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.