SMALL BUSINESS RESEARCH PROGRAMS

Additional Actions Needed to Incorporate Best Practices for Addressing Foreign Risks

GAO-26-107972 January 2026

A report to congressional committees.

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

What GAO Found

In March 2023, the Small Business Administration (SBA) established 12 best practices to help participating agencies manage risks posed by small business applicants in their Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) programs. GAO found that participating agencies and selected components have incorporated some best practices in their due diligence efforts, but gaps remain. For example, as of August 2025 all agencies had incorporated three of the 12 best practices, such as leveraging standardized foreign affiliation disclosures to capture consistent information. Most agencies incorporated additional practices, such as documenting a risk-based approach to their due diligence processes, and some incorporated practices such as determining "covered individuals" required to submit disclosures (see figure). The SBIR and STTR Extension Act of 2022 (Extension Act) requires participating agencies to incorporate the applicable best practices in their due diligence programs to the extent practicable. Doing so may improve agencies' ability to manage potential foreign risks.

Examples of Small Business Administration's Best Practices	Status of agencies incorporating best practices
Leverage standardized disclosures	●●●●●●●●●●
Document risk-based processes to due diligence	●●●●●●●●◒◒
Determine 'covered individuals'	●●●●●●◒◒◒○

● Agency incorporated ◒ Agency minimally incorporated
◒ Agency partially incorporated ○ Agency has not incorporated

Source: GAO analysis of agency information; toonsteb/adobestock.com (icons). | GAO-26-107972

The Extension Act also requires participating agencies to assess SBIR and STTR applicants' cybersecurity practices. GAO found that nine of the 11 participating agencies and selected components did so using a variety of mechanisms, including business intelligence tools and self-assessment forms. However, two of the agencies GAO reviewed—the National Science Foundation (NSF) and the U.S. Department of Agriculture (USDA)—are not assessing all applicants' cybersecurity practices. NSF officials told GAO that its applicants are small and nascent companies with limited electronic assets or systems to protect. USDA officials stated they previously understood training applicants on cybersecurity would suffice as an assessment. Until NSF and USDA incorporate cybersecurity assessments into their due diligence programs, they are at an increased risk of making awards to applicants that are vulnerable to cyberattacks.

SBA conducts information sharing meetings for agencies to discuss due diligence efforts, but GAO found agencies have gaps in how they have incorporated SBA's best practices to manage and reduce foreign risks. For example, GAO found some agencies are not incorporating certain best practices because, in part, they lack clarity on the intent of the practice or the best means to incorporate it. In August 2025, SBA officials acknowledged that based on the gaps and agency needs we identified in this report, additional opportunities may exist for SBA to engage with agencies on the challenges and impacts of incorporating the best practices and due diligence programs. The SBA-facilitated meetings could provide a discussion forum on agencies' challenges in incorporating the best practices, potential for additional guidance, and possible revisions.

Why GAO Did This Study

The SBIR and STTR programs fund research and development (R&D) performed by U.S. small businesses. In fiscal year 2023, federal agencies issued more than 6,300 such awards in areas such as defense and environmental protection. However, Congress and U.S. intelligence agencies have expressed concerns about foreign adversaries exploiting potential vulnerabilities in these programs and in entrepreneurial small businesses.

The Extension Act requires the 11 participating agencies to implement due diligence programs to assess the security risks posed by small business applicants. It includes a provision for GAO to issue a series of reports on the implementation and best practices of agencies' due diligence. This report is the third in this series and examines (1) agencies' incorporation of the best practices, (2) their assessments of applicants' cybersecurity practices, and (3) interagency mechanisms for sharing information on due diligence programs.

To determine the extent to which agencies have incorporated SBA's best practices, GAO reviewed agencies' policies and procedures for conducting due diligence and assessing applicants' cybersecurity practices. GAO also interviewed SBA and SBIR and STTR program officials at the participating agencies and selected components on the best practices.

What GAO Recommends

GAO is making a total of 26 recommendations: 25 to 10 agencies on incorporating SBA's best practices on due diligence programs and one to SBA on leveraging its interagency meetings to discuss the practices and help agencies address them. The agencies agreed with the recommendations.