United States Government Accountability Office

Report to Congressional Committees

December 2023

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

Strengthening Disclosure Requirements and Assessing Training Could Improve Research Security

GAO-24-106074

GAO Highlights

Highlights of GAO-24-106074, a report to Congressional Committees

December 2023

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

Strengthening Disclosure Requirements and Assessing Training Could Improve Research Security

Why GAO Did This Study

Countries of concern pose security risks to U.S. research and innovation. Such countries have sought to access information through collaborative research efforts. NIST employees regularly collaborate with outside researchers from academia or private-sector companies. The Research and Development, Competition, and Innovation Act includes a provision for GAO to review NIST's research security program.

This report examines, among other things, NIST's efforts to (1) meet federal disclosure requirements for intramural and extramural researchers, (2) collect and review disclosures from foreign national associates and domestic associates, and (3) align its security training with selected leading training practices.

GAO reviewed NIST's information and available data on identified risks, research security policies, and procedures, and interviewed agency officials. GAO also compared NIST's policies and practices against selected federal requirements and leading practices on training.

What GAO Recommends

GAO is making three recommendations: one to OSTP on issuing timely research security guidance; and two to NIST on strengthening disclosure requirements for domestic associates and evaluating its training program. OSTP and NIST agreed with the recommendations.

View GAO-24-106074. For more information, contact Candice Wright at (202) 512-6888 or WrightC@gao.gov.

What GAO Found

Researchers employed at the National Institute of Standards and Technology (NIST) collaborate on research projects with about 2,500 domestic and foreign national researchers (known as "associates") each year. The agency also awards grants and cooperative agreements under which extramural (i.e., external) researchers carry out research. While such collaborations are intended to benefit NIST, they may pose security risks. NIST has taken steps to help ensure research security by requiring researchers to disclose information that can help it determine whether they have potential conflicts of interest or commitment.

However, at the time of our review, NIST had not fully implemented federal disclosure requirements as the agency was waiting for the Office of Science and Technology Policy (OSTP) to issue government-wide guidance in two areas:

- uniform disclosure forms for extramural researchers, and
- guidelines on foreign talent recruitment programs, which seek to recruit researchers—sometimes with malign intent.

According to NIST officials, OSTP's delays in issuing the forms and guidelines have delayed NIST's collection of certain disclosures. Without these disclosures, NIST is missing key information—such as domestic researchers' participation in foreign talent recruitment programs—that could help it address research security risks.

Separately, NIST requires fewer disclosures from domestic associates than from foreign national associates. Officials said the agency primarily focuses on risks posed by foreign national associates and by certain countries of concern. However, domestic researchers can also have concerning affiliations with foreign entities. By not requiring domestic associates to disclose the same information as foreign national associates, NIST is missing opportunities to assess and mitigate risks.

Information That NIST Requires Associates to Disclose

Type of researcher	Organizational affiliations/ employment	Positions/ appointments	Participation in foreign talent recruitment programs	Current and pending research support
Foreign national associate	✓	✓	✓	✓
Domestic associate	✓	-	-	-

Source: GAO analysis of the National Institute of Standards and Technology (NIST) information. | GAO-24-106074

NIST and Commerce also help ensure research security by training researchers. The training program generally aligns with most selected leading training practices. However, because they do not evaluate the program's effectiveness, the agencies are limited in their ability to identify opportunities for improvement. For example, NIST employees told GAO that NIST could provide more examples of risks that employees may encounter. Collecting and analyzing such feedback could help strengthen the agency's training and improve research security.

Contents

Tables

Figures

Abbreviations

CITADEL	Counterintelligence Threat Actor Discovery and Exploitation Landscape
FBI	Federal Bureau of Investigation
NCSC	National Counterintelligence and Security Center
NIST	National Institute of Standards and Technology
NSPM-33	National Security Presidential Memorandum 33
ODNI	Office of the Director of National Intelligence
OIG	Office of Inspector General
OSTP	Office of Science and Technology Policy
R&D	research and development
section 223	section 223 of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

December 14, 2023

Congressional Committees

An open and collaborative research and development (R&D) enterprise supports U.S. innovation, science and technology leadership, economic competitiveness, and national security.[1] However, some foreign governments are working vigorously to acquire U.S. research and technology, through both legal and illicit means, according to the Office of Science and Technology Policy (OSTP).[2] Protecting federally funded research from such threats is of critical importance.

Within the Department of Commerce, the National Institute of Standards and Technology (NIST) promotes U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve quality of life. NIST employees who conduct research supported by the agency—known as intramural researchers—work on emerging technologies—such as quantum computing—that could have significant economic and national security implications. In fiscal year 2022, the agency employed nearly 1,400 intramural researchers.

To meet the agency's mission, intramural researchers sometimes collaborate with researchers from industry and academia at NIST facilities. These researchers are not NIST employees and may be foreign nationals—foreign national associates—or U.S. citizens—domestic

[1]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).

[2]National Science and Technology Council, Subcommittee on Research Security, Joint Committee on the Research Environment, *Guidance for Implementing National Security Presidential Memorandum-33 (NSPM-33) on National Security Strategy for the United States Government-Supported Research and Development*, (Jan. 2022).

associates.[3] On average, NIST researchers have collaborated with about 800 foreign national associates and about 1,700 domestic associates each fiscal year since 2013. Associates may collaborate with NIST over a period of weeks, months, or years. The collaborations are intended to benefit both the agency and the associate. However, such collaborations may also pose research security risks.

NIST also awards grants and cooperative agreements to aid U.S. industry through research and measurement services.[4] For example, NIST's Measurement Science and Engineering Research Grant Programs awards grants in broad areas including bioscience, advanced manufacturing, and high-speed electronics.[5] The research conducted under these grants is carried out by extramural researchers. For the purposes of this report, we define extramural researchers to mean individuals who develop or execute a research and development project proposed to be carried out under a research and development award from a federal research agency. These individuals are not agency employees and must contribute in a substantive, meaningful way to the project, including as a principal investigator or as other senior/key personnel, and are designated as a covered individuals by the agency.

The Research and Development, Competition, and Innovation Act, contained in what is commonly referred to as the CHIPS and Science Act of 2022, includes a provision for GAO to review NIST's research security

[3]Foreign national associates include foreign nationals (non-U.S. citizens), lawful permanent residents, and protected persons, who are not NIST employees. A domestic associate is a non-employee who is a U.S. citizen, comes to a NIST campus or uses NIST information technology resources, and is either working in a lab for any period of time or will be on campus for more than 10 working days. While NIST associates include both research and non-research associates—such as cafeteria workers—for the purposes of this report, the term "associates" refers to associates engaged in research activities at NIST. See NIST, *NIST Foreign National Associates Programs*, NIST O1402.00 (May 2021); NIST, *Domestic Associates Program*, NIST O1401.00 (Oct. 2019).

[4]A grant is the legal instrument reflecting a relationship between the agency and a recipient when: (a) the principal purpose of the relationship is to transfer anything of value in order to accomplish a public purpose of support or stimulation authorized by federal statute; and not to acquire property or services for the awarding agency's direct benefit or use and (b) no substantial involvement is anticipated by the awarding agency during the performance of the contemplated activity. A cooperative agreement differs from a grant in that substantial involvement (e.g., collaboration, participation, or intervention by the agency in the management of the project) is anticipated by the awarding agency. Unless otherwise specified, we use the term "grant" throughout this report to mean both grants and cooperative agreements. See, 2 C.F.R. § 200.1.

[5]NIST, *Notice of Funding Opportunity (NOFO) Measurement Science and Engineering (MSE) Research Grants Programs*, 2021-NIST-MSE-01 (May 2022).

program.[6] This report examines NIST's efforts to (1) meet federal disclosure requirements for intramural and extramural researchers; (2) collect and review disclosures from foreign national associates and domestic associates; (3) identify, address, and collaborate on research security risks; and (4) align its security training with selected leading training practices.

To determine the extent to which NIST is meeting federal disclosure requirements for intramural and extramural researchers, we reviewed relevant statutes and guidance, NIST policies, and conducted interviews with cognizant officials. We compared NIST's efforts to collect disclosures from intramural and extramural researchers with relevant statutes and federal guidance, including the National Security Presidential Memorandum 33 (NSPM-33) and section 223 of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (section 223).[7]

To determine the extent to which NIST collects and reviews disclosures from foreign national associates and domestic associates, we reviewed Commerce's and NIST's policies and procedures and discussed them with cognizant officials. We reviewed the foreign national associate case review forms pertaining to the 10 applicants that the agency identified as medium or high risk during the time period from fiscal years 2020 through fiscal year 2022.

To determine the extent to which NIST has identified and addressed risks to research security, we reviewed written responses and interviewed cognizant NIST and Commerce officials to discuss the types of risks identified and their responses to them. We also reviewed agency and departmental policies and procedures related to research security practices, including those for foreign access management. We also compared NIST's collaborative efforts with the eight leading practices for interagency collaboration discussed in GAO-23-105520 *Government*

[6]Research and Development, Competition, and Innovation Act, Pub. L. No. 117-167, div. B, tit. II, subt. C, § 10247, 136 Stat. 1366, 1494-95 (2022).

[7]The White House, NSPM-33; William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No 116–283, div. A, tit. II, subt. B, § 223, 134 Stat. 3388, 3470-72 (codified at 42 U.S.C. § 6605).

Performance Management: Leading Practices to Enhance Interagency Collaboration and Address Crosscutting Challenges.[8]

To determine the extent to which NIST and Commerce's research security-related training courses align with selected leading practices, we reviewed training documents used by NIST and conducted interviews with cognizant NIST and Commerce officials. We also conducted semi-structured interviews with a non-generalizable sample of 12 NIST researchers who served as sponsors of foreign national associates, domestic associates, or both to obtain their views on the training courses. We compared NIST's training efforts against selected leading practices in *Human Capital: A Guide for Assessing Strategic Training and Development Efforts in the Federal Government*.[9] For more information on our objectives, scope, and methodology, see appendix I.

We conducted this performance audit from May 2022 to December 2023 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

Researchers Supported by NIST

To conduct its research, NIST employs and supports its own researchers, awards grants under which extramural researchers carry out research, and collaborates with foreign national associates and domestic associates (see table 1).

[8]GAO, *Government Performance Management: Leading Practices to Enhance Interagency Collaboration and Address Crosscutting Challenges*, GAO-23-105520 (Washington, D.C.: May 2023).

[9]GAO, *Human Capital: A Guide for Assessing Strategic Training and Development Efforts in the Federal Government*, GAO-04-546G (Mar. 2004).

Table 1: Kinds of Researchers Supported by the National Institute of Standards and Technology (NIST)

Category	Employee status	Description
Intramural researcher	NIST employee	NIST employee who conducts research supported by the agency.
NIST sponsor of foreign national or domestic associate	NIST employee	NIST employee who is responsible for the security oversight of the assigned associate.
Extramural researcher[a]	Non-NIST employee	Individuals who develop or execute a research and development project proposed to be carried out under a research and development award from a federal research agency. These individuals must contribute in a substantive, meaningful way to the project, including as a principal investigator and other senior/key personnel, and are designated as a covered individuals by the agency.
Domestic associate	Non-NIST employee	A non-employee who is a U.S. citizen, comes to a NIST campus or uses NIST information technology resources, and is either working in a lab for any period of time or will be on campus for more than 10 days.
Foreign national associate	Non-NIST employee	Any foreign nationals (non-U.S. citizen), lawful permanent residents, and protected persons, who are not NIST employees.[b] They may be an employee of a foreign government agency; an employee of federal, state, or local government agency; an employee of a for-profit company or non-profit organization (including a college or university); a postgraduate researcher, graduate or undergraduate student; a contractor; personnel under a grant or cooperative agreement; or self-employed.
NIST further characterizes both foreign national associates and domestic associates into types by the relationship they have with NIST programs:		
	Research and Science	Associate who is technically qualified, collaborates with NIST on research projects of mutual interest, or works under a federal funding agreement with a U.S. university or U.S. company.
	Technical	Associate who is technically qualified, collaborates with NIST on technical activities of mutual interest, or works under a federal funding agreement with a U.S. university or U.S. company. This category includes those individuals who provide on-site technical computer services (e.g., programming, network or systems administration) or conduct market research, strategic planning, and other consulting services.
	Special Programs	Associate who is a technically qualified student who participates in the Summer Undergraduate Research Fellowships Program, the Professional Research Experience Program, or an individual brought in for special NIST training.

Source: GAO analysis of NIST information. | GAO-24-106074

[a]Extramural researchers include "covered individuals" as defined by section 223 of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (Pub. L. No. 116-283).

[b]A protected person is a non-U.S. citizen granted asylum under the Immigration and Naturalization Act (see 8 U.S.C. § 1324b(a)(3)).

Research-Security-Related Statutes and Guidance

Various federal statutes and guidance address how agencies should collect information from researchers that could be used to determine whether researchers have potential conflicts of interest and commitment, including whether they are participating in foreign talent recruitment programs. These terms are defined as follows:

- **Conflict of interest:** The researcher, or researcher'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.[10]
- **Conflict of commitment:** The researcher accepts or incurs conflicting obligations between or among multiple employers or other entities.[11]
- **Foreign talent recruitment program:** A foreign talent recruitment program is an effort organized, managed, or funded by a foreign government, or a foreign government entity, to recruit science and technology professionals or students (regardless of citizenship or national origin, or whether having a full-time or part-time position). Many programs use legitimate, transparent mechanisms of talent recruitment, including research fellowships, student and scholar exchanges, and grants. Others operate with the intent to import or otherwise acquire from abroad, sometimes through illicit means, proprietary technology or software, unpublished data or methods, or intellectual property to advance the military modernization goals or economic goals of a foreign government.[12]

Table 2 provides an overview of these disclosure requirements and more detailed information on each source of federal requirements follow. Neither domestic associates nor foreign national associates are expressly covered under these disclosure requirements.

[10]Joint Committee on the Research Environment, *Guidance for Implementing NSPM-33*.

[11]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 efforts to improperly share information with, or withhold information from, an employer or research agency, can also threaten research security and integrity, and are an element of the broader concept of conflicts of commitment used in this report. Joint Committee on the Research Environment, *Guidance for Implementing NSPM-33*.

[12]Joint Committee on the Research Environment, *Guidance for Implementing NSPM-33*.

Table 2: Overview of Federal Disclosure Requirements

Source of federal requirement	National Security Presidential Memorandum 33 (NSPM-33) and implementation guidance[a]	Section 223 of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021[b]	Sections 10631 and 10632 of the CHIPS and Science Act of 2022[c]
Who is covered	Extramural researchers, intramural researchers, and federal program officers[d]	Extramural researchers[e]	Extramural researchers[e]
Organizational affiliations/employment	✓	-	-
Positions/appointments	✓	-	-
Participation in foreign talent recruitment programs	✓	-	✓
Current and pending research support (monetary and non-monetary)	✓	✓	-

Legend:

✓= requires disclosure

- = does not require disclosure

Source: GAO analysis of federal disclosure requirements for researchers receiving federal funds. | GAO-24-106074

[a]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); Office of Science and Technology Policy, Guidance for Implementing NSPM-33 on National Security Strategy for the United States Government-supported Research and Development, (Jan. 2022).

[b]William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No 116–283, div. A, tit. II, subt. B, § 223, 134 Stat. 3388, 3470-72 (codified at 42 U.S.C. § 6605).

[c]Research and Development, Competition, and Innovation Act, Pub. L. No. 117-167, 136 Stat. 1366, 1664-66, div. B, tit. VI, subt. D, §§ 10631, 10632, 136 Stat. 1366, 1664-66, (2022).

[d]NSPM-33 and its implementation guidance also include requirements for peer reviewers and advisory committee/panel members to disclose organizational affiliations/ employment, positions/ appointments, and participation in foreign talent recruitment programs.

[e]For the purposes of this report, extramural researchers include individuals who develop or execute a research and development project proposed to be carried out under a research and development award from a federal research agency. These individuals are not agency employees and must contribute in a substantive, meaningful way to the project, including as a principal investigator or other senior/key personnel, and who are designated as a covered individuals by the agency.

These statutes and guidance documents are:

- **NSPM-33 and implementation guidance:**[13] NSPM-33 directs action to strengthen protections of U.S.-government-supported R&D against foreign government interference and exploitation. This includes requiring R&D funding agencies to require certain participants in the

[13]The White House, NSPM-33.

U.S. R&D enterprise to provide disclosures of information that can reveal potential conflicts of interest and conflicts of commitment. Participants in the R&D enterprise include principal investigators and other senior or key personnel seeking or receiving federal funding, intramural researchers, and program officials.[14] In January 2022, OSTP provided guidance to federal departments and agencies regarding their implementation of NSPM-33.[15] Among other things, the guidance states that agencies should integrate implementation of NSPM-33 requirements with implementation of applicable statutes, including section 223. Figure 1 provides an overview of disclosure requirements from NSPM-33.

Figure 1: Overview of Disclosure Requirements for Participants in the Research and Development Enterprise as Specified in National Security Presidential Memorandum-33 (NSPM-33) and Implementation Guidance

Source: GAO analysis of NSPM-33. | GAO−24−106074

Note: With the exception of current and pending research support, NSPM-33 requires disclosures of the same information from peer reviewers and advisory committee panel members.

[14]Senior or key personnel include an individual who (a) contributes in a substantive, meaningful way to the scientific development or execution of a R&D project proposed to be carried out with a R&D award from a federal research agency; and (b) is designated as a covered individual by the federal research agency concerned. Consistent with NSPM-33, this means principal investigators and other senior or key personnel seeking or receiving federal R&D funding (i.e., extramural funding) and researchers at federal agency laboratories and facilities (i.e., intramural researchers, whether or not federally employed), including government-owned, contractor-operated laboratories and facilities. Joint Committee on the Research Environment, *Guidance for Implementing NSPM-33*.

[15]Joint Committee on the Research Environment, *Guidance for Implementing NSPM-33*.

- **Section 223:**[16] Section 223, among other things, requires each covered individual listed on an application for an R&D award from a federal research agency to disclose the amount, type, and source of all current and pending research support (both monetary and non-monetary) received by or expected to be received by the individual at the time of disclosure and certify that the disclosure is current, accurate, and complete as part of the application for an R&D award.[17] In addition, covered individuals must agree to update disclosures, if requested by the agency before the award is made and during the term of the award. The entity applying for the award must also certify that each covered individual who is employed by the entity and listed on the application has been made aware of these requirements. Figure 2 provides an overview of section 223 disclosure requirements.

[16]William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No 116–283, div. A, tit. II, subt. B, § 223, 134 Stat. 3388, 3470-72 (codified at 42 U.S.C. § 6605).

[17]Section 223 defines a "covered individual" as an individual who—"(A) contributes in a substantive, meaningful way to the scientific development or execution of a R&D project proposed to be carried out with a R&D award from a Federal research agency; and (B) is designated as a covered individual by the Federal research agency concerned." The term current and pending research support is defined as all resources made available, or expected to be made available, to an individual in support of the individual's research and development efforts regardless of whether the source of the resource is foreign or domestic; whether the resource is made available through the entity applying for a research and development award or directly to the individual; or whether the resource has monetary value. This includes in-kind contributions requiring a commitment of time and directly supporting the individual's research and development efforts, such as the provision of office or laboratory space, equipment, supplies, employees, or students. Pub. L. No 116–283, div. D, tit. II, subt. B, § 223(d)(1)-(2), 134 Stat. at 3471-72 (codified at 42 U.S.C. § 6605).

Figure 2: Overview of Current and Pending Research Support Disclosure Requirements for Covered Individuals Specified in Section 223

Source: GAO analysis of section 223 of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021. | GAO−24−106074

- **CHIPS and Science Act of 2022:**[18] Section 10631 of the act requires federal research agencies to, no later than August 9, 2023, issue policies that, among other things, prohibit agency personnel from participating in foreign talent recruitment programs, and prohibit federal research agencies from making R&D awards for any proposal in which a covered individual is participating in a malign foreign talent recruitment program. In addition, covered individuals will be required, as part of section 223 disclosure requirements, to disclose if they are

[18]Research and Development, Competition, and Innovation Act, Pub. L. No. 117-167, div. B, 136 Stat. 1366 (2022).

a party to a foreign talent recruitment program.[19] Further, pursuant to section 10632, not later than August 9, 2024, federal research agencies are to require that covered individuals in proposals for R&D awards certify, at the time of award and annually thereafter, they are not participating in malign foreign talent recruitment programs.[20] OSTP officials told us that they are planning to issue guidance regarding both research requirements, to support existing efforts at federal research agencies.

Policies for Reviewing and Sponsoring Foreign National and Domestic Associates

Commerce and NIST have developed a range of processes and policies that govern collaboration with foreign national associates and domestic associates. NIST has separate policies and procedures related to reviewing and hosting each type of associate.

Foreign national associates. NIST's International and Academic Affairs Office manages the foreign national associates program. Commerce's *Foreign Access Management Program* sets forth departmental policies and procedures for foreign national associates' access to the department's facilities, resources, and activities.[21] NIST implements Commerce's Foreign Access Management Program through its own policies and procedures. For example, it established a research security review program in January 2020 for assessing each foreign national associate's disclosures and information from other sources. The NIST Research Security Review team reviews each associate prior to initial

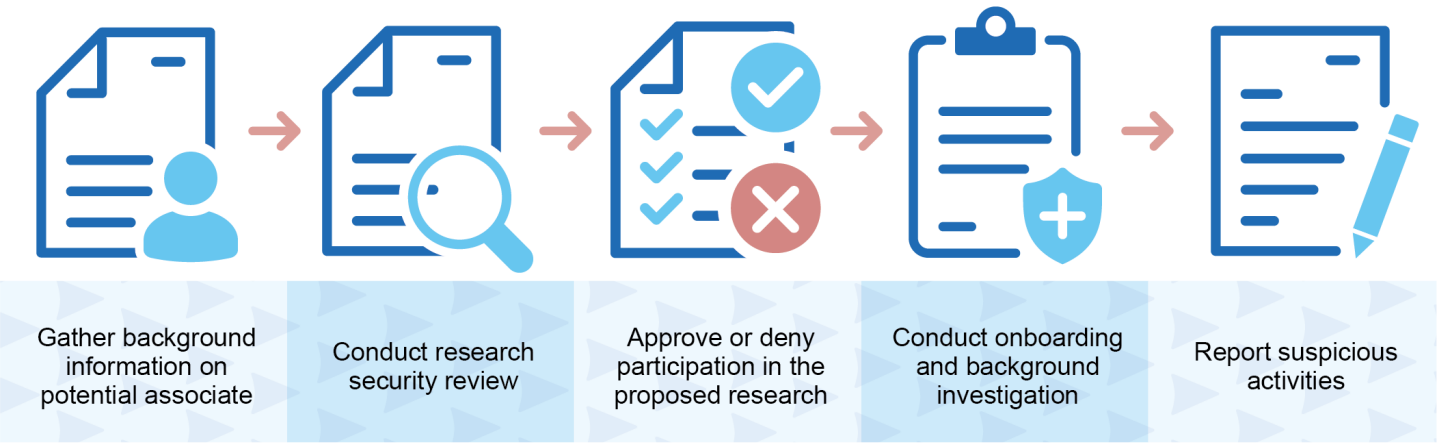
[19]Research and Development, Competition, and Innovation Act, Pub. L. No. 117-167, div. B, tit. VI, subt. D, § 10631,136 Stat. at 1664-65 (2022). This section also directs OSTP, in coordination with the interagency working group established under section 1746 of the National Defense Authorization Act for Fiscal Year 2020 (Public Law 116–92), to issue uniform guidelines for federal research agencies that are to include these requirements within 6 months of enactment of the act. Federal research agencies are to issue policies utilizing these guideline within 1 year of the act's enactment. As of December 2023, OSTP has not yet issued uniform guidelines.

[20]Research and Development, Competition, and Innovation Act, Pub. L. No. 117-167, div. B, tit. VI, subt. D, § 10632,136 Stat. at 1665-6 (2022). In addition, the entity that is applying for an R&D award from a federal research agency must certify that each covered individual employed by the entity has been made aware of and complied with this certification requirement.

[21]Department of Commerce, *Foreign Access Management Program*, DAO 207-12 (June 2021).

acceptance and annually thereafter. NIST's process for reviewing and hosting foreign national associates is summarized below (see fig.3).[22]

Figure 3: Summary of NIST's Process for Reviewing and Hosting Foreign National Associates



Source: GAO analysis of National Institute of Standards and Technology (NIST) information (analysis); Designer/stock.adobe.com (images). | GAO−24−106074

Domestic associates. NIST's Technology Partnerships Office manages the domestic associates program. NIST's process for reviewing and hosting domestic associates is the same as that for foreign national associates, with one key exception: NIST does not conduct research security reviews of domestic associates. Instead, the agency relies on other mechanisms—including standard background checks, access controls, and research security training courses for its employees to ensure research security.

Additionally, foreign national associates and domestic associates work under the oversight of a designated NIST employee, known as a sponsor. Commerce and NIST policies define responsibilities for sponsors.[23] Among other things, NIST sponsors must:

[22]Foreign national associates must not be citizens of countries which have been designated as State Sponsors of Terrorism by the Department of State unless they are U.S. Lawful Permanent Residents/Green Card holders. As of May 2023, four countries have been designated as State Sponsors of Terrorism: Cuba, North Korea, Iran, and Syria.

[23]See Department of Commerce, *Foreign Access Management Program*, DAO 207-12 (June 2021); NIST, *NIST Foreign National Associates Programs*. NIST also assigns sponsors for domestic associates, who are responsible for their assigned associate. NIST, *Domestic Associates Program*, NIST O1401.00 (Oct. 2019).

- successfully complete a counterintelligence awareness training before serving as a sponsor and annually thereafter to maintain eligibility;
- take reasonable steps to ensure the associate is given access only to data and facilities needed to perform their research; and
- immediately report suspicious activities or anomalies involving associates.

For more information about background checks conducted for foreign national associates and domestic associates, see appendix II.

Research Security Risks and Related NIST Activities

NIST defines foreign threats and undue foreign influence as broad risks to national security, economic security, and intellectual property.[24] The agency focuses primarily on risks posed by countries of concern.[25] According to NIST, technologies targeted by countries of concern include quantum computing, 5G, and artificial intelligence. Emerging technologies—particularly in fields such as artificial intelligence—are proliferating faster than agencies can prepare for, which can lead to the development of additional threats to U.S. interests, according to the Office of the Director of National Intelligence (ODNI).[26] Many of these technologies may have both military and commercial applications.[27] Table 3 describes a range of agency activities that are subject to threats from countries of concern.

[24]According to training slides on operations security issued by the Office of the Director of National Intelligence in October 2022, a threat is as an adversary with the intent and capabilities to compromise an agency's mission or sensitive activities. A vulnerability is a weakness that an adversary can exploit to get an agency's critical information. Risk is the probability that an adversary will compromise the agency's critical information or exploit a vulnerability and the potential impact of the adversary's success.

[25]See 15 U.S.C. § 4651(7), which defines "foreign country of concern" as (A) a country that is a covered nation (as defined in 10 U.S.C. § 4872(d)); and (B) any country that the Secretary of Commerce, in consultation with the Secretary of Defense, the Secretary of State, and the Director of National Intelligence, determines to be engaged in conduct that is detrimental to the national security or foreign policy of the United States.

[26]See ODNI, *Annual Threat Assessment of the U.S. Intelligence Community*, (Feb. 2023).

[27]According to the Department of State, "military-civil fusion" is an aggressive strategy used by the Chinese government to reorganize the Chinese science and technology enterprise to ensure that innovations simultaneously advance economic and military development. The Chinese government uses this strategy through legal and illicit means, including investment in private industries, talent recruitment programs, directing academic and research collaboration for military gain, forced technology transfer, intelligence gathering, and outright theft. Department of State, *Military-Civil Fusion and the People's Republic of China.*

Table 3: Examples of NIST Activities Potentially Vulnerable to Threats from Countries of Concern

Activity	Description	Possible threats
Research collaboration with foreign national associates	NIST hosts foreign researchers to collaborate on projects.	Foreign national associates might share proprietary technology, unpublished research results, or intellectual property.
Foreign travel requests	NIST staff undertake travel to present at conferences and conduct site visits at peer institutions.	Foreign researchers participating in conferences might seek to uncover sensitive or high-risk information.
Assistance-in-kind offers	Foreign entities offer non-monetary assistance such as providing accommodations for NIST visitors.	Foreign talent recruitment programs might try to recruit NIST staff to gain access to sensitive information.[a]
Measurement services requests	NIST services help researchers meet scientific standards such as calibrations of instruments.	Countries of concern might use NIST services to advance military and commercial applications for their own military and economic gain.
• Standard reference materials	NIST creates uniform and highly accurate samples of a variety of substances, such as cast iron, paint, or peanut butter.	
• Standard reference data	NIST makes highly accurate and precise measurements of important scientific quantities, such as the tensile strength of steel.	
• Standard reference instruments	NIST builds highly accurate measurement devices.	
• Calibrations	NIST helps other entities tune and fix their scientific tools.	

Source: GAO analysis of National Institute of Standards and Technology (NIST) information. | GAO-24-106074

[a]A foreign talent recruitment program is an effort organized, managed, or funded by a foreign government, or a foreign government entity, to recruit science and technology professionals or students (regardless of citizenship or national origin, or whether having a full-time or part-time position). National Science and Technology Council, Subcommittee on Research Security, Joint Committee on the Research Environment, Guidance for Implementing National Security Presidential Memorandum-33 (NSPM-33) on National Security Strategy for the United States Government-Supported Research and Development, (Jan. 2022).

Research Security Training

NIST and Commerce offer a range of training courses on research security. Among the four primary research security training courses offered, the agency directly administers two and Commerce administers two—including one that NIST modified for its internal use. Specifically:

- **Counterintelligence awareness training.** This course teaches basic counterintelligence awareness and general awareness of threats. For example, participants learn that an individual's unexplained affluence or a lifestyle inconsistent with their known income can be an indicator of espionage. Commerce provides a basic version of this course, and NIST administers a tailored version to its employees. Sponsors of foreign national associates must take the training annually. This

training is recommended for co-workers and others having regular contact with foreign personnel accessing agency facilities.

- **Operations security training.** This Commerce-administered training explains how countries of concern acquire information, such as hacking mobile devices or soliciting researchers at professional conventions. This training is required for all employees.
- **Safeguarding international science**. This NIST-administered course focuses on collaborative research with entities from countries of concern and foreign national associates disclosures, and provides examples of research security threats such as malign foreign talent recruitment programs. According to NIST officials, the agency's operating units have the discretion to determine which employees are required to take the training. It is offered annually and as requested.
- **IT security training**. This NIST-administered training informs staff on how to access, use, and enforce access controls to protect non-public information found on the agency's IT systems. All agency personnel must take this course.

NIST also requires training on foreign travel and ethics:

- **Foreign travel training.** The agency requires its personnel, including researchers, who are travelling internationally to take a State Department foreign travel training course. This training covers risk management, surveillance detection, and awareness of threats from explosives and countermeasures, among other topics.
- **Ethics training.** New employees receive ethics training during orientation. This includes information on Office of Government Ethics rules, which address conflicts of interest.[28] Each year, agency employees, including researchers, must also complete ethics training, and some employees must also file financial disclosure forms. Both the orientation and annual training course address conflicts of interest. The agency also maintains an internal webpage that contains links to ethics resources for its employees to access.

In addition to training for its staff, NIST informs its foreign national and domestic associates on research security practices through their sponsors and onboarding process:

- **Communication from the NIST sponsor.** Sponsors must communicate information to their associates about security and IT

[28]All NIST employees receive a copy of the Standards of Ethical Conduct published by the Office of Government Ethics and are asked to certify that they have read them.

security requirements. According to officials, sponsors should tailor the information they provide to each associate on a case-by-case basis.

- **Onboarding process.** Associates complete physical security and IT security training. For example, foreign national associates are instructed that Commerce will restrict individuals from taking pictures of sensitive areas and will, as necessary, confiscate film or cameras (including cell phones) from unauthorized individuals taking pictures in those areas.

NIST Has Not Fully Implemented Federal Disclosure Requirements

NIST officials said the agency has not yet implemented all disclosure requirements under NSPM-33 with regard to extramural researchers—about 21 months after the January 2022 deadline specified in NSPM-33 for establishing policies requiring disclosures (as of October 2023). This is because, at the time of our review, OSTP had not yet issued finalized uniform disclosure forms for agency use as part of its NSPM-33 implementation.[29] Existing disclosures, including those provided pursuant to U.S. Office of Government Ethics rules, generally align with the disclosure requirements specified in NSPM-33 for intramural researchers and other employees. Additionally, NIST has implemented some, but not all, of the section 223 disclosure requirements for its extramural researchers. NIST officials said they will implement the remaining requirements for both NSPM-33 and section 223 following issuance of the finalized uniform disclosure forms, which occurred in November 2023. Separately, OSTP has not yet issued guidance on foreign talent recruitment programs required under section 10631 of the CHIPS and Science Act of 2022—about 10 months after the February 2023 deadline. As a result, NIST's implementation of certain requirements contained in the act have been delayed—about 4 months after the deadline.

Lack of Timely Federal Guidance Has Delayed NIST's Implementation of Federal Disclosure Requirements

NIST had not fully implemented NSPM-33 and section 223 requirements because OSTP had not issued uniform disclosure forms for agency use in a timely manner. Existing disclosures for intramural researchers generally align with requirements outlined in NSPM-33, but disclosures for extramural researchers do not fully align with NSPM-33 and section 223.

Disclosures responsive to NSPM-33 requirements include:

[29]NSPM-33 designates the Director of OSTP, along with the Director of the Office of Management and Budget and the Assistant to the President for National Security Affairs, to coordinate implementation of the memorandum.

- **Intramural researchers.** As NIST employees, intramural researchers must submit disclosures outlined by the U.S. Office of Government Ethics, such as sources of income and outside positions.[30] Intramural researchers and other employees must also follow agency ethics rules—such as those barring financial interests or engaging in outside employment or activities that conflict with the employee's duties—and resolve any conflicts by not participating in any activity creating a conflict of interest.[31] The agency requires all its employees to seek its approval prior to participating in any foreign-government funded program, which would include foreign talent recruitment programs.[32] Sponsors of foreign national associates must further disclose all sources of current and pending support, foreign and domestic; all current external professional appointments and affiliations, foreign and domestic, including any titled position whether or not payment is received; and foreign collaborations.[33]
- **Extramural researchers.** Extramural researchers seeking research funding must disclose the source and kind of monetary resources that they have received or applied for. However, the agency has not yet adopted the NSPM-33 requirement for extramural researchers to disclose non-monetary sources of support, participation in foreign

[30]Most NIST employees must complete OGE form 450, the Confidential Financial Disclosure Report. The purpose of this report is to assist employees and their agencies in avoiding conflicts between official duties and private financial interests or affiliations. U.S. Office of Government Ethics, *Confidential Financial Disclosure Report*, OGE form 450. Senior executive officials at NIST must instead complete form 278, the Public Financial Disclosure Report. See U.S. Office of Government Ethics, *Public Financial Disclosure Guide*. See also U.S. Department of Commerce, Office of the General Counsel, *Financial Disclosure*.

[31]NIST, *Summary of Ethics Rules* (2022).

[32]Such participation must have direct benefit to the U.S. and to NIST. NIST, *Participation in Foreign-Government Funded Programs,* P9300.00, (Jan. 2022).

[33]These requirements are established in NIST policy and the foreign national associates review form. See NIST, *NIST Foreign National Associates Programs*, NIST O1402.00 (May 2021).

talent recruitment programs, their positions/appointments, or affiliations/employment.[34]

Disclosure requirements for extramural researchers that are responsive to section 223 requirements include:

- Extramural researchers must disclose current and pending monetary research support they receive.[35] However, the agency does not require extramural researchers to disclose non-monetary current and pending research support or agree to update disclosures, if the agency requests an update.

NIST officials said the agency uses disclosures from extramural R&D award applications to monitor disclosures and assess certain risks. The officials said that the agency determines whether individuals that are part of a grant application have other obligations that could prevent them from fully conducting research funded by NIST, such as commitments to multiple research projects. NIST officials said that they verify each applicant's submitted information through discussions with the applicants and additional supporting research, as needed. This assessment is completed as part of NIST's R&D award proposal review process.[36]

[34]Additionally, the CHIPS and Science Act of 2022 requires federal research agencies to, no later than August 9, 2023, issue policies that, among other things, prohibit agency personnel from participating in foreign talent recruitment programs, prohibit making R&D awards for any proposal in which a covered individual is participating in a malign foreign talent recruitment program, and require covered individuals, as part of section 223 disclosures, to disclose if they are a party to a foreign talent recruitment program. Research and Development, Competition, and Innovation Act, Pub. L. No. 117-167, div. B, tit. VI, subt. D, § 10631,136 Stat. at 1664-65 (2022). No later than August 9, 2024, federal research agencies are to require that covered individuals included in proposed R&D awards certify that they are not participating in malign foreign talent recruitment programs. Research and Development, Competition, and Innovation Act, Pub. L. No. 117-167, div. B, tit. VI, subt. D, § 10632,136 Stat. at 1665-6 (2022).

[35]Section 223 requires each covered individual listed on an application for an R&D award from a federal research agency to disclose the amount, type, and source of all current and pending research support, both monetary and non-monetary. Each covered individual is also required to certify that the disclosure is current and accurate as part of the application, and must agree to update disclosures, if requested by the agency, before the award is made and during the term of the award.

[36]Other Commerce offices are generally not involved in monitoring or enforcing conflict of interest or disclosure policies, except in certain cases. Specifically, officials from Commerce's Office of Security and Office of Intelligence and Security said they can provide intelligence information in support of NIST's risk assessments at NIST's request. Additionally, Commerce's Office of Inspector General (OIG) may conduct criminal investigations of a narrowly defined set of issues, such as an undisclosed conflict of interest.

NIST officials said that the agency will implement the remaining disclosure requirements contained in both NSPM-33 and section 223 for extramural researchers after issuance of the final uniform disclosure forms for agencies to use to collect disclosures from extramural researchers. In November 2023, the National Science Foundation, on behalf of OSTP, issued the final uniform biographical sketch and current and pending research support disclosure forms.[37] Consistent with NSPM-33, the forms include fields for disclosing organizational affiliations/employment, positions/appointments, participation in foreign talent recruitment programs, and current and pending research support (monetary and non-monetary). The inclusion of current and pending research support (monetary and non-monetary) is also consistent with section 223 disclosure requirements and NSPM-33 implementation guidance to integrate NSPM-33 implementation with that of applicable statutes, including section 223. According to NIST officials, the agency will adopt the uniform disclosure forms. We did not assess NIST's implementation of the new uniform disclosure forms because of their recentness.

NSPM-33 requires federal research agencies to establish disclosure policies consistent with the memorandum within 12 months of its issuance (i.e., by January 14, 2022). However, NIST officials said the agency had not met this requirement—as of October 2023—nearly 21 months after the deadline because OSTP, one of the entities tasked with coordinating the implementation of NSPM-33, had not yet issued the uniform disclosure forms.[38] OSTP officials said that its development of guidance and forms had been delayed because of the need to reconcile them with

[37]The purpose of the Biographical Sketch is to assess how well qualified the individual, team, or organization is to conduct the proposed activities. Consistent with NSPM-33, the final instructions for submission of the biographical sketch instruct individuals to disclose appointments/positions and education/training, among other items. The purpose of Current and Pending (Other) Support is to assess the capacity of the individual to carry out the research as proposed and to help identify any potential scientific and budgetary overlap/duplication with the project being proposed.

[38]OSTP facilitates the coordination of the federal R&D agencies through the National Science and Technology Council. According to NSPM-33 implementation guidance, "[a]gencies should avoid taking major NSPM-33 implementation actions, including but not limited to new regulations, requirements, and disclosure forms, unless coordinated through the [National Science and Technology Council]". Joint Committee on the Research Environment, *Guidance for Implementing NSPM-33,* p.1. The goal of the standardized forms is to ensure that applying for awards from any federal research funding agency will require disclosing the same information in the same manner, to increase clarity and reduce administrative burden on the research community. See the Guidance, p. v.

agencies' varying mission requirements. The OSTP officials said that proposed legislation, if passed, could also affect what information certain agencies are required to collect and associated penalties.

With the disclosures that will be collected under the new uniform forms, once adopted, NIST will obtain key information—such as extramural researchers' participation in foreign talent recruitment programs—that will help the agency's efforts to identify and respond to research security risks. According to OSTP, "[e]ffective implementation of research security policy will make it more difficult for individuals to conceal materially important support, obligations, conflicts of interest, [or] relationships that, when concealed, could lead to Federal research agencies…making inadequately informed funding decisions."[39]

Lack of Timely Federal Guidance Has Delayed Agency Implementation of CHIPS and Science Act of 2022 Requirements

NIST has been unable to fully implement certain requirements under the CHIPS and Science Act of 2022 because of delays in receiving guidance from OSTP on foreign talent recruitment programs.[40] Not later than 180 days after the date of the enactment of the act (i.e., by February 5, 2023), OSTP was to publish and widely distribute a uniform set of guidelines for federal research agencies regarding foreign talent recruitment programs.[41] As of December 2023—10 months after the deadline—OSTP has not published these guidelines.

Additionally, not later than 1 year after the date of the act's enactment (i.e., by August 9, 2023), the act requires federal research agencies to issue a policy based on OSTP's guidelines on foreign talent recruitment programs.[42] NIST had not issued such a policy as of December 2023—4 months after the deadline.

NIST officials said that they are waiting for OSTP to issue the guidelines before the agency develops policy responsive to the act. According to

[39]Joint Committee on the Research Environment, *Guidance for Implementing NSPM-33*.

[40]Specifically, section 10631 of the act directs actions to prohibit federal research agency personnel from participating in foreign talent recruitment programs and covered individuals involved in federal research agency R&D awards from participating in malign foreign talent recruitment programs. Research and Development, Competition, and Innovation Act, Pub. L. No. 117-167, div. B, tit. VI, subt. D, § 10631(a), 136 Stat. at 1664 (2022).

[41]Research and Development, Competition, and Innovation Act, Pub. L. No. 117-167, div. B, tit. VI, subt. D, § 10631(b)(c),136 Stat. at 1664-65 (2022).

[42]Research and Development, Competition, and Innovation Act, Pub. L. No. 117-167, div. B, tit. VI, subt. D, § 10631(d), 136 Stat. at 1665 (2022).

OSTP officials, future proposed legislation, if passed may change the definition of a malign foreign talent recruitment program, making it difficult to develop the guidelines.[43] These officials said that they intend to form an interagency working group to accelerate development of the guidelines which will include descriptions of a foreign talent recruitment program and what federal employees are and are not permitted to do related to them. The officials stated that they do not have a set timeline for completing this effort. However, without these guidelines, NIST is unable to develop its own policy based on the guidelines, as required by the CHIPS and Science Act of 2022.

NIST Collects and Reviews More Disclosures from Foreign National Associates Than Domestic Associates

NIST collects and reviews disclosures from both foreign national associates and domestic associates, but it collects more information on foreign national associates and reviews them much more closely. These reviews are conducted pursuant to Commerce and NIST policy.[44] While neither type of associate is expressly covered under federal disclosure requirements, we use the requirements established under NSPM-33 for other types of researchers as a framework for our discussion.[45]

NIST Collects and Reviews a Broad Range of Information on Foreign National Associates

NIST assesses each foreign national associate based on their disclosures and information from other sources. The review for foreign national associates occurs before these associates are approved and annually thereafter. NIST's reviews of prospective foreign national associates from countries of concern occur via a meeting with the NIST Research Security Review team, sponsor, and the sponsor's management chain, while reviews of other foreign associates generally occur asynchronously.

[43]At the time of our review, section 10638 of the CHIPS and Science Act of 2022 includes a comprehensive definition of "malign foreign talent recruitment program," that is applicable to section 10631 of the act, which requires OSTP to publish and widely distribute uniform guidelines for federal research agencies regarding foreign talent recruitment programs.

[44]Department of Commerce, *Foreign Access Management Program*, DAO 207-12 (June 2021); NIST, *NIST Foreign National Associates Programs*; and NIST, *Domestic Associates Program*.

[45]OSTP officials told us in June 2023 that, while associates, including domestic associates collaborating with NIST researchers, are not the focus of NSPM-33 implementation, the memo can still serve as an appropriate research security framework to inform disclosure requirements for associates.

To conduct its reviews, NIST considers key information on the foreign national associate—such as affiliations—to identify threats and vulnerabilities. Prospective foreign national associates must disclose information about non-U.S. sources of funding—such as funding from a foreign talent recruitment program—information about education, and any external affiliations. A foreign national associate must not receive financial support from a foreign government-sponsored talent recruitment program, unless they receive agency approval.[46]

NIST then makes a risk determination and decides whether to accept each individual. NIST applies countermeasures, as needed, to mitigate identified risks. Table 4 provides examples of information that NIST assesses during these reviews.

Table 4: Examples of Information Used by NIST to Assess Risk of Prospective Foreign National Associates

Review element	Description
Affiliations	What past or present formal relationships or obligations has the prospective foreign national associate had with any foreign and domestic organization—including foreign talent recruitment programs, universities, scholarships, and professional societies?
Funding source	What are the current sources of funding for the prospective foreign national associate and the specific research project? Foreign national associates funded by other agencies require written permission from the funding agency to participate as a foreign national associate at NIST.
Project plan	What is the research being performed and what is the importance of the science?
Benefits to NIST	What will the prospective foreign national associate do at NIST that directly benefits the project and what will the scientific contribution be if the project is successful?
Export control/ technology control plan	What access to sensitive, proprietary, or export-controlled information will the prospective foreign national associate have? According to NIST, while most of the agency's research is exempt from export controls, due diligence is necessary to ensure compliance with U.S. law and regulatory requirements.
Fundamental research plan	What is the fundamental research being performed? This is described in terms of a publication abstract and specifies that the research program's scope is limited to basic or applied research in science or engineering.
Military and civilian commercial applications	What are the technologies (current or emerging) that a competitor nation could use to accelerate economic or national security interests? This includes fundamental research outcomes that may have military and civilian commercial applications in the next 5 years and access that the foreign national associate will have to controlled or proprietary information that may be used for military and civilian commercial applications.
Origin and method of recruitment	How and when did the NIST sponsor meet and recruit the prospective foreign national associate? For example, the foreign national associate may have approached the sponsor directly, or been recommended by a colleague.

[46]NIST, *NIST Foreign National Associates Programs.*

Review element	Description
NIST sponsor affiliations	What are the (1) foreign and domestic sources of current and pending research support, (2) current foreign and domestic professional appointments outside of NIST, and (3) foreign collaborations for the NIST sponsor assigned to the associate?

Source: GAO analysis of National Institute of Standards and Technology (NIST) information. | GAO-24-106074

NIST officials said they also use publicly available information and information provided by the intelligence community and Commerce's Office of Intelligence and Security to inform their reviews. Publicly available information sources include:

- **The Consolidated Screening List**. This is a list of parties for which the U.S. government maintains restrictions on certain exports, reexports, or transfers of items.[47]
- **Google Scholar.** This online service allows the user to search for scholarly literature across many disciplines and sources, including articles, books, and universities. Information obtained through this service can be used to determine whether the applicant is actively publishing through a competitor nation sponsored foreign university.
- **Australian Strategic Policy Institute.**[48] This institute manages an online tool for tracking entities from China. The tool indicates whether the entities are known for espionage or misconduct.

The agency also uses information from the intelligence community to inform its reviews. For example, it uses the Counterintelligence Threat Actor Discovery and Exploitation Landscape (CITADEL) verification system. CITADEL is a U.S. interagency law enforcement, homeland

[47]The Consolidated Screening List is an online consolidation of multiple export screening lists maintained by Commerce, State, and the U.S. Department of the Treasury and used by industry to screen potential parties to regulated transactions. The U.S. government implements export controls to (1) manage risks associated with exporting sensitive items while ensuring that legitimate trade can still occur and (2) advance U.S. national security and foreign policy objectives. These export controls are governed by a complex set of laws, regulations, and processes that multiple federal agencies administer to ensure compliance. A "re-export" is the shipment or transmission of an item subject to the Export Administration Regulations from one foreign country (i.e., a country other than the United States) to another foreign country. A re-export also occurs when there is "release" of technology or software (source code) subject to the Export Administration Regulations in one foreign country to a national of another foreign country.

[48]The Australian Strategic Policy Institute was formed in 2001 as an independent, non-partisan think tank. Its core aim is to provide the Australian Government with ideas on Australia's defense, security, and strategic policy choices. Australian Strategic Policy Institute, *The China Defence Universities Tracker* (Nov. 2019).

security, and intelligence community web-based platform used to screen foreign nationals accessing federal facilities or information resources.

During its reviews of foreign national associates, NIST analyzes the potential threats and vulnerabilities specific to each case and makes a risk determination (low, medium, or high). If risks are identified, the agency can apply one or more of a standard set of security countermeasures to mitigate risks associated with a potential foreign national associate (see table 5).

Table 5: Security Countermeasures Used by NIST to Mitigate Risks Related to Prospective Foreign National Associates

Countermeasure	Description
Threat awareness briefing	The NIST sponsor and other employees designated by the agency participate in a threat awareness update provided by NIST's Research Security Review team.
Operations security training	The NIST sponsor and other employees designated by NIST satisfactorily complete the Department of Commerce's operations security training.
Workspace integrity	The NIST sponsor and other employees designated by NIST review assigned laboratory, workspace, and the integrity of physical and digital access to identify potential vulnerabilities. The agency then takes corrective action as needed.
Sponsor affirmation	The NIST sponsor affirms that, prior to the arrival of the foreign national associate, all personnel assigned to the relevant project or program understand the foreign national associate's role, duration of the associate's collaboration with NIST, scope of authorized physical and digital access, and procedures for reporting unauthorized or questionable activity by the foreign national associate.
Status update	At a predetermined point during the duration of the foreign national associate's agreement, the NIST sponsor provides NIST management and the NIST Research Security Review team with a status update on the foreign national associate's contributions and any findings affecting workspace integrity or the sponsor affirmation.
Deny associate	Denial of the foreign national associate's application.
Reassign associate	Reassignment of the foreign national associate to other research initiatives.

Source: GAO analysis of National Institute of Standards and Technology (NIST) information. | GAO-24-106074

From fiscal year 2020 through fiscal year 2022, of the approximately 1,900 research-related foreign national associates that NIST reviewed, it denied applications of two prospective foreign national associates. Both individuals had concerning affiliations with foreign governments. During that same time, the agency also categorized 10 additional prospective foreign national associates—all Chinese citizens—as medium to high risk. However, NIST officials said they submitted information on all 10 foreign national associates for CITADEL reviews, which subsequently revealed no concerning information. According to our analysis of documents we reviewed for these 10 foreign national associates, the agency applied countermeasures to mitigate risks in all 10 cases. Operations security training was the most common countermeasure applied.

NIST Collects Few Disclosures for Domestic Associates and Reviews Them Less Closely

NIST collects and reviews fewer disclosures from domestic associates than it does from foreign national associates.[49] Specifically, as part of their applications, prospective domestic associates must disclose basic biographical details, such as their employer/home organization and education. The agency does not require its domestic associates to disclose participation in foreign talent recruitment programs, positions or appointments, or sources of current or pending research support.

In contrast to its procedures for foreign national associates, NIST also does not conduct a research security review prior to acceptance of domestic associates. Instead, the agency relies on other mechanisms—including standard background checks, access controls, and research security training courses for its employees to ensure research security. These mechanisms are administered by various NIST and Commerce offices and groups, including Commerce's Office of Security, NIST's Technology Partnership Office, NIST's Research Security Review team, and NIST's International and Academic Affairs Office.

NIST officials said that the agency collects and reviews disclosures more closely from foreign national associates than domestic associates because it primarily focuses on foreign threats to its research. However, according to OSTP officials, both foreign and domestic researchers may pose risks as participants in the U.S. R&D enterprise. For example, in April 2023, a former Harvard professor involved with federally funded research at the National Institutes of Health and the Department of Defense was sentenced for (1) lying to federal authorities about his affiliation with China's Thousand Talents program and a Chinese university, and (2) failing to report foreign income.[50] As with foreign researchers, domestic associates could also be enticed to participate in foreign talent recruitment programs through offers of compensation, such as cash, research funding, or career advancement opportunities.

[49]NIST's Technology Partnerships Office collects and reviews disclosures from domestic associates. NIST's research security team and the International and Academic Affairs Office collect and review disclosures from foreign national associates.

[50]The Thousand Talents program was one of the most prominent Chinese foreign talent recruitment programs designed to attract, recruit, and cultivate high-level scientific talent to advance China's scientific development, economic prosperity, and national security. U.S. Attorney's Office, District of Massachusetts, Press Release: F*ormer Harvard University Professor Sentenced for Lying About His Affiliation with Wuhan University of Technology; China's Thousand Talents Program; and Filing False Tax Returns*, (April 26, 2023).

OSTP officials told us in June 2023 that while associates, including domestic associates collaborating with NIST researchers, are not the focus of NSPM-33 implementation, the memo can still serve as an appropriate research security framework to inform disclosure requirements for associates. According to NSPM-33, agencies may require disclosures from a broader range of R&D participants than those specified in the memo.[51] In the context of this report, that could include foreign national associates and domestic associates. While NIST's disclosure requirements for its foreign national associates are consistent with the NSPM-33 framework, gaps exist in the information that NIST collects for domestic associates. Requiring its domestic associates to disclose the information described under the NSPM-33 framework—including updating those disclosures as appropriate—and then reviewing that information, would enhance NIST's ability to assess and respond to risks posed by domestic associates.

NIST Assesses Risks and Collaborates with the Intelligence Community and Commerce to Identify Threats

In addition to its review of foreign national associates, NIST assesses and responds to research security risks to its other research activities, such as providing measurement services to foreign entities. Identified risks generally involve countries of concern or research in emerging areas—such as quantum and 5G technologies.[52] Such activities make up a small portion of the overall volume of NIST's activities. When assessing the risk of these activities, the agency weighs the scientific benefits against the potential harms to national interests and considers countermeasures for mitigation. NIST also collaborates with the intelligence community and other Commerce offices to identify threats.

[51]Under NSPM-33, R&D participants include "researchers at academic research institutions, independent research institutes, medical centers and institutes, private companies, and Federal Government research centers and laboratories, as well as those who participate in the process of allocating and awarding Federal R&D funding."

[52]According to ODNI training materials on operations security, a threat is as an adversary with the intent and capabilities to compromise an agency's mission or sensitive activities. A vulnerability is a weakness that an adversary can exploit to get an agency's critical information. Risk is the probability that an adversary will compromise the agency's critical information or exploit a vulnerability and the potential impact of the adversary's success. ODNI NCSC, *Understanding OPSEC - The OPSEC Cycle National OPSEC Awareness Month, January 2023, Bulletin 2*, (Jan. 2023).

NIST Assesses and Responds to Risks to Research Activities Involving Countries of Concern

Separate from its review of foreign national associates, NIST reviews its research-related activities involving entities or researchers from countries of concern to assess and respond to risks, such as the potential theft of scientific information by foreign talent recruitment programs. Based on our review of agency-provided data and supporting documentation, these reviews resulted in the rejection of approximately 740 requests from countries of concern between fiscal year 2013 and April 2023 (see table 6).

Table 6: Results of NIST Review of Research Activities Requested by Countries of Concern

		Number of requests from foreign countries of concern			
Requested activity	**Total number of requests[a]**	**Total**	**Rejected**	**Accepted**	**Time period**
In-person foreign travel	5,300	1	0	1	March 2017-April 2023[b]
Virtual meetings	200	11	2	9	August 2021-April 2023[c]
Assistance-in-kind offers	1,500	69	68	1	2015-2022[d]
Measurement service					
Standard reference materials	308,200	8,771	327	8,444	FY2013-2022
Standard reference data	27,200	1,284	340	944	FY2013-2022
Standard reference instruments	100	19	0	19	FY2013-2022
Calibrations	22,700	125	2	123	FY2013-2022

FY = fiscal year

Source: GAO analysis of National Institute of Standards and Technology (NIST) information. | GAO-24-106074

[a]Data in this column are rounded to the nearest hundred.

[b]NIST's records only dated back to March 2017, at which time the agency had migrated to a new IT system.

[c]The NIST research security team started reviewing virtual meeting requests in August 2021.

[d]NIST only retains records of assistance-in-kind for the prior 6 years.

Identified risks generally involved countries of concern and research in areas known to be of interest to countries of concern, such as quantum computing. For example:

- According to training slides from fiscal year 2023, the agency declined to collaborate on an experimental research project with foreign researchers determined to be affiliated with a malign foreign talent recruitment program and instead decided to work on a non-experimental paper with only the NIST author.

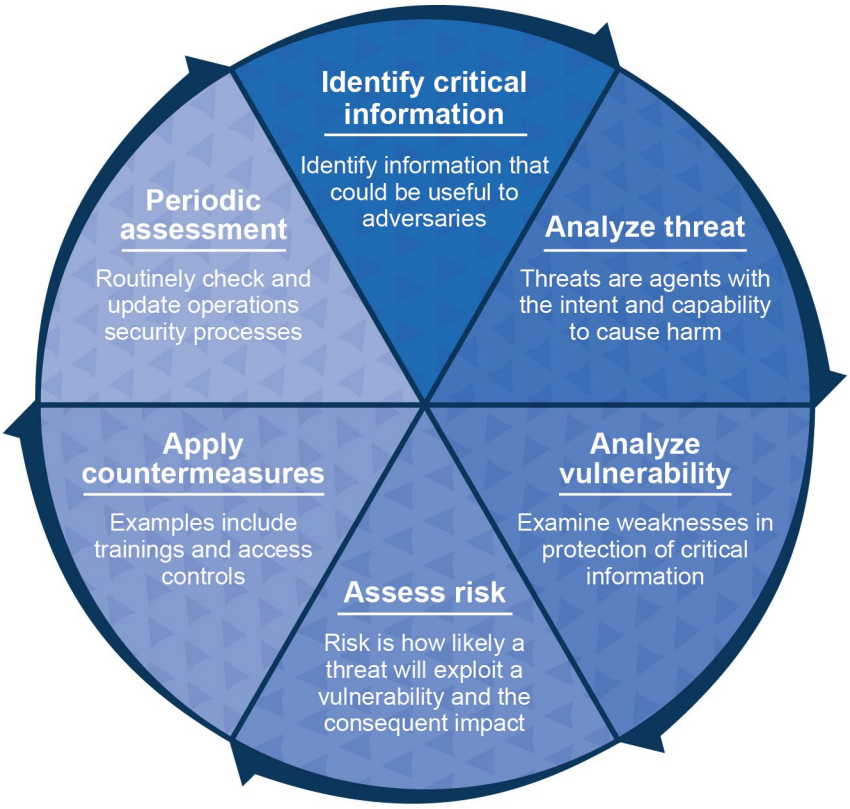
- In fiscal year 2022, a Chinese institute requested NIST's assistance in calibrating a scientific tool. The agency rejected this request because the United States (through NIST) had a technical advantage in this area and the tool had potential military applications.

To identify and respond to risks, NIST follows the operations security process described by ODNI's National Counterintelligence and Security Center (NCSC).[53] This process involves identifying and protecting critical information, identifying vulnerabilities, and applying countermeasures to counter threats (see fig. 4).[54]

[53]ODNI is responsible for identifying foreign threats to the U.S. including federally funded research activities. Within ODNI, NCSC leads and supports the U.S. government's counterintelligence and security activities critical to protecting the nation by providing outreach to U.S. entities at risk of foreign penetration and issuing warnings regarding intelligence threats. According to NCSC, taking appropriate steps to make it harder for adversaries to collect public, unclassified information can improve an organization's overall security exponentially. The process of identifying key data, anticipating the motives and goals of potential adversaries, and actively seeking threat information increases the likelihood of thwarting efforts to acquire more sensitive data.

[54]Critical information is information that an agency determines is important to its organization, which if exposed, could be useful by itself or in aggregate to a known or unknown adversary. Examples of information that could be critical information include R&D and proprietary operational information. ODNI NCSC, *Understanding OPSEC*.

Figure 4: The National Counterintelligence and Security Center's Operations Security Process



Source: GAO analysis of National Counterintelligence and Security Center information. | GAO−24−106074

In following the NCSC's process, the agency conducts various reviews including:[55]

- **Foreign travel requests.** NIST's International and Academic Affairs Office, in coordination with the Research Security Review team, reviews all requests from staff to travel to foreign countries (both in-person and virtual). Reasons for travel could include activities such as participation in a conference. Officials told us the Research Security Review team determines, for example, if there are any concerns with the entity paying for the trip or the trip's purpose.
- **Assistance-in-kind offers.** NIST's International and Academic Affairs Office reviews and approves all offers of assistance-in-kind from foreign countries. Officials stated that NIST typically does not accept assistance-in-kind from any entity in a country of concern.[56]
- **Measurement service requests.** NIST's Research Security Review team reviews measurement service requests from countries of concern. For example, it reviews foreign requests for standard reference materials that are not sold commercially for export controls and against the consolidated screening list, according to officials.

Given the risks and potential threats facing NIST, the agency has various countermeasures it can take to mitigate those risks and threats (see fig. 5).

Unearned Authorship for Collaborators from Countries of Concern

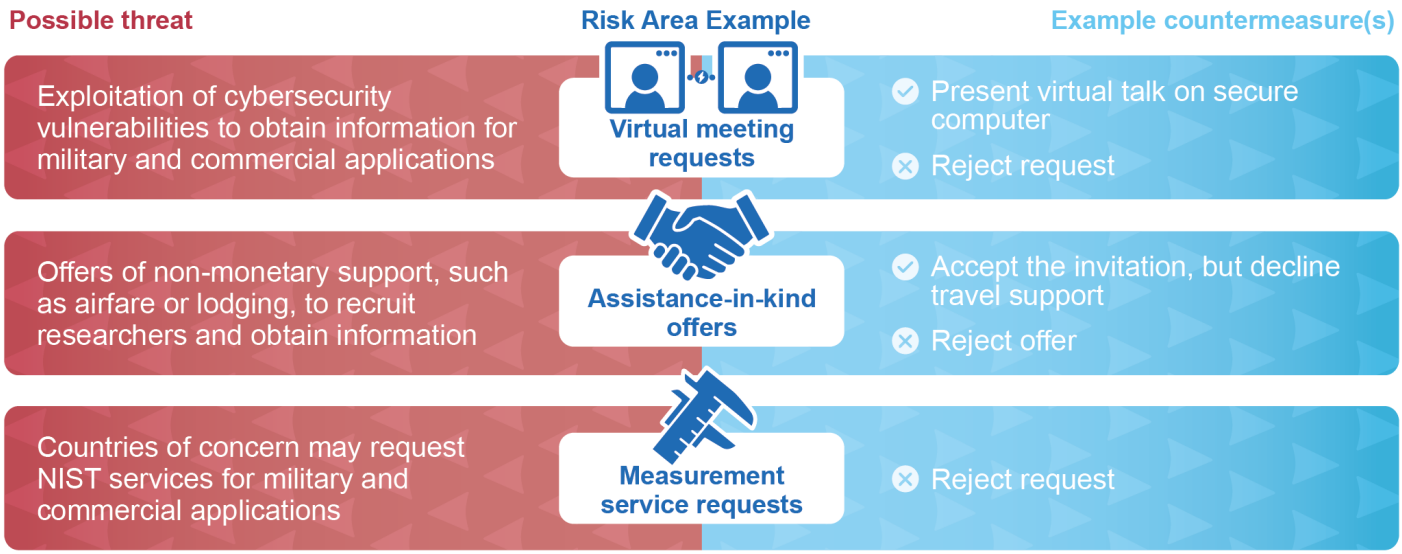
The NIST Research Security Review team reviews draft research publications that include foreign contributors prior to publication if one of the authors is from a country of concern. These reviews do not include draft publications through collaborations with foreign national associates. NIST determines whether any names of people who did not contribute to the publication were added to the list of authors. Such additions could harm NIST's reputation because the individual would receive unearned credit from being listed as an author of a publication that is associated with NIST. Moreover, these individuals may have concerning affiliations, including with malign foreign talent recruitment programs. The NIST Research Security Review team provided training to encourage NIST researchers to consult with the team before engaging in a collaborative research effort with an entity from a country of concern.

Source: GAO analysis of NIST information. | GAO-24-106074

[55]Collaborations with foreign national associates are discussed earlier in this report.

[56]One exception NIST told us about occurred in February 2020, when a NIST employee visited the National Institute of Metrology of China. NIST approved the trip because the trip allowed NIST to better understand how its calibration services compared to those of China. NIST accepted assistance-in-kind in the form of airfare and lodging from the National Institute of Metrology for this visit.

Figure 5: Examples of Countermeasures that NIST Takes to Mitigate Risks and Threats to Its Research Security



Source: GAO analysis of National Institute of Standards and Technology (NIST) information (analysis); Happyart/martialred/stock.adobe.com (images). | GAO-24-106074

NIST Generally Followed Leading Collaboration Practices

NIST collaborates with the intelligence community and Commerce to receive information on identified threats and share research security practices. In our prior work, we found that effective interagency collaboration benefits from certain leading practices, such as clarifying roles and responsibilities.[57] In its work with both the intelligence community and Commerce, NIST generally followed all eight leading practices for interagency collaboration (see table 7). For more information on the leading practices and our assessment, see appendix III.

[57]GAO, *Government Performance Management: Leading Practices to Enhance Interagency Collaboration and Address Crosscutting Challenges*, GAO-23-105520 (Washington, D.C.: May 2023).

Table 7: NIST Implementation of Leading Practices for Interagency Collaboration

Leading practice[a]	Assessment of whether NIST followed leading practice
Define common outcomes	**Generally followed:** Various federal statues and guidance direct NIST and its partners to implement disclosure requirements for federal researchers. Separately, National Security Presidential Memorandum 33 (NSPM-33) directs the Director of the Office of Science and Technology Policy (OSTP) to coordinate with the Director of National Intelligence (ODNI) and other agencies, including NIST, to enhance awareness of risks to research security and policies and measures for mitigating those risks.[b]
Ensure accountability	**Generally followed:** Various federal statutes and guidance establish deadlines for the issuance of uniform disclosure policies. Additionally, NIST shares information about its research security program via the Safeguarding Science Roundtable. Based on NIST's contributions to the roundtable, ODNI formally recognized and commended NIST's research security program.
Bridge organizational cultures	**Generally followed:** Collaboration between NIST and ODNI via the Safeguarding Science initiative helps alleviate cultural differences by creating shared definitions and best practices.
Identify and sustain leadership	**Generally followed:** NIST takes primary responsibility for developing and managing its own research security program with support from Commerce and ODNI.
Clarify roles and responsibilities	**Generally followed:** NSPM-33 clearly establishes the responsibilities of research agencies like NIST, such as the need to obtain disclosures from researchers. It also details the role of ODNI and OSTP in enhancing federal research agencies' awareness of research security risks and policies.
Include relevant participants	**Generally followed:** NIST actively coordinates with Commerce's Office of Intelligence and Security as well as ODNI to obtain information about research security threats.
Leverage resources and information	**Generally followed:** NIST receives information from Commerce through weekly briefings, an embedded liaison from the Office of Security, and a dedicated analyst from the Office of Intelligence and Security. In addition, ODNI provides NIST with online tools to access information.
Develop and update written guidance and agreements	**Generally followed:** NSPM-33 establishes responsibilities for NIST and ODNI related for research security. For example, NSPM-33 states that ODNI should work with agencies to develop research security products to, among other things explain foreign government supported collection methods and means of exploitation. It also requires research and development funding agencies, such as NIST, to require certain participants in the U.S. research and development enterprise to provide disclosures of information that can reveal potential conflicts of interest and conflicts of commitment.

Source: GAO analysis of National Institute of Standards and Technology (NIST) information and GAO-23-105520. | GAO-24-106074

Note: We evaluated the extent to which NIST actions generally followed, partially followed, or did not follow each leading practice based on evidence NIST and other agencies provided. "Generally followed" means NIST and other agencies provided evidence that it has generally followed a leading practice. "Partially followed" means NIST and other agencies provided evidence that it has taken some steps toward following a leading practice. "Did not follow" means NIST and other agencies provided evidence that its actions do not align with a leading practice.

[a]GAO, *Government Performance Management: Leading Practices to Enhance Interagency Collaboration and Address Crosscutting Challenges*, GAO-23-105520 (Washington, D.C.: May 2023).

[b]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).

NIST collaborates with the NCSC to identify potential research security threats.[58] For example, when the agency awards grants, it can request additional information about supply chain, counterintelligence, and cybersecurity risks from ODNI's Supply Chain and Counterintelligence Risk Management Task Force.[59] Further, NCSC identifies and shares information with NIST on strategic foreign threats to U.S. interests and provides the agency with best practices to prevent threat actors from exploiting, manipulating, or stealing its research and intellectual property. As an example of sharing information on best practices, NIST uses the operations security process from NCSC depicted in figure 4 (above).

NIST has also worked with NCSC and other federal agencies with research security programs via the Safeguarding Science Roundtable. The roundtable is a forum facilitated by NCSC and is comprised of agencies that support a significant amount of research activity such as NIST, the National Science Foundation, and the Department of Health and Human Services. NIST and the other members of the roundtable develop best practices on topics such as insider threats, operations security, and defensive counterintelligence. According to NIST officials, the agency leads discussions on research security review for foreign national associates, sale of scientific products, and international collaborations. NCSC also publishes research security resources for federal agencies in its Safeguarding Science online toolkit.[60]

Further, in August 2023, NIST issued the Safeguarding Science Research Security Framework to provide guidance to the U.S. science and research community on research security topics.[61] According to the framework, it is "…designed to enable organizations to implement a

[58]NSPM-33 directs ODNI to coordinate intelligence community activities to identify and assess the capabilities, activities, and intentions of foreign actions as they relate to the security of U.S. federally funded research activities. NCSC leads and supports federal counterintelligence and security activities critical to protecting the nation by providing outreach to U.S. entities at risk of foreign penetration and issuing warnings regarding intelligence on potential threats.

[59]Authorized in 2019, the Supply Chain and Counterintelligence Risk Management Task Force's mission is to standardize information sharing between the federal government's intelligence and acquisition communities regarding supply chain and counterintelligence risks. 50 U.S.C. § 3370.

[60]The Safeguarding Science online toolkit can be accessed at https://www.dni.gov/index.php/safeguarding-science.

[61]NIST, *Safeguarding International Science: Research Security Framework*, NIST IR 8484, (Aug. 2023).

mission-focused, integrated, risk-balanced program through the application of research security principles and best practices that fosters the safeguarding of international science while mitigating risks to the integrity of the open collaborative environment."

NIST also works with other members of the intelligence community, such as the FBI. NIST and Commerce officials told us that they refer all suspected threats to the FBI, the principal law enforcement agency for the federal government.[62] The officials said that NIST and Commerce do not have the authority to investigate suspected threats, whereas the FBI does.

NIST and Commerce officials told us that the agency also collaborates with the following Commerce offices to identify potential research security threats:[63]

- **Office of Security.** This office is responsible for ensuring personnel and physical security requirements are met. The office also provides an expert in counterintelligence and foreign access management who participates in NIST's Research Security Review team meetings and provides advice on physical security matters.
- **Office of Intelligence and Security.** This office ensures that the department's intelligence needs are coordinated both across the federal government and with the intelligence community. It provides information on competitor countries, conducts research with its contacts in the intelligence community regarding potential threats, and communicates intelligence information. A dedicated analyst from the office provides day-to-day intelligence support to the agency. NIST can request information on specific threats from the analyst, such as an assessment of a particular scholarship organization. The dedicated analyst also coordinates with the intelligence community on these requests, as needed.
- **Insider Risk Management Program Office**. This office serves as the department's hub for intake, analysis, and referrals of information on

[62]For example, Section 811 of the Intelligence Authorization Act for Fiscal Year 1995 requires departments and agencies to immediately notify the FBI when classified information is being, or may have been, disclosed in an unauthorized manner to a foreign power or an agent of a foreign power. Pub. L. No. 103-359, tit. VIII, § 811(c)(1), 108 Stat. 3423, 3455 (1994) (codified at 50 U.S.C. § 3381 (e)(1)(A)).

[63]The Office of Intelligence and Security leads the department's intelligence, security, and insider risk management offices to protect U.S. economic and national security interests from foreign economic and strategic threats.

insider risks.[64] Staff communicate, train, and educate the Commerce workforce on insider risk policy, process, and indicators. It does not conduct investigations and instead refers issues to appropriate authorities, such as the FBI.

Additionally, NIST collaborates with Commerce's Office of Inspector General (OIG). In particular, employees must refer the possible existence of certain activities—including mismanagement, waste of funds, abuse of authority, or a violation of law or regulation—to OIG.[65] In the context of research security, this would generally include criminal conflicts of interest or grant fraud, according to an OIG official. OIG can also conduct program audits of NIST's implementation of research security-related policies and procedures, but has not done so recently.[66]

NIST and Commerce Did Not Fully Follow Selected Leading Practices for Evaluating Their Research Security Training

We found that research security training for intramural research staff generally followed selected leading practices in the area of implementation of its training courses, but not in the area of evaluating effectiveness.[67] The agency communicates and emphasizes the importance of these training courses, but neither it nor Commerce systematically evaluate their effectiveness.

In our prior work, we developed a framework that summarizes leading practices for effective training and development programs and presents related questions concerning the components of the training and

[64]According to the Insider Risk Program Office's website, an insider risk is the risk that an insider—a person within a group or organization with access to information, facilities, and other personnel—will use their authorized access, wittingly or unwittingly, to do harm to U.S. security. This risk can include damage resulting from espionage, terrorism, unauthorized disclosure of national security information, or the loss or degradation of departmental resources or capabilities.

[65]Department of Commerce, *Inspector General Investigations and Related Activity* DAO 207-10 (June 2021).

[66]In July 2015, OIG announced an audit to determine whether NIST has adequate processes and procedures to ensure that foreign nationals have the proper access to NIST information systems and data to prevent unauthorized use. In December 2017, OIG ended the audit because of major ongoing revisions to NIST's and Commerce's security policies.

[67]We selected relevant leading practices in the areas of implementation and evaluation from GAO, *Human Capital: A Guide for Assessing Strategic Training and Development Efforts in the Federal Government*, GAO-04-546G (Mar. 2004). Implementation involves ensuring effective and efficient delivery of training and development opportunities in an environment that supports learning and change. Evaluation involves assessing the extent to which training and development efforts contribute to improved performance and results.

development process.[68] The questions are designed for federal agencies to consider in ensuring that training and development investments are targeted strategically and are not wasted on efforts that are irrelevant, duplicative, or ineffective. Based on our assessment, NIST's and Commerce's research security training courses generally followed three, partially followed three, and did not follow one of the seven selected leading practices (see table 8). See appendix IV for additional information on our assessment.

Table 8: Assessment of NIST Training Against Selected Leading Practices

Component	Leading practice	Key questions	Assessment of whether NIST followed leading practice
Implementation	Communicate importance of training	What steps do agency leaders take to communicate the importance of training and developing employees, and their expectations for training and development programs to achieve results?	**Generally followed:** NIST communicated to staff on the importance of training courses through a variety of verbal and written methods, such as during meetings and its internal website.
	Encourage employee buy-in	What steps does the agency take to encourage employees to buy in to the goals of training and development efforts, so that they participate fully and apply new knowledge and skills when doing their work?	**Generally followed:** NIST encouraged employee buy-in by in several ways, including through recruiting prominent internal ambassadors to speak on the importance of research security.
	Collect data	Does the agency collect data during implementation to ensure feedback on its training and development programs?	**Partially followed:** NIST solicited some informal feedback from participants and their supervisors. However, it did not collect a broader range of data across its training courses.
Evaluation	Evaluate effectiveness	To what extent does the agency systematically plan for and evaluate the effectiveness of its training and development efforts?	**Did not follow:** NIST did not systematically assess the effectiveness of its training courses.
	Use performance data	What performance data (including qualitative and quantitative measures) does the agency use to assess the results achieved through training and development efforts?	**Partially followed:** NIST considered some informal feedback from participants and their supervisors and assessed participants' understanding of one training course. However, it did not use additional information that could help the agency determine what changes, if any, may be necessary for its training courses.
	Incorporate feedback	How does the agency incorporate evaluation feedback into the planning, design, and implementation of its training and development efforts?	**Partially followed:** NIST informally considered some feedback on its training courses to identify areas for improvement. However, it did not establish systematic monitoring and feedback processes.

[68]GAO-04-546G.

Component	Leading practice	Key questions	Assessment of whether NIST followed leading practice
	Compare training	Does the agency compare its training investments, methods, or outcomes with those of other organizations to identify innovative approaches or lessons learned?	**Generally followed:** NIST collaborated on training courses with the Department of Commerce and regularly meets with other agencies on research security topics.

Source: GAO analysis of National Institute of Standards and Technology (NIST) information and GAO-04-546G. | GAO-24-106074

Note: We evaluated the extent to which NIST actions related to the training of its intramural researchers on research security generally followed, partially followed, or did not follow each leading practice based on evidence NIST provided. “Generally followed” means NIST provided evidence that it has generally followed a leading practice. “Partially followed” means NIST provided evidence that it has taken some steps toward following a leading practice. “Did not follow” means NIST provided evidence that its actions do not align with a leading practice. We did not assess training efforts for associates because of their limited nature.

As noted in the table above, NIST and Commerce do not systematically collect information on their training courses or otherwise make efforts to evaluate their effectiveness. For example, while NIST solicits and considers some informal feedback from participants and their supervisors on its research security training courses, it does not systematically assess their effectiveness. Three of the 12 sponsors we spoke with stated they were not sure what agency requirements were for disclosing external affiliations. Similarly, four of the 12 sponsors noted that they were not aware of agency requirements regarding participation in foreign talent recruitment programs. Moreover, half of the sponsors identified areas for improvement in the training, such as providing more examples of risks that employees may encounter. While these results cannot be generalized, they illustrate the potential benefit of a more formalized evaluation of the effectiveness of research security training.

Training courses should be evaluated to ensure that they effectively achieve their goals—in this case, to ensure that they inform staff on research security policies and practices. According to our prior work, training evaluations enable agencies to ensure the accountability of their trainings and achieve desired results.[69] However, the agency only collects informal feedback on its training courses, and it does not use this information to formally evaluate the course’s effectiveness. These training courses are a key mechanism to inform employees about agency policies and requirements. If NIST conducted evaluations of its training courses, consistent with training leading practices, then it would be better able to make decisions on whether to modify or redesign them.

[69]GAO-04-546G.

Conclusions

NIST has taken steps to help ensure research security. These include collecting and reviewing selected disclosures, reviewing and sponsoring foreign national associates, assessing and responding to risks, collaborating within Commerce and the intelligence community, and implementing research security training.

NIST's implementation of key disclosure requirements depends, in part, on OSTP's issuance of timely and actionable guidance. However, OSTP has not issued some required guidance leading to delays in NIST collecting additional disclosures that could help the agency respond to research threats.

While NIST has disclosure requirements in place for its researchers, it does not require domestic associates to disclose information that could be used to determine conflicts of interest or conflicts of commitment. Given the potential for critical research being divulged to foreign entities, the agency must ensure that it has the information necessary to identify and respond to research security risks posed by all of its researchers, including its domestic associates.

Effective training is also critical to helping ensure research security. However, NIST and Commerce do not systemically evaluate the effectiveness of their research security training courses. Without doing so, they are limited in their ability to identify opportunities to improve their training courses. Such improvements could better inform agency personnel on research security policies and practices and better enable them to safeguard NIST's research activities.

Recommendations for Executive Action

We are making a total of three recommendations, including one to OSTP and two to NIST. Specifically:

The Director of OSTP should expedite the development and issuance of guidelines on foreign talent recruitment programs as required by section 10631 of the CHIPS and Science Act of 2022. (Recommendation 1)

The Director of NIST should, consistent with applicable statutes and regulations, collect and review disclosures from domestic associates—including information on positions and appointments, current and pending research support, and participation in foreign talent recruitment programs—and require updates to these disclosures, as appropriate. (Recommendation 2)

The Director of NIST should, in coordination with the Secretary of Commerce as appropriate, evaluate the effectiveness of research security training courses for NIST staff. For example, this could include collecting and analyzing employee feedback. (Recommendation 3)

Agency Comments

We provided a draft of this report to NIST, OSTP, and ODNI for review and comment. In its comments, reproduced in appendix V, NIST, through Commerce, agreed with our recommendations, stating that it will prepare a formal action plan to address them. NIST also provided technical comments, which we incorporated as appropriate.

The Deputy General Counsel and Chief Operating Officer of OSTP provided comments via email, stating that OSTP concurred with the recommendation and that it was working on expediting development and issuance of the guidelines on foreign talent recruitment programs.

ODNI did not have any comments on the report.

We are sending copies of this report to the Director of NIST, the Director of National Intelligence, and the Director of OSTP. 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 (202) 512-6888 or WrightC@gao.gov. GAO staff who made key contributions to this report are listed in appendix VI.

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

List of Committees

The Honorable Maria Cantwell
Chair
The Honorable Ted Cruz
Ranking Member
Committee on Commerce, Science, and Transportation
United States Senate

The Honorable Mark Warner
Chairman
The Honorable Marco Rubio
Vice Chairman
Select Committee on Intelligence
United States Senate

The Honorable Frank Lucas
Chairman
The Honorable Zoe Lofgren
Ranking Member
Committee on Science, Space, and Technology
House of Representatives

The Honorable Michael Turner
Chairman
The Honorable Jim Himes
Ranking Member
Permanent Select Committee on Intelligence
House of Representatives

Appendix I: Objectives, Scope, and Methodology

This report examines the National Institute of Standards and Technology's (NIST) efforts to (1) meet federal disclosure requirements for intramural and extramural researchers;[1] (2) collect and review disclosures from foreign national associates and domestic associates; (3) identify, address, and collaborate on research security risks;[2] and (4) align its security training with selected training leading practices.

To determine the extent to which NIST is meeting federal disclosure requirements for intramural and extramural researchers, we reviewed relevant statutes and guidance, and NIST policies, and conducted interviews with cognizant officials from NIST, Commerce, Commerce's Office of Inspector General (OIG), and the Office of Science and Technology Policy (OSTP). We compared NIST's implementation of disclosure requirements with the requirements included in:

- National Security Presidential Memorandum 33 (NSPM-33)[3] and OSTP guidance for implementing NSPM-33,[4]
- Section 223 of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (section 223),[5] and
- CHIPS and Science Act of 2022.[6]

To determine the extent to which NIST collects and reviews disclosures from foreign national associates and domestic associates, we reviewed Commerce's and NIST's policies and procedures regarding reviewing and

[1]This section includes an assessment of the ability of the Department of Commerce's offices and the National Institute of Standards and Technology (NIST) to monitor and enforce conflict of interest and disclosure policies and requirements and conduct risk assessments. This report also includes an assessment of NIST's review process for foreign national associates.

[2]This section includes an analysis of NIST's coordination with Commerce offices and other federal agencies and an analysis and summary of incidents of undue foreign influence at Institute-supported research facilities and programs over the past 10 years.

[3]The White House, NSPM-33.

[4]Joint Committee on the Research Environment, *Guidance for Implementing NSPM-33*.

[5]William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No 116–283, div. A, tit. II, subt. B, § 223, 134 Stat. 3388, 3470-72 (codified at 42 U.S.C. § 6605).

[6]Research and Development, Competition, and Innovation Act (contained in what is commonly referred to as the CHIPS and Science Act of 2022), Pub. L. No. 117-167, div. B, tit. VI, subt. D, §§ 10631-32, 136 Stat. 1366, 1664-66 (2022).

hosting foreign national associates and domestic associates.[7] We discussed these policies with NIST and Commerce officials in interviews. In November 2022, we observed two in-person research security program reviews of potential foreign national associates from countries of concern to enhance our understanding of the reviews.[8] Prior to the reviews, NIST provided us with copies of the foreign national associate review form for each foreign national associate. We observed the discussion of the research security review team and asked follow-up questions for clarification following the observations. NIST officials said that these review meetings were representative of other review meetings.

Further, we reviewed the foreign national associate case review forms pertaining to the 10 applicants that NIST identified as medium or high risk during the time period from fiscal years 2020 through fiscal year 2022. We reviewed these forms to check for completeness and to learn what countermeasures NIST used to respond to the risks.

To determine the extent to which NIST has identified and addressed risks to research security, we reviewed written responses and interviewed cognizant NIST and Commerce officials to discuss the types of risks identified and their responses to them. We also reviewed NIST and Commerce policies and procedures related to research security practices, including those for foreign access management.[9]

Further, we requested data on activities that may pose risks to research security from NIST. For each area of risk and each fiscal year from 2013-2022, we requested both the total number of activities and the number of activities that NIST identified as potentially posing research security risks. Of these activities, we further asked for the number that NIST ultimately rejected based on further review, and the number that NIST ultimately proceeded with, possibly with modifications. We reviewed the aggregate information we received from NIST for obvious errors or potential inconsistencies and discussed the data with knowledgeable officials. We determined that the data were reliable for the purpose of presenting NIST's data on its associates and their disclosures, threats identified by NIST, and disclosures made by NIST grant applicants.

[7]NIST, *NIST Foreign National Associates Programs*; NIST, *Domestic Associates Program*.

[8]NIST focuses primarily on risks posed by countries of concern.

[9]For example, Commerce, *Foreign Access Management Program*, DAO 207-12, (June 2021); *NIST Foreign National Associates Programs*.

We also compared NIST's collaborative efforts with the eight leading practices for interagency collaboration discussed in GAO-23-105520 *Government Performance Management: Leading Practices to Enhance Interagency Collaboration and Address Crosscutting Challenges*.[10] The eight leading practices are: (1) define common outcomes; (2) ensure accountability; (3) bridge organizational cultures; (4) identify and sustain leadership; (5) clarify roles and responsibilities; (6) include relevant participants; (7) leverage resources and information; and (8) develop and update written guidance and agreements. To learn about the collaborative efforts, we interviewed NIST, Commerce, and OIG staff, and reviewed written responses from the Office of the Director of National Intelligence (ODNI) to determine the extent to which NIST's coordination efforts align with the leading practices.

To determine the extent to which NIST and Commerce's research security-related training courses align with selected leading practices, we reviewed training documents used by NIST and conducted interviews with cognizant NIST and Commerce officials. For example, we reviewed training requirements for NIST intramural researchers, including sponsors, and associates outlined under Commerce and NIST policies. We also reviewed materials used to facilitate training, such as slide decks.

We also discussed research security training courses with NIST and Commerce officials, including via semi-structured interviews with NIST sponsors to obtain their views on the training courses they receive. From January 2023 to February 2023, we conducted semi-structured interviews with a non-generalizable random stratified sample of 12 NIST sponsors—four sponsors of foreign national associates, four sponsors of domestic associates, and four sponsors of both foreign national associates and domestic associates. We randomly selected participants from each of the three groups based on a list provided by NIST of all sponsors from NIST's Gaithersburg, MD and Boulder, CO campuses who were active in fiscal year 2022. Through these interviews, we obtained sponsors' perspectives on roles, responsibilities, and experiences with implementing research security-related policies, procedures, and training at NIST.

Prior to conducting the interviews, we discussed and incorporated feedback from cognizant NIST officials on our semi-structured interview

[10]GAO, *Government Performance Management: Leading Practices to Enhance Interagency Collaboration and Address Crosscutting Challenges*, GAO-23-105520 (Washington, D.C.: May 2023).

questionnaire. After incorporating this feedback, we also conducted a pretest with a randomly selected sponsor of both foreign national associates and domestic associates. We made changes to the content and format of the questionnaire, based on the feedback we received. We then compared NIST's training efforts against selected leading practices in *Human Capital: A Guide for Assessing Strategic Training and Development Efforts in the Federal Government*.[11] The guide includes leading practices in four areas: planning/front-end analysis, design/development, implementation, and evaluation. We focused our review on practices in the implementation and evaluation areas because NIST had already developed its training courses and was implementing them during the time of our review.

We conducted this performance audit from May 2022 to December 2023 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.

[11]GAO, *Human Capital: A Guide for Assessing Strategic Training and Development Efforts in the Federal Government*, GAO-04-546G (Mar. 2004).

Appendix II: Background Checks for Foreign National Associates and Domestic Associates

Homeland Security Presidential Directive-12 mandates a federal standard for secure and reliable forms of identification issued by the government to its employees and contractors.[1] In accordance with this directive, Commerce submits applications on foreign national associates and domestic associates to the Defense Counterintelligence and Security Agency for background checks during the onboarding processes, prior to issuing a site badge.

The minimum background investigation requirements for foreign national associates accessing department facilities, resources, or activities are (1) a Special Agreement Check by the Defense Counterintelligence and Security Agency, (2) FBI fingerprint criminal history check, (3) FBI Investigations File (Terrorist Screening Database) name check, and (4) a systematic check of the U.S. Citizenship and Immigration Services alien verification program.[2] For foreign national associates with at least 3 years of residency in the United States within a 5-year period, the Defense Counterintelligence and Security Agency conducts a Tier 1, Questionnaire for Non-Sensitive Position investigation.[3]

NIST's background investigation requirements for domestic associates vary by the associate's length of stay.[4]

- An associate working at NIST for less than 30 calendar days undergoes a fingerprint check and must be escorted at all times.
- Associates working at NIST between 30 and 180 calendar days undergo a Special Agreement Check. This consists of a modified National Agency Check—including searches of national, state, and local law enforcement records—and checks made by the Office of Personal Management, Department of Defense, and FBI.
- Associates working at NIST between 180 and 365 calendar days undergo a National Agency Check and Inquiry. This consists of a National Agency Check plus written inquiries and record searches

[1]U.S. Department of Homeland Security, *Homeland Security Presidential Directive-12: Policy for a Common Identification Standard for Federal Employees and Contractors* (Aug. 2004).

[2]Department of Commerce, *Foreign Access Management Program*, DAO 207-12 (June 2021).

[3]The Defense Counterintelligence and Security Agency investigates individuals working for or on behalf of the executive branch of the United States.

[4]Department of Commerce, *Manual of Security Policies and Procedures* (Dec. 2012).

covering employment, residence, and education during the past 5 years.

Appendix III: National Institute of Standards and Technology (NIST) Implementation of Leading Practices for Interagency Collaboration

In assessing NIST's implementation of interagency collaboration practices, we found that the agency generally followed the leading practices for interagency collaboration discussed in GAO-23-105520 Government Performance Management: Leading Practices to Enhance Interagency Collaboration and Address Crosscutting Challenges.[1] In our prior work, we found that effective interagency collaboration benefits from certain leading practices, such as clarifying roles and responsibilities (see fig. 6).

Figure 6: Leading Interagency Collaboration Practices and Key Considerations

Source: GAO (data); GAO (icons). | GAO-24-106074

[1]GAO, *Government Performance Management: Leading Practices to Enhance Interagency Collaboration and Address Crosscutting Challenges*, GAO-23-105520 (Washington, D.C.: May 2023).

Below are additional details on our assessment for NIST's implementation of each of the eight leading practices. We found that NIST generally followed all eight leading practices.

Define Common Outcomes. Various policy documents and federal statutes establish cross-cutting goals for NIST and its collaborators. NIST is required to protect national security interests as detailed in the Department of Commerce's Strategic Plan for 2022-2026.[2] Also, National Security Presidential Memorandum 33 (NSPM-33), section 223 of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, and the CHIPS and Science Act of 2022 detail the responsibilities of federal research agencies to require disclosures of certain information from specified individuals that could indicate conflicts of interests and commitment.[3] NSPM-33 directs the Director of OSTP to coordinate with the Director of National Intelligence and other agencies, such as NIST, to enhance awareness of risks to research security and policies and measures for mitigating those risks.

Ensure Accountability. Various federal statutes and guidance implement deadlines for NIST and its collaborators. NSPM-33 requires federal research agencies to establish disclosure policies consistent with the memorandum by January 14, 2022.[4] The CHIPS and Science Act of 2022 further requires agencies to issue policies that include prohibitions on participation in certain foreign talent recruitment programs by August

[2]Department of Commerce, *2022–2026 Strategic Plan: Innovation, Equity, and Resilience - Strengthening American Competitiveness in the 21st Century* (Mar. 2022).

[3]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); William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No 116–283, div. A, tit. II, subt. B, § 223, 134 Stat. 3388, 3470-72 (codified at 42 U.S.C. § 6605); Research and Development, Competition, and Innovation Act, Pub. L. No. 117-167, div. B, tit. VI, subt. D, §§ 10631-10632, 136 Stat. 1366, 1664-66 (2022).

[4]NIST officials said the agency had not met this requirement because OSTP, one of the entities tasked with implementation of NSPM-33, had not yet issued certain uniform disclosure forms during the period of our review. Final Uniform Disclosure forms were issued in November 2023.

9, 2023.[5] Furthermore, NIST communicates progress on implementing a research security program via the Safeguarding Science Roundtable. Members of the roundtable have the opportunity to share feedback with one another. Based on NIST's contributions to the roundtable, ODNI formally recognized and commended NIST's research security program.

Bridge Organizational Cultures. NIST and its partners respond to differences in organizational cultures by documenting shared definitions. With respect to Commerce, DAO 207-12 establishes common definitions for terminology related to foreign national visitors and guests.[6] With respect to coordination with ODNI, officials from both NIST and ODNI said that they worked to overcome challenges inherent to the differing missions of each. NIST, as a federal research agency, operates in an environment that prioritizes the open sharing of knowledge in order to advance science. ODNI, as a member of the intelligence community, must restrict access to sensitive information to counter foreign threats. NIST officials said that their collaboration with ODNI and others on the Safeguarding Science initiative helps alleviate these cultural differences by creating shared definitions and best practices.

Identify and Sustain Leadership. Research security collaborations generally make clear when NIST is or is not the lead agency. The agency takes primary responsibility for developing and managing its own research security program with support from Commerce and ODNI. Under Commerce and agency policy, the Senior Bureau Official—in conjunction with agency operating units—reviews requests for foreign national associate access to departmental facilities, staff, and information.[7] In other areas, such as the development of federal

[5]Research and Development, Competition, and Innovation Act, Pub. L. No. 117-167, div. B, tit. VI, subt. D, §§ 10631 136 Stat. 1366, 1664-65 (2022). Section 10631 of the Act requires federal research agencies to, no later than August 9, 2023, issue policies that, among other things, prohibit agency personnel from participating in foreign talent recruitment programs, and prohibit making R&D awards for any proposal in which a covered individual is participating in a malign foreign talent recruitment program. The section directs OSTP, in coordination with the interagency working group established under section 1746 of the National Defense Authorization Act for Fiscal Year 2020 (Public Law 116–92), to issue uniform guidelines for federal research agencies that are to include these requirements within 6 months of enactment of the act. Federal research agencies are to issue policies utilizing these guideline within 1 year of the act's enactment. As of the date of this report, OSTP has not issued guidelines.

[6]Commerce, *Foreign Access Management Program*, DAO 207-12, (June 2021).

[7]Commerce, *Foreign Access Management Program*, DAO 207-12, (June 2021); NIST, *NIST Foreign National Associates Programs*.

disclosure requirements, NIST supports OSTP as the lead agency for such matters.

Clarify Roles and Responsibilities. Various policy documents and federal statutes establish roles and responsibilities for NIST and its collaborators. NSPM-33 clearly establishes the responsibilities of research agencies like NIST, such as the need to obtain disclosures from researchers. It also directs the Office of the Director of National Intelligence (ODNI) to coordinate intelligence community efforts to identify and assess capabilities, activities, and intentions of foreign actions as they related to research security. Additionally, it directs the Director of OSTP to coordinate with the Director of National Intelligence and other agencies to enhance awareness of risks to research security and policies and measures for mitigating those risks. Furthermore, Commerce policy DAO 207-12 establishes both department-level and bureau-level responsibilities with respect to all foreign nationals.

Include Relevant Participants. To implement its own research security program, NIST actively coordinates with Commerce's Office of Intelligence and Security as well as ODNI to obtain information about research security threats. When needed to respond to a potential risk, NIST also informs additional members of the Intelligence Community. In the development of federal research disclosure policies, NIST works with relevant parties, such as other federal agencies with scientific research programs, via the Safeguarding Science Roundtable.

Leverage Resources and Information. NIST receives information from Commerce through weekly briefings, an embedded liaison from the Office of Security, and a dedicated analyst from the Office of Intelligence and Security. The newly established Commerce Insider Risk Management Program Office will also work with NIST in the future. In addition, ODNI provides NIST with online tools to access information. One example is CITADEL, a system for screening specific individuals that NIST uses as part of its foreign national associate case review.

Develop and Update Written Guidance and Agreements. While there are no direct written agreements between ODNI and NIST, NSPM-33 establishes responsibilities for NIST and ODNI related for research

security.[8] For example, NSPM-33 states that ODNI should work with NIST on general awareness of and best practices for research security.

[8]According to GAO-23-105520, not all collaborative arrangements need to be documented fully through written guidance and agreements.

Appendix IV: National Institute of Standards and Technology's (NIST) Implementation of Selected Training Leading Practices

We assessed NIST's implementation of research security training practices for its NIST employees against the seven selected leading practices for training found in GAO-04-546G, *Human Capital: A Guide for Assessing Strategic Training and Development Efforts in the Federal Government* (see table 9).[1]

Table 9: Selected Leading Practices for Training

Component	Leading practice	Key questions
Implementation	Communicate importance of training	What steps do agency leaders take to communicate the importance of training and developing employees, and their expectations for training and development programs to achieve results?
	Encourage employee buy-in	What steps does the agency take to encourage employees to buy in to the goals of training and development efforts, so that they participate fully and apply new knowledge and skills when doing their work?
	Collect data	Does the agency collect data during implementation to ensure feedback on its training and development programs?
Evaluation	Evaluate effectiveness	To what extent does the agency systematically plan for and evaluate the effectiveness of its training and development efforts?
	Use performance data	What performance data (including qualitative and quantitative measures) does the agency use to assess the results achieved through training and development efforts?
	Incorporate feedback	How does the agency incorporate evaluation feedback into the planning, design, and implementation of its training and development efforts?
	Compare training	Does the agency compare its training investments, methods, or outcomes with those of other organizations to identify innovative approaches or lessons learned?

Source: GAO-04-546G. | GAO-24-106074

Additional detail and our assessment on each of the selected leading practices follows. NIST generally followed three, partially followed three, and did not follow one of the seven selected leading practices.

NIST generally followed two and partially followed one selected implementation practices for its research security training courses:

- **Communicate importance of training.** We found that NIST generally followed this leading practice. For example, NIST communicated on the importance and requirements of research security training during meetings and in writing, such as via emails and its intranet.
- **Encourage employee buy-in.** We found that NIST generally followed this leading practice. For example, NIST recruited a prominent NIST

[1]GAO, *Human Capital: A Guide for Assessing Strategic Training and Development Efforts in the Federal Government*, GAO-04-546G (Mar. 2004).

researcher and other internal ambassadors in the agency to communicate the importance of research security and foster cultural buy-in among staff. NIST officials said that during in-person reviews of foreign national associates, NIST management regularly reminds sponsors about research security trainings.

- **Collect data.** We found that NIST partially followed this leading practice. For example, NIST solicited some informal feedback on its training courses, including from training participants, security officials, and trainees' supervisors. NIST also has data on which staff have and have not completed required research security trainings. However, neither NIST nor Commerce has systematically collected a broader range of data across its training courses, such as requiring feedback from all course participants. NIST sponsors we interviewed cited several strengths of one of the training courses, the Counterintelligence Awareness Training, including covering appropriate information and frequency of that training course. However, they also provided suggestions for how NIST could improve that training course, such as by providing more examples of specific scenarios that staff may encounter (4 of the 12 NIST sponsors that we spoke to).[2]

NIST generally followed one, partially followed two, and did not follow one of the four selected leading practices on evaluating its training courses:

- **Evaluate training effectiveness.** We found that NIST did not follow this leading practice. NIST collects limited qualitative and quantitative data on its training courses, including receiving some feedback and requiring a self-assessment during one training course, the counterintelligence awareness training. However, neither Commerce nor NIST have a systematic way to evaluate the effectiveness of their training courses. NIST officials said they rely on employee buy-in and an openness to feedback to ensure its training courses are successful.
- **Use performance data.** We found that NIST partially followed this leading practice. NIST considered some informal feedback from

[2]We conducted semi-structured interviews with a non-generalizable random stratified sample of 12 NIST sponsors—four sponsors of foreign national associates, four sponsors of domestic associates, and four sponsors of both foreign national associates and domestic associates. We randomly selected participants from each of the three groups based on a list provided by NIST of all sponsors from the agency's Gaithersburg and Boulder campuses who were active in fiscal year 2022. Through these interviews, we obtained sponsors' perspectives on roles, responsibilities, and experiences with implementing research security-related policies, procedures, and training at NIST. See appendix I for additional information.

participants and their supervisors and assessed participants' understanding of one training course. However, NIST but has no systematic way to collect a broader range of data on its training courses. Commerce officials said they are considering more systematically collecting performance data in the future.

- **Incorporate feedback.** We found that NIST partially followed this leading practice. Based on feedback received, NIST has made some changes to its training courses, including updating one to state the intended goal and outcome of that course. However, neither Commerce nor NIST conducts evaluations of its research security training, preventing the agency from incorporating such assessments into the planning, design, and implementation of its training courses. Commerce officials said they are considering evaluating the effectiveness of the agency's training by adding formal evaluations in the future.
- **Compare training.** We found that NIST generally followed this leading practice because the agency has collaborated extensively with other offices within Commerce and met with other agencies to discuss research security training practices. For example, NIST shares best practices with other agencies through the Safeguarding Science roundtable.

Appendix V: Comments from the Department of Commerce

UNITED STATES DEPARTMENT OF COMMERCE
Office of the Acting Chief Financial Officer and
Assistant Secretary for Administration
Washington, D.C. 20230

November 22, 2023

Candice N. Wright
Director, Science, Technology Assessment, and Analytics
U.S. Government Accountability Office
441 G Street NW Washington, DC20548

Dear Ms. Wright

Thank you for the opportunity to respond to the GAO draft report entitled *NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY: Strengthening Disclosure Requirements and Assessing Training Could Improve Research Security* (GAO-24-106074SU).

The Department agrees with the recommendations and will prepare a formal action plan upon issuance of GAO's final report.

If you have any questions, please contact MaryAnn Mausser, Department GAO Audit Liaison, at (202) 482-8120 or mmausser@doc.gov.

Sincerely,

JEREMY PELTER Digitally signed by JEREMY PELTER Date: 2023.11.21 15:53:07 -05'00'

Jeremy Pelter

Deputy Assistant Secretary for Administration,
performing the nonexclusive functions and
duties of the Chief Financial Officer and
Assistant Secretary for Administration

Department of Commerce's Comments on
GAO Draft Report entitled *NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY: Strengthening Disclosure Requirements and Assessing Training Could Improve Research Security (GAO-24-106074SU)*

The Department of Commerce has reviewed the draft report and we offer the following comments for GAO's consideration.

Comments on Recommendations
The Government Accountability Office (GAO) made two recommendations to the Department of Commerce in the report.

- **Recommendation 3:** The Director of NIST should, consistent with applicable statutes and regulations, collect and review disclosures from domestic associates – including information on positions and appointments, current and pending research support, and participation in foreign talent recruitment programs – and require updates to these disclosures, as appropriate.

  Commerce Response: The Department of Commerce agrees with this recommendation.

- **Recommendation 4:** The Director of NIST should, in coordination with the Secretary of Commerce as appropriate, evaluate the effectiveness of research security training courses for NIST staff. For example, this could include collecting and analyzing employee feedback.

  Commerce Response: The Department of Commerce agrees with this recommendation.

Appendix VI: GAO Contact and Staff Acknowledgments

GAO Contact

Candice N. Wright at (202) 512-6888 or WrightC@gao.gov

Staff Acknowledgments

In addition to the contact named above, Tind Shepper Ryen (Assistant Director), Douglas G. Hunker (Analyst-in-Charge), Jenny Chanley, Louise Fickel, Lauren Gomez, Katie Hickman, Carolyn R. Johnson, Amy Pereira, Carl Ramirez, Joseph Rando, David Reedy, and Michael Yang 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 Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or 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 or (202) 512-7700

Congressional Relations

A. Nicole Clowers, Managing Director, ClowersA@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

Stephen J. Sanford, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548