November 2024

SMALL BUSINESS RESEARCH PROGRAMS

Agencies Identified Foreign Risks, but Some Due Diligence Programs Lack Clear Procedures

GAO Highlights

Highlights of GAO-25-107402, a report to congressional committees

Why GAO Did This Study

U.S. intelligence agencies have warned that emerging technology companies in the U.S could be targeted by foreign actors seeking to obtain proprietary data, advance their nation's economic and military capabilities, and threaten our national security. Small businesses seeking a SBIR or STTR award may face such risks. In fiscal year 2022, the 11 participating agencies collectively provided more than 6,500 SBIR and STTR awards valued at more than $4.4 billion to over 4,000 small businesses, according to the Small Business Administration.

The Extension Act includes a provision for GAO to issue a series of reports on the implementation of agencies' due diligence programs to assess security risks presented by small businesses seeking a federally funded award. This report, the second in the series, examines (1) the types of foreign risks agencies identified and mitigated; and (2) agencies' activities to refine their SBIR/STTR due diligence programs.

GAO reviewed 11 participating agencies' documents and interviewed relevant officials on their program implementation.

What GAO Recommends

GAO is making three recommendations—one each to DHS, EPA, and NASA—to document agreed-upon procedures between the SBIR/STTR program office and counterintelligence office for supporting due diligence reviews. All three agencies concurred with our recommendations.

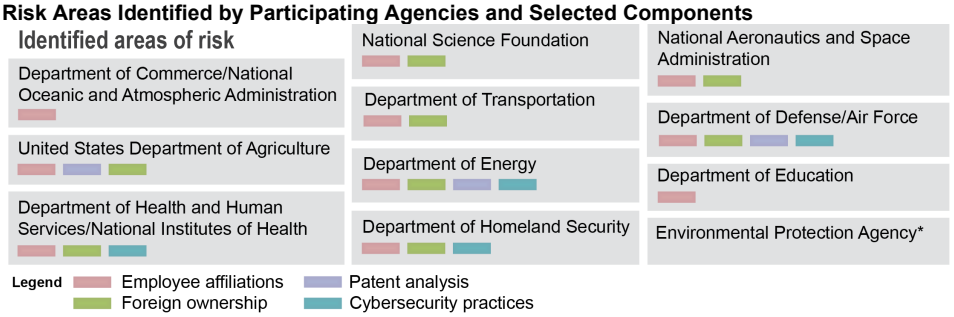
View GAO-25-107402. For more information, contact Candice N. Wright at (202) 512-6888 or wrightc@gao.gov.

What GAO Found

The Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) programs were established to enable small businesses to engage in federally funded research. However, these programs face risks of foreign actors seeking to illicitly acquire federally funded research and technologies. In response to requirements in the SBIR and STTR Extension Act of 2022 (Extension Act), the 11 federal agencies that participate in one or both programs implemented due diligence programs to assess the security risks posed by small business applicants.

GAO found that most participating agencies identified risks in at least one of the four required assessment areas: cybersecurity practices, patents, foreign ownership, and employee affiliations. Agencies most commonly told GAO they had identified risks associated with employee affiliations and ownership in foreign countries of concern (see figure). For example, one agency found that although an applicant did not disclose foreign affiliations for key personnel on their disclosure form, the Principal Investigator had likely received funding from a Chinese malign talent recruitment program—which seek to recruit researchers, sometimes with malign intent. Therefore, the agency did not make an award to that small business.

Risk Areas Identified by Participating Agencies and Selected Components



Source: GAO analysis of agency information. | GAO-25-107402

*According to Environmental Protection Agency officials, no risks have been identified to date.

GAO found that all participating agencies undertook activities to refine their due diligence programs in the first year of implementation. For example, some agencies acquired tools to aid in vetting applicants and conducted training for staff or applicants, and all used intra-agency support in conducting due diligence reviews. However, GAO found that three participating agencies—the Department of Homeland Security (DHS), Environmental Protection Agency (EPA), and National Aeronautics and Space Administration (NASA)—did not have documented processes for requesting analytical support and sharing information, including classified information, to support due diligence activities. For example, officials from EPA told GAO that there is no documented process for the program office to request counterintelligence analysis or for the counterintelligence office to communicate the resulting information to the program office. In interviews, all three agencies noted they plan to continue to use counterintelligence resources in their due diligence programs. Documenting processes and ensuring program officials have necessary information gathered and analyzed will be key as agencies continue to identify and mitigate risk in award decisions.