 (NSPM-33) on National Security Strategy for United States Government-Supported Research and Development* (Jan. 2022).

active, NIH policy would not have required their disclosure. GAO could not determine when the U.S.-based PI held those professorships. NIH officials also stated that, in their view, the scientific topic of the award did not pose risks to U.S. national security or economic competitiveness.

Summary: This case study illustrates how reliance on self-reported information in required documentation—without routine use of external information sources—may limit NIH's ability to identify incomplete disclosures that could signal elevated foreign interference risk.

Case Study 2: PI
Coauthorship with
Researchers on DOD's
List of Institutions
Engaging in Problematic
Activity

Background: A PI at a U.S. university coauthored a publication with five researchers affiliated with Chinese institutions on the DOD list. The publication acknowledges funding from an NIH award involving the PI.

Potential risk indicators: The PI coauthored a separate publication in 2020—which was not supported by the award but was published when the award was active—that gave his affiliation as a university hospital in China. The PI's U.S. institution did not disclose that affiliation to NIH in the documents we reviewed. GAO could not determine when the PI was affiliated with the hospital. If the affiliation was not current when the award was active, disclosure may not have been required.

NIH risk review: NIH officials told GAO they had reviewed required documents and found no discrepancies indicating undisclosed foreign affiliations or activities. NIH officials told us that the collaboration did not need to be reported as a foreign component because the publication's subject matter was unrelated to the award. They also noted that the PI had a history of acknowledging NIH awards on unrelated publications, perhaps because supplies purchased with funds from one award also benefited other projects.

Summary: This case study illustrates that not all publications coauthored with foreign researchers reflect a foreign component that must be disclosed to NIH.

Case Study 3: Former PI
Employed by an Institution
on DOD's List of
Institutions Engaging in
Problematic Activity

Background: A researcher completed a PhD in China and subsequently took a postdoctoral position at a U.S. university. While in that position, the researcher was appointed PI on a new NIH award to the university. Less than a year later, the researcher accepted a position at a laboratory in China and left the U.S. university. At the U.S. university's request, the researcher's former supervisor assumed the role of PI. After returning to China, the researcher and the new PI on the award were named as coauthors on a publication that acknowledged funding from the award.

Potential risk indicators: The researcher who served as the first PI on the award became employed by a laboratory in China on the DOD list. Our review found that prior to serving as PI, that researcher had publications listing his institutional affiliation as the laboratory in China where he took a position after serving as PI on the NIH award. However, the U.S. university did not disclose his affiliation with the laboratory either before or after the period when he was employed at the U.S. university, naming only the laboratory's parent university.

NIH risk review: NIH officials told us that disclosure of the researcher's prior affiliation with the laboratory in China may not have been required if he had no active affiliation with the laboratory at the time of application. They also told us that the coauthored publication likely did not reflect a foreign component requiring disclosure because the researcher had worked on the award while based in the United States. NIH officials reported reviewing required documents for discrepancies that could indicate undisclosed foreign activities or affiliations and told us they found none. However, NIH officials told us the information GAO identified was concerning and they would likely refer the case to the Office of Extramural Research (OER) for further review.

Summary: GAO did not identify any clear violations of NIH disclosure requirements in this case. Rather, the case illustrates how NIH policies do not require the disclosure of all a researcher's past affiliations.

Case Study 4: PI with Undisclosed Foreign Funding and Collaboration

Background: During a compliance review involving a researcher at a U.S. university, NIH learned that another researcher who served as PI on multiple NIH awards had received funding from Chinese sources that was not disclosed to NIH as required. In addition, the second researcher was engaged in a concerning scientific collaboration with a foreign national. NIH opened a compliance review into the second researcher.

NIH risk review: While the compliance review into the second researcher was ongoing, NIH did not allow that researcher to receive a salary or benefits from any NIH award. After discussing the undisclosed funding with the recipient institution, NIH concluded that it did not pose a foreign interference risk. Furthermore, the NIH program officer determined that foreign collaboration was not essential to the project and could be discontinued rather than reported as a foreign component. The university agreed to monitor the researcher's compliance with the requirement to discontinue the collaboration, and NIH removed the funding restriction. The researcher has since continued to work on NIH awards. GAO subsequently found that, since the conclusion of NIH's compliance

review, he has coauthored four publications with researchers affiliated with Chinese institutions on the DOD list. These publications do not necessarily indicate violations of NIH policies, but NIH officials told us they would review the researcher's current awards and activities to determine whether further review is warranted.

Summary: This case study illustrates that NIH takes steps to mitigate foreign interference risks while compliance reviews are ongoing. It also illustrates that NIH may determine through compliance reviews that violations of its foreign interference policies do not necessarily pose a risk of foreign interference.

Case Study 5: PI Subject to an NIH Compliance Investigation

Background: NIH learned that a U.S.-based professor who served as PI on multiple NIH awards was previously affiliated with a Chinese foundation and may have held funding from this foundation that was not disclosed to NIH as other support.

NIH risk review: OER opened a compliance review and requested information from the university to determine whether the professor's association with and funding from the Chinese foundation could have created a conflict of interest or commitment with his research funded through NIH awards. While the review was ongoing, OER restricted the PI's ability to draw salary and benefits from NIH awards. NIH officials told us that the PI did not receive NIH-awarded funds during the review period.

The university reported to NIH that the PI had appropriately disclosed all activities and funding sources since joining its faculty. Specifically, none of the evidence the university obtained suggested that the PI had an active relationship with the Chinese foundation during the time when he was employed at the university. They reported that his funding from the foundation had evidently ended before he joined the university's faculty. Since taking a position with the university, the PI had appropriately disclosed all his professional activities and sources of funding. Based on this information, NIH closed the investigation and lifted the restrictions.

Summary: This case illustrates NIH's use of compliance reviews and interim funding restrictions when potential disclosure violations are identified. It also illustrates that NIH may determine that a violation of its foreign interference policies does not pose a risk of foreign interference.

Case Study 6: PI
Collaboration with
Researcher Affiliated with
a Seven Sons of National
Defense University

Background: A U.S.-based PI coauthored a publication with five researchers affiliated with a Chinese Seven Sons of National Defense (Seven Sons) university.⁴

Potential risk indicators: GAO found no evidence that the PI failed to disclose any foreign activities or affiliations to NIH. However, one of the coauthors affiliated with the Seven Sons university was affiliated with the PI's U.S. university from 2015 to 2021, and it is possible that they had a substantial professional relationship.

NIH risk review: The U.S. university did not disclose any foreign components for the award acknowledged in the publication on which we based this case study. After we brought the publication to NIH's attention, program staff determined that the collaboration was not related to the research funded by the award. Thus, not only was disclosure of a foreign component not required, but the publication's authors should not have included the award in their acknowledgements. The NIH institute staff responsible for managing the grant found no cause for concern based on their review of the grant application, and NIH officials told us they did not believe there was any reason to be concerned about foreign interference in relation to the award associated with this case study.

Summary: This case study illustrates that collaborations resulting in coauthored publications may not meet the criteria to be considered a foreign component requiring disclosure, even if the publications acknowledge funding from an NIH award. It also illustrates that NIH does not verify whether coauthored publications reflect a foreign component unless potential foreign interference risks are brought to their attention.

Case Study 7: PI
Coauthorship with
Researcher at Russian
Institution on the DOD List

Background: A U.S.-based PI coauthored a publication with a researcher affiliated with a Russian institution on the DOD list. The publication acknowledged funding from an NIH award on which the PI served.

Potential risk indicators: GAO found no evidence that personnel receiving awarded funds failed to disclose foreign affiliations or activities,

⁴The universities designated as the "Seven Sons of National Defense" are administered with China's Ministry of Industry and Information Technology, and they are thought to have close ties with the People's Liberation Army. All seven universities are on the DOD List.

although one of the PI's disclosed affiliations was the parent institution of a DOD-listed institution.

NIH risk review: NIH officials told us that acknowledgement of an NIH award in a publication does not necessarily indicate that all coauthors had access to NIH-awarded funds or that the award supported the research underlying the publication. After we brought the publication from which we identified the grant to NIH's attention, program officials determined that the publication was not related to the funded research and should not have acknowledged the award. The officials did not consider the collaboration to constitute a foreign component requiring disclosure, noting that such acknowledgements may be intended to strengthen future applications.

Summary: This case study illustrates that not all publications coauthored with foreign researchers reflect a foreign component that must be disclosed to NIH.

Appendix III: Alignment Between NIH’s Risk Management Program and Selected GAO Fraud Risk Framework Overarching Concepts

Table 4 shows our detailed assessment of the alignment between the National Institutes of Health (NIH) risk management program and GAO Fraud Risk Framework leading practices, organized by selected overarching concepts.

Table 4: National Institutes of Health (NIH) Risk Management Program Alignment with Leading Practices of Selected GAO Fraud Risk Framework Overarching Concepts

Leading practices by overarching concept	NIH risk management program activities	Alignment
2.1 Plan regular fraud risk assessments that are tailored to the program		
Tailor the fraud risk assessment to the program	NIH has not conducted a fraud risk assessment for the extramural research program.	×
Plan to conduct fraud risk assessments at regular intervals and when there are changes to the program or operating environment, as assessing fraud risks is an iterative process	NIH officials told us they have not conducted a fraud risk assessment tailored to the extramural research program and have not planned to conduct such assessments at regular intervals. NIH officials told us the agency has no stand-alone fraud risk assessment. While NIH conducts annual risk inventory assessments that consider fraud, they are not a documented, program-specific assessment of fraud schemes, controls, and residual risks in the extramural research program.	×
Identify specific tools, methods, and sources for gathering information about fraud risks, including data on fraud schemes and trends from monitoring and detection activities	NIH uses multiple sources of information to identify and assess fraud-related risks, including annual risk inventory assessments, oversight reviews, investigative and allegation trends, internal control assessments, and subject-matter expertise from program integrity and grants oversight officials. NIH officials told us that the agency’s institutes and centers submit risk inventories during their annual risk inventory assessment process, and that this process includes consideration of risks related to fraud, waste, abuse, foreign influence, and research integrity as appropriate to their individual operational environments.	✓
Involve relevant stakeholders in the assessment process, including individuals responsible for the design and implementation of fraud controls	NIH identifies key stakeholders based on their responsibility for managing or influencing risks, subject-matter expertise, role in compliance, and impact on vulnerability to risks. Internal stakeholders include NIH institutes and centers leadership, grants management, enterprise risk management (ERM) officials, and compliance offices. External stakeholders include recipient institutions, oversight agencies, and advisory bodies. NIH officials stated that this broad identification approach ensures informed and effective risk management.	✓
2.2 Identify and assess risks to determine the program’s fraud risk profile		
Identify inherent fraud risks affecting the program	NIH also provided documentation of a fraud risk profile that identifies NIH’s top fraud risks, including foreign influence, and assigns them priority and risk levels based on the likelihood and impact. NIH officials told us that the fraud risk profile was informed by various sources of information such as consultations with subject matter experts, results from internal control reviews, the fraud risk assessment for NIH’s National Center for Advancing Translational Sciences Clinical and Translational Science Awards program, and lessons learned from compliance cases. NIH officials did not tell us that the fraud risk profile was informed by NIH’s annual risk inventory assessment process.	✓

Appendix III: Alignment Between NIH's Risk Management Program and Selected GAO Fraud Risk Framework Overarching Concepts

Assess the likelihood and impact of inherent fraud risks	NIH's annual risk inventory assessment incorporates assessment of the likelihood, impact, existing controls, and risk response decisions, including fraud risks. NIH officials told us their Office of Extramural Research (OER) fiscal year 2025 risk inventory assessment identified and assessed risks related to foreign influence and peer review integrity and included an impact and likelihood score related to the impact on the integrity of NIH-awarded research by undue outside and foreign involvement if researchers do not fully disclose foreign affiliations and funding information.	✓
Determine fraud risk tolerance	NIH's January 2025 fraud risk profile identifies risk priority and risk level based on the impact and likelihood of risk occurrence. However, NIH's fraud risk profile does not document the extramural research program's fraud risk tolerance or assess the suitability of existing controls and prioritize residual fraud risks for the extramural research program.	✗
Examine the suitability of existing fraud controls and prioritize residual fraud risks	NIH provided documentation of a fraud risk assessment conducted on their Clinical and Translational Science Awards Program, which identified a lack of fraud-focused internal controls. NIH's fraud risk profile does not document the extramural research program's fraud risk tolerance. Nor does it assess the suitability of existing controls or prioritize residual fraud risks for the extramural research program.	✗
Document the program's fraud risk profile	NIH has developed an agency-level fraud risk profile. NIH officials did not state that the fraud risk profile was informed by NIH's annual risk inventory, and the fraud risk profile does not include information regarding how the fraud risks were identified, assess the suitability of existing controls, or prioritize residual fraud risks for the extramural research program.	✓
3.1 Determine risk responses and document an antifraud strategy based on the fraud risk profile		
Use the fraud risk profile to help decide how to allocate resources to respond to residual fraud risks	NIH officials told us that NIH leadership uses the fraud risk profile as a data source for formulating risk-based budget analyses and defending resource allocations, but they did not tell us how fraud risks related to foreign interference inform resource allocation decisions to respond to that risk.	✗
Develop, document, and communicate an antifraud strategy to employees and stakeholders that describes the program's activities for preventing, detecting, and responding to fraud, as well as monitoring and evaluation	NIH has not developed, documented, or communicated an antifraud strategy, based on a fraud risk assessment, for the extramural research program that describes the program's activities for preventing, detecting, and responding to fraud risks identified, as well as monitoring and evaluation.	✗
Establish roles and responsibilities of those involved in fraud risk management activities, such as the antifraud entity and external parties responsible for fraud controls, and communicate the role of the Office of Inspector General to investigate potential fraud	NIH has established roles and responsibilities of those involved in fraud risk management activities. NIH's Policy Manual outlines a risk management chain of command involving NIH's Office of Management Assessment (OMA) which is to develop and maintain NIH's risk management program policy and guidance, provide risk management expertise and guidance, and conduct assessments and reviews. The risk management chain of command also includes NIH's Management and Budget Working Group, which serves as the risk management governance body, as well as risk management officers, risk management champions, and risk managers that have risk management roles and responsibilities. NIH's Enterprise Risk Management Guidebook states that OMA, in cooperation with the Department of Health and Human Services Office of the Inspector General (HHS OIG), is responsible for reviewing allegations of fraud, waste, and abuse. NIH officials told us that, as part of NIH's oversight functions, they communicate with the HHS OIG and law enforcement to share information related to ongoing cases and refer findings of potential fraud, waste, and abuse, as well as to obtain support on how to detect and prevent fraud.	✓

Appendix III: Alignment Between NIH's Risk Management Program and Selected GAO Fraud Risk Framework Overarching Concepts

Create timelines for implementing fraud risk management activities, as appropriate, including monitoring and evaluations	NIH's Enterprise Risk Management Guidebook requires the completion of an annual risk inventory reassessment, under which risks are reviewed for applicability. The guidebook also states that if shifts in the internal or external environments have changed the potential impact or likelihood of a risk occurring, NIH officials must review and make appropriate adjustments. NIH's Enterprise Risk Management Guidebook states that every institute and center and the Office of the Director is expected to continually monitor the operating effectiveness of its internal controls as part of its normal course of business. The guidebook also states that management's controls serve to mitigate the risk of fraud in federal programs and provide reasonable assurance that NIH's operational, reporting, and compliance objectives will be achieved.	✓
Demonstrate links to the highest internal and external residual fraud risks outlined in the fraud risk profile	NIH's fraud risk profile identifies major fraud risks and summarizes the controls NIH has in place in its grant application and management process. However, the fraud risk profile does not assess the suitability of existing controls or describe how those controls address the identified foreign influence fraud risk.	✓
Link antifraud efforts to other risk management activities, if any	NIH has not developed or documented an antifraud strategy, but NIH's Enterprise Risk Management Guidebook identifies fraud risk management as a specialized risk management focus area and states that continuous monitoring of risks is essential. NIH also links antifraud efforts to the grant application and monitoring process.	✓
3.2 Design and implement specific control activities to prevent and detect fraud		
Focus on fraud prevention over detection and response to avoid a "pay-and-chase" model, to the extent possible	NIH has not developed or documented an antifraud strategy based on a fraud risk assessment that would provide a basis for designing and evaluating specific control activities for the extramural research program. NIH officials stated that they conduct pre-award risk assessments for all awards and confirm compliance with NIH policies and standard terms and conditions prior to award. NIH officials stated that they communicate with external recipients to resolve or mitigate foreign interference risks before awards are made. NIH officials told us that the agency also allows NIH institutes and centers to negotiate restrictive terms to reduce risk.	✓
Consider the benefits and costs of control activities to address identified residual risks	According to NIH officials, NIH's Enterprise Risk Management Guidebook states that management should evaluate risk responses to consider the effect on the likelihood of occurrence and impact of a potential risk and the costs and benefits. NIH provided written descriptions of the benefits and costs associated with some of its activities to address fraud risks. However, these descriptions were not grounded in a documented assessment of the prevalence or potential impact of fraud risks, including foreign interference.	✗

Appendix III: Alignment Between NIH's Risk Management Program and Selected GAO Fraud Risk Framework Overarching Concepts

Design and implement the following control activities to prevent and detect fraud: (1) data analytics activities, (2) fraud awareness initiatives, (3) reporting mechanisms, (4) employee integrity activities	NIH did not provide evidence that it conducted data analytics activities called for in this leading practice. NIH collects data on the results of compliance cases stemming from allegations of potential foreign interference. However, these data provide limited insight into the prevalence of foreign interference in research supported by NIH. While NIH tracks allegations received and compliance review outcomes, it does not estimate the prevalence of foreign interference across NIH's award portfolio. NIH officials also told us they do not have data on foreign interference risk indicators identified prior to awards being made. NIH officials told us they provide training for grants and program staff that covers fraud. NIH officials stated that fraud awareness and risk identification competencies are supported through a combination of mandatory ethics training, risk management and internal control training, and operational grants management controls, such as pre-award screenings and disclosure reviews. NIH officials said this approach provides practical mechanisms to identify and elevate fraud allegations and risk factors. NIH's Grants Policy Statement states that individuals should report fraud, waste, or abuse related to NIH grants to their institution, the NIH Chief Grants Management Officer for the institute or center that awarded the grant, NIH's Division of Grants Compliance and Oversight, NIH's Office of Policy for Extramural Research Administration (OPERA), NIH's OER, and the HHS OIG. NIH publishes information on its public website about making foreign interference disclosures and anonymous reporting. NIH also provided an example of fraud awareness training that includes a variety of internal reporting mechanisms for staff to report fraud. NIH officials stated that employee integrity and screening processes follow federal and HHS-wide personnel and ethics frameworks. NIH's Division of Personnel Security website describes the new employee screening process and suitability criteria used to assess applicant integrity.	X
3.3 Develop a plan outlining how the program will respond to identified instances of fraud		
Develop a plan outlining how the program will respond to identified instances of fraud and ensure the response is prompt and consistently applied	NIH's Enterprise Risk Management Guidebook states that the agency is committed to responding promptly to instances of fraud, including working with appropriate parties to take proper disciplinary actions and implementing remedial measures to prevent recurrence. NIH's fraud risk profile identifies foreign interference as a fraud risk, and NIH's foreign interference website describes the agency's process for responding to allegations including referring cases that may rise to the level of civil or criminal fraud to HHS's OIG.	✓
Refer instances of potential fraud to the Office of Inspector General (OIG) or other appropriate parties, such as law enforcement entities or the Department of Justice, for further investigation	NIH officials also told us that OMA's Division of Program Integrity reviews allegations of fraud, waste, and abuse in cooperation with the HHS OIG and that NIH refers cases of potential foreign interference, such as those involving undisclosed foreign affiliations, to the HHS OIG and, when appropriate, to the Department of Justice (DOJ). An HHS OIG official told us that their Office of Investigations routinely receives referrals and information on potential violations of disclosure requirements from NIH, and they use that information strictly for law enforcement purposes as part of their broader grant fraud investigations.	✓

Appendix III: Alignment Between NIH's Risk Management Program and Selected GAO Fraud Risk Framework Overarching Concepts

3.4 Establish collaborative relationships with stakeholders and create incentives to help ensure effective implementation of the antifraud strategy

Establish collaborative relationships with internal and external stakeholders, including other offices within the agency; federal, state, and local agencies; private-sector partners; law-enforcement entities; and entities responsible for control activities to share information on fraud risks and emerging fraud schemes, and to share lessons learned related to fraud control activities, among other things	NIH has not developed or documented an antifraud strategy. NIH officials told us that they have established collaborative relationships with internal and external stakeholders to share information on fraud risks and emerging fraud schemes. NIH officials stated that they collaborate with other federal agencies, such as the DOJ, FBI, and the HHS OIG to investigate and address potential cases of fraud and foreign interference. NIH officials told us that this collaboration enhances the agency's ability to leverage expertise and resources to effectively combat fraud. NIH officials told us they engage with the broader research community to share best practices and lessons learned from fraud incidents and that they provide training and outreach to award recipients on fraud risks, red flags, and preventive measures. These activities help support awareness of fraud risk and compliance responsibilities.	✓
Collaborate and communicate with the OIG to improve understanding of fraud risks and align efforts to address fraud	NIH officials stated that they collaborated with HHS OIG to investigate and address potential cases of fraud and foreign interference.	✓
Create incentives for employees to manage risks and report fraud, including (1) creating performance metrics that assess fraud risk management efforts and employee integrity, particularly for managers, and (2) balancing fraud-specific performance metrics with other metrics related to employees' duties	NIH does not integrate fraud-related responsibilities into incentive structures or performance metrics for the extramural research program. NIH officials told us that managers are expected to identify and mitigate fraud risks within the ERM cycle, and their performance is assessed through various enterprise risk management practices. NIH officials told us that they invest in training and educating their staff on risk management principles and practices that help build a risk-aware culture within the agency and ensure that employees are equipped to identify and respond to risks effectively.	✗
Provide guidance and other support and create incentives to help external parties, including contractors, effectively carry out fraud risk management activities	NIH officials stated that they require training for award recipients that includes case studies to provide information on fraud risks, red flags, and preventive measures, which help ensure that everyone is aware of their role in preventing fraud. NIH officials stated they conduct outreach and education programs to inform the research community about the risks of foreign interference and the importance of adhering to disclosure requirements, which helps to build awareness and promote a culture of compliance.	✓

4.1 Conduct risk-based monitoring and evaluate all components of the fraud risk management framework

Monitor and evaluate the effectiveness of preventive activities, including fraud risk assessments and the antifraud strategy, as well as controls to detect fraud and response efforts	NIH has not monitored and evaluated the effectiveness of existing fraud prevention activities and controls. NIH also has not conducted a fraud risk assessment specific to the extramural research program or developed an antifraud strategy against which it can assess the effectiveness of the fraud prevention and response activities. NIH officials have not demonstrated that they monitor and evaluate the effectiveness of existing fraud prevention activities and controls, such as conducting site visits and unannounced examinations, which GAO's Fraud Risk Framework suggests.	✗
--	---	---

Appendix III: Alignment Between NIH's Risk Management Program and Selected GAO Fraud Risk Framework Overarching Concepts

Collect and analyze data, including data from reporting mechanisms and instances of detected fraud, for real-time monitoring of fraud trends and identification of potential control deficiencies	NIH officials told us they collect information on instances of fraud, including those related to foreign interference, and perform trend analysis. NIH officials told us that based on the insights from those data, they revise their policies and procedures to close gaps that have been exploited, such as updating their pre- and post-award disclosures relating to the biographical sketch and other support. NIH officials also stated that they implement stronger internal controls and safeguards in areas identified as high-risk, which may include more rigorous vetting, enhanced monitoring, and stricter enforcement of compliance requirements. While NIH tracks foreign interference allegations received and compliance review outcomes, it does not estimate the prevalence of foreign interference across NIH's award portfolio.	✓
Employ a risk-based approach to monitoring by considering internal and external factors that can influence the control environment, such as organizational changes and emerging risks	NIH has not conducted a fraud risk assessment for the extramural research program. Without this assessment, NIH may not have full awareness of the internal and external factors that can influence the control environment. Such an assessment would guide a risk-based monitoring approach for foreign interference and related fraud risks.	✗
Engage stakeholders responsible for specific fraud risk management activities in the monitoring and evaluation process	NIH officials told us that OER and OPERA monitor emerging foreign interference risks and communicate the status and resolution of compliance cases to NIH program and grants staff through the NIH Alert Module, the Research Misconduct Allegation Review System, and direct e-mail communication. NIH officials also said they hold monthly meetings with the HHS OIG to discuss ongoing cases and biweekly research integrity meetings to review research security procedures.	✓
4.2 Monitor and evaluate fraud risk management activities with a focus on measuring outcomes		
Measure outcomes, in addition to outputs, of fraud risk management activities	NIH provided data on the number of allegations of potential foreign interference that had at least one violation of NIH disclosure policies related to potential foreign interference. However, those data do not show how often NIH found actual conflicts of interest or commitment, scientific overlap, or misappropriation of federally funded research to the detriment of U.S. national security or economic competitiveness.	✗
In the absence of sufficient data, assess how well managers follow recommended "leading practices" for designing fraud risk management activities	NIH officials told us that managers are expected to identify and mitigate fraud risks within the ERM cycle, but NIH did not provide examples showing how managers are assessed against leading practices specific to fraud risk management, including the risk of foreign interference.	✗
4.3 Adapt fraud risk management activities and communicate the results of monitoring and evaluations		
Use the results of monitoring and evaluations to improve the design and implementation of fraud risk management activities	NIH does not monitor and evaluate the effectiveness of its fraud prevention activities and use those results to improve the design and implementation of fraud risk management activities.	✗
Use analysis of identified instances of fraud and fraud trends to improve fraud risk management activities, including prioritizing and taking corrective actions, as well as enhancing fraud awareness trainings	As discussed in overarching concept 4.1 above, NIH officials told us they collect information on instances of fraud, including those related to foreign interference, and perform trend analysis. NIH officials told us they revise their policies and procedures based on the insights from those data to close gaps that have been exploited and implement stronger internal controls and safeguards in areas identified as high risk.	✓

Appendix III: Alignment Between NIH's Risk Management Program and Selected GAO Fraud Risk Framework Overarching Concepts

Use results of investigations and prosecutions to enhance fraud prevention and detection	NIH officials stated that they incorporate lessons learned from investigations, enforcement actions, and publicly reported prosecutions related to foreign interference into policy updates and operational safeguards. According to NIH officials, patterns identified through investigations and allegations, such as undisclosed foreign affiliations, overlapping foreign funding, inappropriate data access, and disclosure failures, informed enhancements in several areas. Such enhancements include strengthened disclosure requirements, enhanced pre-award screening, prohibition on data access from countries of concern, enhanced monitoring requirements for data access, improved incident reporting and escalation, and incorporation of fraud risk drivers and residual risk prioritization insights from foreign interference cases into the fraud risk profile. NIH officials told us that lessons from prior cases informed refinements and expansions to NIH's risk-based screening processes, including review of foreign affiliations, overlap analysis, and SEAR-based risk indicators.	✓
Communicate results of monitoring and evaluations, including corrective actions taken, if any, to relevant stakeholders	Without conducting monitoring and evaluations of its fraud prevention activities, NIH does not have results, including corrective actions, to communicate with relevant stakeholders.	✗

✓ – Aligned
✗ – Not aligned

Source: GAO analysis of National Institutes of Health (NIH) information. | GAO-27-107848

Appendix IV: Comments from the Department of Health and Human Services



DEPARTMENT OF HEALTH & HUMAN SERVICES

OFFICE OF THE SECRETARY

Assistant Secretary for Legislation
Washington, DC 20201

September 11, 2026

Candice N. Wright
Director
Science, Technology Assessment,
and Analytics
U.S. Government Accountability Office
441 G Street NW
Washington, DC 20548

Dear Ms. Wright:

Attached are comments on the U.S. Government Accountability Office's (GAO) report entitled, **"RESEARCH SECURITY: NIH Action Needed to Strengthen Foreign Interference Risk Management"** (GAO-26-107848).

The Department appreciates the opportunity to review this report prior to publication.

Sincerely,

A handwritten signature in cursive script, reading "Gary Andres", is positioned above the typed name.

Gary Andres
Assistant Secretary for Legislation

Attachment

**GENERAL COMMENTS FROM THE DEPARTMENT OF HEALTH & HUMAN
SERVICES ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S DRAFT
REPORT – RESEARCH SECURITY: NIH ACTION NEEDED TO STRENGTHEN
FOREIGN INTERFERENCE RISK MANAGEMENT (GAO-26-107848)**

The Department of Health and Human Services (HHS) appreciates the opportunity to review and comment on the draft report.

GAO Recommendation 1

The Director of NIH should ensure that the risks of malign foreign talent recruitment programs are included as a topic to be covered in institution-provided training for covered individuals used to address research security training requirements in the Research and Development, Competition, and Innovation Act.

HHS Response

NIH concurs with GAO's recommendation and considers it closed, implemented. On August 17, 2026, NIH added an [FAQ](#) to the NIH Grants & Funding website clarifying the required content of institution-provided Research Security Training. The FAQ specifies that the training must address the risks of malign foreign talent recruitment programs, including the prohibition on NIH senior/key personnel participating in such programs. This requirement supplements the Research Security Training and certification requirements implemented through NIH [GPS 8.4.1.11](#), for applications submitted for due dates on or after May 25, 2026.

GAO Recommendation 2

The Director of NIH should conduct and document, at regular intervals and in accordance with GAO's Fraud Risk Framework, a fraud risk assessment tailored to NIH's extramural research program that considers risks related to foreign interference.

HHS Response

NIH concurs with GAO's recommendation. NIH will incorporate applicable elements of GAO's Fraud Risk Framework into its existing risk management and internal control processes. NIH will strengthen consideration of fraud risk within its annual risk inventory assessment evaluations and will periodically conduct and document a fraud risk assessment tailored to the extramural research program that considers foreign interference.

Appendix V: GAO Contact and Staff Acknowledgments

GAO Contact

Candice N. Wright, WrightC@gao.gov

Staff Acknowledgments

In addition to the contact named above, Terrance N. Horner Jr. (Assistant Director), Mason Thorpe Calhoun (Analyst-in-Charge), Karen M. Bryson, Caroline Christopher, Rachael Johnson, Mark Kuykendall, Toby Lister, Amy Pereira, Joe Rando, and Andrew Stavisky made key contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its [website](#) newly released reports, testimony, and correspondence. You can also [subscribe](#) to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, <https://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on [X](#), [LinkedIn](#), [Instagram](#), and [YouTube](#).
Subscribe to our [Email Updates](#). Listen to our [Podcasts](#).
Visit GAO on the web at <https://www.gao.gov>.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: <https://www.gao.gov/about/what-gao-does/fraudnet>

Automated answering system: (800) 424-5454

Media Relations

Sarah Kaczmarek, Managing Director, Media@gao.gov

Congressional Relations

David A. Powner, Acting Managing Director, CongRel@gao.gov

General Inquiries

<https://www.gao.gov/about/contact-us>



Please Print on Recycled Paper.