GAO Highlights

INDUSTRIAL SECURITY

Improved Risk Management and Stakeholder Engagement Needed to Help DOD Address Mission Gaps

GAO-26-107861 April 2026

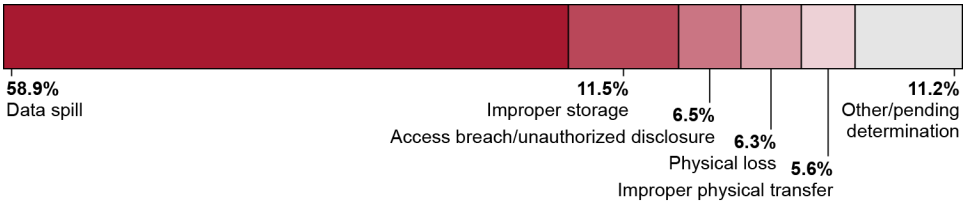
A report to congressional committees

Contact: Joseph Kirschbaum at kirschbaumj@gao.gov

What GAO Found

In fiscal year 2025, the Defense Counterintelligence and Security Agency (DCSA) conducted over 4,600 security reviews. The agency also documented over 800 security violations (see figure) and over 1,000 open security vulnerabilities associated with cleared contractor facilities. To conduct its industrial security mission, DCSA relied on over 470 industrial security mission personnel and spent over $160 million in fiscal year 2025.

Defense Counterintelligence and Security Agency (DCSA) Documented 815 Security Violations by Category Type, Fiscal Year 2025



Source: GAO analysis of Department of Defense information. | GAO-26-107861

Note: Security violations are incidents where a contractor fails to comply with the National Industrial Security Program Operating Manual's policies and procedures that could reasonably result in the loss or compromise of classified information. For example, data spills are when classified information appears, or "spills," onto an unclassified system. Security vulnerabilities are identified weaknesses in a contractor's industrial security program that could be exploited to gain unauthorized access to classified information or information systems accredited to process classified information.

DCSA has taken steps to manage risk with the industrial security mission. These include efforts to identify, assess, and respond to risk. However, DCSA has not addressed gaps to fully assess and respond to risks to its operational activities in line with DOD guidance on risk management. For example, DCSA has not identified and developed analytic capabilities to better support field operators' assessments of risk at the regional level. With such capabilities, the agency could identify the most significant regional trends affecting its overall performance objectives.

Further, DCSA began an initiative in 2019—the National Access Elsewhere Security Oversight Center (NAESOC)—aimed at mitigating risk partly through the reduction of workload on regional officials. However, participants in all 12 of the focus groups GAO conducted reported on the center's insufficient staffing, limited risk mitigation, and industry dissatisfaction. According to DCSA officials, the agency has not comprehensively assessed the NAESOC risk response effort, including identifying its resourcing needs and outcome-oriented performance goals. Doing so would be in line with DOD risk guidance to conduct regular assessments on risk responses.

Finally, DCSA identified challenges with its current industrial security data system of record and has begun developing a replacement. However, DCSA has not continuously engaged its end-users—DCSA regional and military department officials—throughout the development process, to include requirements development and other stages prior to testing. Without doing this, DCSA risks developing a replacement system with ongoing challenges.

Why GAO Did This Study

Foreign entities continue to attempt to illicitly obtain classified information and technology from industry thousands of times a year. DCSA, a Department of Defense (DOD) component, administers the DOD portion of the National Industrial Security Program (NISP), with the purpose of protecting classified information released to federal contractors, among others. DCSA has responsibility for ensuring that contractors properly access and store classified content for an estimated 90 to 95 percent of U.S. classified contracts across the federal government.

House Report 118-125 includes a provision for GAO to review DOD's administration of the NISP. This report addresses (1) the funding, personnel, and training DCSA dedicates to perform its industrial security mission, and the extent to which DCSA (2) has managed risks within the NISP's core operational activities and (3) is addressing challenges with the National Industrial Security System.

GAO reviewed documents and interviewed officials from DCSA, the military service components, and the National Archives and Records Administration. GAO also conducted a series of focus groups with 80 selected DCSA regional personnel who conduct industrial security operations.

What GAO Recommends

GAO is making four recommendations to DOD, including that the department provide enhanced analytic tools for regional operators; assess the NAESOC risk response effort; and ensure ongoing stakeholder feedback during the development of its new system of record. DOD concurred with the recommendations.