United States Government Accountability Office

Report to Congressional Committees

April 2026

INDUSTRIAL SECURITY

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

GAO-26-107861

GAO Highlights

INDUSTRIAL SECURITY

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

GAO-26-107861 April 2026

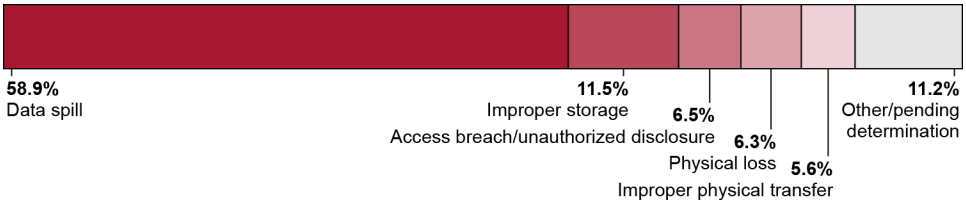
A report to congressional committees

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.

Contents

Tables

Figures

Abbreviations

DCSA	Defense Counterintelligence and Security Agency
DOD	Department of Defense
FOCI	foreign ownership, control, or influence
ISR	Industrial Security Representative
ISSP	Information System Security Professional
IT	information technology
NAESOC	National Access Elsewhere Security Oversight Center
NI2	NISS Increment 2
NISP	National Industrial Security Program
NISPOM	NISP Operating Manual
NISS	National Industrial Security System
OUSD (I&S)	Office of the Under Secretary of Defense for Intelligence & Security
USD (I&S)	Under Secretary of Defense for Intelligence & Security

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

April 24, 2026

Congressional Committees

In 2023, the Defense Counterintelligence and Security Agency (DCSA) identified and reviewed thousands of incidents that likely involved foreign entities attempting to illicitly obtain classified information and technology from industry. Threats to the industrial base include cyberattacks, espionage, exploitation of business relationships, insider threats, academia exploitation, intellectual property theft, and supply-chain disruptions.[1] DCSA, a Department of Defense (DOD) component, has responsibility for ensuring that contractors properly protect classified content, thus mitigating these threats.[2] The agency performs its industrial security mission as part of the National Industrial Security Program (NISP), which is governed by federal regulations.[3] DCSA administers the DOD portion of the NISP on behalf of DOD's components, as well as 35

[1]DCSA, *Targeting U.S. Technologies: A Report of Threats to Cleared Industry* (2023). The top three targeted technology categories were electronics; software; and command, control, communication, and computers. These three technology categories accounted for 36 percent of all suspicious contact reports. Additionally, the East Asia and the Pacific and Near East regions remained the most significant collectors of classified U.S. information and technology, collectively accounting for nearly two-thirds of all suspicious contact reports.

[2]*Targeting U.S. Technologies: A Report of Threats to Cleared Industry* (2023). The report lists a variety of threats to the industrial base to include cyberattacks, espionage, exploitation of business relationships, insider threats, academia exploitation, intellectual property theft, and supply-chain disruptions.

[3]*See* part 117 of title 32, Code of Federal Regulations. Part 117 is referred to as the NISP Operating Manual (NISPOM) and is issued and maintained by DOD in consultation with all affected agencies and with the concurrence of the Secretary of Energy, the Nuclear Regulatory Commission, the Director of National Intelligence, and the Secretary of Homeland Security. *See* Exec. Order No. 12,829, *National Industrial Security Program*, § 201(a), *as amended through* Exec. Order No. 13,708, *Continuance or Reestablishment of Certain Federal Advisory Committees*, 80 Fed. Reg. 60,273 (Sept. 30, 2015). The original Executive Order 12829 was issued in 1993 and amended several times. For purposes of this report, unless indicated otherwise, Executive Order 12829, as amended, refers to the most recent version of Executive Order 12829 as amended through Executive Order 13708 in 2015.

other government agencies.[4] Lastly, DCSA uses the National Industrial Security System (NISS), the agency's system of record, which is a web-based platform, to manage and oversee the industrial security of contractors working with classified information.

In 2024, we reported on national security risks posed when contractors consult for both the U.S. and Chinese governments, and in 2018 on how DOD administers the NISP to protect classified information, including program changes and challenges.[5]

House Report No. 118-125 accompanying a bill for the National Defense Authorization Act for Fiscal Year 2024 includes a provision for us to review DOD's administration of the NISP.[6] 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 with NISP's core operational activities and (3) is addressing challenges with NISS.

For all our objectives, we reviewed DOD issuances, policy, and processes for industrial security. We interviewed officials at DCSA, military department officials responsible for industrial security, officials from the National Archives and Records Administration, and

[4]DOD has entered into agreements with the following 35 departments and agencies for the purpose of providing industrial security services: the Departments of Agriculture, Commerce, Education, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, Treasury, and Veteran Affairs; Environmental Protection Agency; Executive Office of the President; Federal Communications Commission; Federal Reserve System; Government Accountability Office; General Services Administration; Millennium Challenge Corporation; National Aeronautics and Space Administration; National Archives and Records Administration; National Credit Union Administration; National Science Foundation; Nuclear Regulatory Commission; Office of Personnel Management; Overseas Private Investment Corporation; Privacy and Civil Liberties Oversight Board; Small Business Administration; Social Security Administration; U.S. Agency for International Development; U.S. International Trade Commission; U.S. Postal Service; U.S. Trade Representative; and U.S. Trade and Development Agency.

[5]See GAO, *Federal Contracting: Timely Actions Needed to Address Risks Posed by Consultants Working for China,* GAO-24-106932 (Washington, D.C.: Sept. 19, 2024) and GAO, *Protecting Classified Information: Defense Security Service Should Address Challenges as New Approach Is Piloted*, GAO-18-407 (Washington, D.C.: May 14, 2018). The former report made three recommendations, two of which are still open as of February 2026, and the latter report made one recommendation that has been addressed.

[6]H.R. Rep. No. 118-125, at 245-46 (2023).

representatives from an advisory government-industry group.[7] We also collected and analyzed focus group perspectives from DCSA's regional officials—in the Mid-Atlantic, Eastern, Central, and Western regions—responsible for the operational implementation of the NISP.

For objective one, we collected DCSA information on the resources, personnel, and training dedicated to DOD's implementation of the NISP. We reviewed DCSA data on the funding and personnel dedicated to DCSA's industrial security activities for fiscal years 2021 through 2025, as well as the training pipeline and related resourcing. We also reviewed DCSA data on the number of completed industrial security reviews for fiscal years 2021 through 2025, as well as the number and type of security violations and vulnerabilities identified by DCSA for fiscal year 2025.[8]

For objective two, we collected documentation on and evaluated DCSA efforts to manage risks with its industrial security mission, including efforts to identify, assess, and respond to risks. We conducted 12 focus groups of DCSA personnel across the four DCSA regions to collect perspectives on how the NISP is implemented. We asked questions on the impact, analysis, and mitigation of risks; 80 personnel, or 24 percent of their regional workforce, participated in the groups. Participants included managers, industrial security representatives, information systems security professionals, and counterintelligence specialists. (See appendix I for more details on the selection process.) We compared DCSA's risk assessment and response efforts against DOD guidance on risk management and leading practices in government re-organization efforts.[9]

For objective three, we collected documentation on DCSA's current industrial security IT system, NISS, and information on challenges users faced with this system. We used the same focus groups noted above to collect perspectives on operators' challenges with the system and

[7]Specifically, we discussed industrial security issues with the National Archives and Records Administration's Information Security Oversight Office.

[8]We assessed the reliability of this data—funding, personnel, training data—by interviewing DCSA about the controls they have implemented to ensure accuracy. We determined the data were sufficiently reliable for our purposes.

[9]DOD Instruction 5010.40, *DOD Enterprise Risk Management and Risk Management and Internal Control Program* (Dec. 11, 2024); GAO, *Government Reorganization: Key Questions to Assess Agency Reform Efforts*, GAO-18-427 (Washington, D.C., June 13, 2018).

participation in the development of an updated system. We assessed the extent to which DCSA has collected feedback and suggestions related to the functionality of NISS from end users and stakeholders, and whether they have a mechanism in place to collect feedback for the updated system. We assessed DCSA's user engagement efforts against leading practices in Agile software development and requirements from the user agreement.[10] See appendix I for full details on our scope and methodology.

We conducted this performance audit from October 2024 to April 2026 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

National Industrial Security Program (NISP) Overview and Agency Roles

The purpose of the NISP is to protect agency classified information released to federal contractors, among others.[11] Established by executive order in 1993, the NISP replaced industrial security programs operated separately by various federal agencies to serve as a single, integrated, cohesive industrial security program to protect classified information.[12]

To execute the program, the NISP Operating Manual (NISPOM) prescribes, among other things, industrial security procedures and practices, under Executive Order 12829 or successor orders, to safeguard U.S. government classified information that is developed by, or

[10]Office of the Under Secretary of Defense for Acquisition and Sustainment, *Agile Software Acquisition Guidebook: Best Practices & Lessons Learned from the FY18 NDAA Section 873/874 Agile Pilot Program*, version 1.0 (Feb. 27, 2020); GAO, *Agile Assessment Guide: Best Practices for Adoption and Implementation*, GAO-24-105506 (Washington, D.C.: Nov. 28, 2023 (reissued with revisions Dec. 15, 2023)).

[11]*See* 32 C.F.R. § 2004.1 (2026). For the purposes of this report, we will use "contractor" to refer to any party that the program applies to, including contracting companies, grantees, licensees, certificate holders, and their respective employees.

[12]Exec. Order No. 12,829, 58 Fed. Reg. 3,479 (Jan. 6, 1993).

disclosed to, contractors of the U.S. government.[13] Entities with key roles related to the NISP include the:

- **Director, National Archives and Records Administration's Information Security Oversight Office**. Maintains policy oversight over the NISP and, in implementing Executive Order 12829, as amended, ensures that the program operates as a single, integrated program across the executive branch of the federal government.[14]
- **Secretary of Defense**. Serves as the executive agent for the NISP with responsibilities that include issuing and maintaining the NISPOM and providing industrial security services for other federal agencies through agreements with those agencies.[15]
- **Director, DCSA**. Under the authority, direction, and control of the Under Secretary of Defense for Intelligence & Security (USD (I&S)), administers the NISP as a separate program element on behalf of DOD government contracting activities and those agencies with agreements with DOD for security services, among other things.[16] Covers, as part of its NISP administration, an estimated 90-95 percent of U.S. classified contracts across the federal government.[17]
- **Government Contracting Activity** (e.g., contracting agencies within military departments). Incorporates appropriate security requirement clauses in classified contracts and related materials and provides the

[13]*See* 32 C.F.R. §117.1 (2026). The NISPOM also prescribes requirements, restrictions, and other safeguards to prevent unauthorized disclosure of classified information and protect special classes of classified information.

[14]*See* 32 C.F.R. §§ 2004.1, 2004.10 (2026). Specifically, while the National Security Council provides overall policy direction for the NISP, the National Archives and Records Administration's Director of the Information Security Oversight Office is responsible for implementing and monitoring the NISP, in consultation with the National Security Advisor. Additionally, the Director of the Information Security Oversight Office serves as Chairman of the NISP Policy Advisory Committee, which is comprised of both government and industry representatives. The NISP Policy Advisory Committee advises the Director of the Information Security Oversight Office, as chairman, on all matters concerning the policies of the NISP, including recommended changes to those policies, and serves as a forum to discuss policy issues in dispute. Exec. Order No. 12,829, §§ 102, 103, *as amended*.

[15]*See* Exec. Order No. 12,829, §§ 201, 202, *as amended*; 32 C.F.R. § 2004.20 (2026).

[16]32 C.F.R. §117.6 (2026).

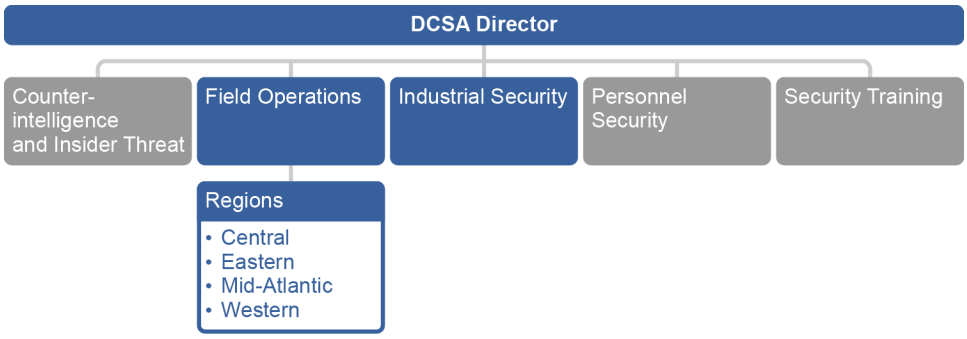
[17]DCSA, *National Industrial Security Program: State of the NISP* (January 2024). Specifically, DCSA administers the NISP on behalf of DOD components and 35 other agencies.

contractor with the security classification guidance needed during performance of the contract, among other things.[18]

DCSA Overview and Organization

In 2019, DOD established DCSA by merging three distinct organizations in response to direction in Executive Order 13869.[19] The three organizations were the Defense Security Service, the Office of Personnel Management's National Background Investigation Bureau, and DOD's Consolidated Adjudications Facility. As part of this consolidation, DCSA established five directorates to oversee and implement its security missions (see fig. 1). We focus primarily on the Industrial Security and Field Operations directorates in this report.

Figure 1: DCSA Organization



Source: GAO analysis of Defense Counterintelligence and Security Agency (DCSA) information. | GAO-26-107861

[18]*See* 32 C.F.R. § 117.13 (2026). According to the NISPOM, a government contracting activity is an element of an agency that the agency head has designated and delegated broad authority regarding acquisition functions, or a foreign government.

[19]Specifically, Executive Order 13869 amended another executive order to, among other things, direct: (1) the Secretary of Defense to rename the Defense Security Service as DCSA; (2) DSCA, in continuation of the former Defense Security Service, to serve as the primary DOD component for the NISP; (3) the Secretary of Defense and Director of the Office of Personnel Management, in consultation with the Director of the Office of Management and Budget and the Director of National Intelligence, to provide for the transfer of the functions of the Office of Personnel Management's National Background Investigation Bureau, including infrastructure and any appropriate personnel and resources, to DCSA. Exec. Order No. 13,869, *Transferring Responsibility for Background Investigations to the Department of Defense*, 84 Fed. Reg. 18,125, 18,125-128, § 2 (Apr. 24, 2019) (amending Exec. Order No. 13,467, *Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information*, 73 Fed. Reg. 38,103 (June 30, 2008)).

According to DCSA, the Industrial Security directorate oversees the NISP on behalf of the Secretary of Defense and performs compliance and security operations in accordance with the NISPOM. The directorate's industrial security mission goal is to reduce threats and mitigate vulnerabilities to classified and sensitive information and technology in the U.S. industrial base. The directorate oversees more than 12,500 cleared facilities and 5,500 classified IT systems in industry, according to an agency overview.[20] Cleared facilities that do not possess classified material or process classified information with IT systems onsite are referred to as "non-possessing," or category "E" facilities.

Further, the Field Operations directorate manages DCSA's set of security missions across the agency's four regions—Central, Eastern, Mid-Atlantic, and Western. Each regional headquarters integrates the operational field components of background investigations, industrial security, cybersecurity, and counterintelligence. The core industrial security-related tasks, particularly security reviews and authorization of contractors' classified IT systems, take place within this regional structure.

Contractor and DCSA Responsibilities for Cleared Facilities

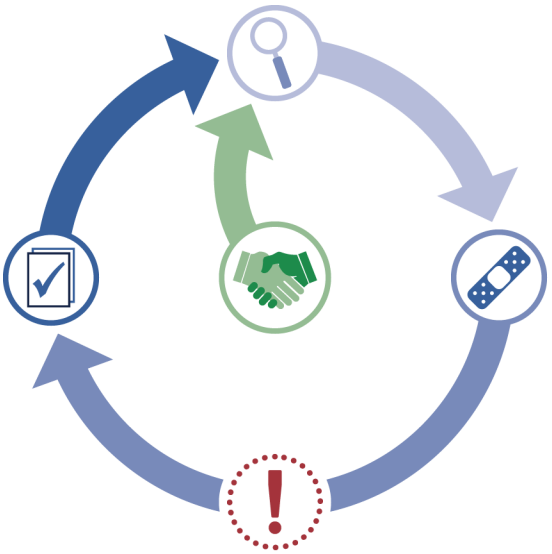
After DCSA determines that a contractor is eligible to access classified information and grants a facility security clearance, the cleared contractor officially enters the NISP. Once in the NISP, contractors establish a security program at cleared facilities and, depending on the facility, security measures may address a variety of industrial security issues.[21] In addition, contractors are required to implement insider threat programs, which are meant to mitigate the likelihood, risk, or potential that an insider, such as contractor employees with approved access to classified information, will use their authorized access, wittingly or unwittingly, to do harm to U.S. national security.

DCSA monitors cleared contractor facilities to determine their compliance with NISPOM requirements for protecting classified information primarily through periodic security reviews, as outlined in the NISPOM. See figure 2 for a summary of DCSA's process for monitoring contractor facilities in the program.

[20]DCSA, *DCSA Overview* (November 2024).

[21]For example, a contractor may be required to start using visitor logs or badges to track every person with physical access to a facility or establish separate computer systems for the sole purpose of storing classified information.

Figure 2: Overview of DCSA's Process for Monitoring Contractor Facilities Cleared to Handle Classified Information



If cleared, contractor enters the National Industrial Security Program and implements agreed upon security program or security measures to protect classified information. Once in the program, the contractor facility is subject to periodic security reviews.

DCSA conducts periodic security reviews to assess a contractor's compliance with the National Industrial Security Program Operating Manual.

Contractor addresses vulnerabilities identified by DCSA.

DCSA notifies the government contracting activity of the intent to invalidate or revoke a facility clearance, if DCSA determines that the contractor has made insufficient progress towards addressing security vulnerabilities.

Government contracting activity decides whether to proceed with performance on a contract involving classified information.

Source: GAO analysis of Defense Counterintelligence and Security Agency (DCSA) processes and interviews with DCSA officials; GAO (icons). | GAO-26-107861

DCSA determines the frequency of the security reviews, although DOD guidance sets a baseline frequency to generally conduct the reviews every 12 or 18 months.[22] DCSA officials responsible for ensuring NISP compliance include:

- **Industrial Security Representatives** (ISR): Conduct formal security reviews of contractor facilities and provide informal advice, assistance, and oversight. Additionally, ISRs receive suspicious contact reports from facility security and reports of security violations,

[22]DOD Manual 5220.32, *National Industrial Security Program: Industrial Security Procedures for Government Activities*, vol. 1 (Aug.1, 2018) (incorporating change 2, effective Dec. 10, 2021). Specifically, the manual states that facilities authorized to possess classified materials and all facilities cleared under foreign ownership, control, or influence mitigation mechanisms will be reviewed every 12 months, and all other facilities will be reviewed every 18 months. The manual also states that frequency of reviews will be consistent with the principle of risk management in accordance with Executive Order 12829, as amended, and the manual, and includes a process to defer, accelerate, or continue the baseline inspection frequency based on risk management methodology. The duration of security reviews and the size of the team conducting them vary by facility. For example, a single industrial security representative can perform a review of a small facility with no classified information stored on site in one day. By comparison, a large facility may require a lengthier review that involves additional DCSA officials, such as information system security professionals who review a facility's IT systems if they are needed to store or process classified information.

and coordinate with other DCSA entities to oversee all aspects of a contractor's industrial security program, among other tasks.[23]

- **Information System Security Professionals** (ISSP): Execute a program of certification, accreditation, and oversight of IT systems used to process and store classified information at cleared contractor facilities. ISSPs review risk packages that contractors submit to document security controls in place on their systems, and they work closely with ISRs to support facility security reviews, among other tasks.[24]
- **Field Office Chiefs and ISSP Team Leads**: Manage and oversee the ISRs and the ISSPs in the four regions. For example, field office chiefs determine schedules and priorities for security reviews.

ISRs and ISSPs located in the agency's four regions across the country generally conduct the security reviews. A contractor's facility clearance may be subject to invalidation or revocation if DCSA identifies certain vulnerabilities in a security review, among other things.[25]

DCSA Dedicates Funding, Personnel, and Training to Perform the Industrial Security Mission

DCSA funding and personnel for the industrial security mission fluctuated from fiscal year 2021 through 2025. The agency also provides resources to train both government and industry personnel for this mission and has recently expanded core training for DCSA personnel. DCSA has conducted over 4,600 security reviews for cleared facilities in fiscal years 2024 and 2025—identifying in fiscal year 2025 over 800 security violations and over 1,000 open security vulnerabilities.

[23]DCSA, *IS Manpower Assessment: Final Report* (June 15, 2023) provides an overview of key responsibilities of DCSA officials.

[24]*IS Manpower Assessment: Final Report* (June 15, 2023).

[25]See DOD Manual 5220.32, vol. 1. Specifically, DCSA will invalidate a cleared facility if there is a changed condition or non-compliance with other requirements as set forth in the NISPOM that affect the ability of a contractor to adequately protect classified information. Invalidation of a contractor's facility clearance is an interim measure that would render the contractor ineligible to receive new classified contracts or material, while providing an opportunity to correct deficiencies in its security program. Invalidation is a step DCSA can take before revoking a facility clearance. If the contractor refuses or is unable to take action to correct the situation that caused invalidation or has consistently demonstrated an unwillingness or inability to properly protect classified information, then DCSA can revoke the contractor's facility clearance.

DCSA's Industrial Security Mission Funding and Personnel Levels Have Fluctuated and Training Efforts Have Generally Expanded Since 2021

Funding

DCSA dedicates funding annually to support the industrial security mission (see table 1 for fiscal years 2021 through 2025). According to DCSA officials, the funding provided addresses labor and contract expenses for the industrial security mission across the industrial security and field operations directorates, as well as support for the research, development, test, and evaluation of NISS (the system of record for managing and documenting industrial security tasks and information), with some exceptions.[26]

Table 1: Defense Counterintelligence and Security Agency (DCSA) Industrial Security Mission Expenditures, Fiscal Years 2021 through 2025

Fiscal Year	Expenditures (in millions)
2021	$109.4
2022	$103.7
2023	$102.8
2024	$139.0
2025	$163.2

Source: DCSA information. | GAO-26-107861

Note: Expenditures provided by DCSA officials include mission-related labor expenses (e.g., DCSA official salaries); non-labor expenses (e.g., contract support); and research, development, test, and evaluation expenses and costs for the National Industrial Security System.

In 2023, DCSA officials reported that since the agency's establishment 4 years prior, funding and personnel had increased significantly agencywide to meet other priority efforts, such as personnel vetting, but that funding dedicated to the industrial security mission had remained relatively flat. In comparison, DCSA dedicated approximately $1.2 billion to $1.3 billion to its personnel vetting mission annually over the same

[26]For example, the expenditure figures for the industrial security mission in Table 1 do not include training costs for the industrial security mission, according to officials.

period.[27] Additionally, according to DCSA officials, the significant increase in funding from fiscal year 2023 through 2025 was due in part to initial research and development costs for a system to replace NISS and full-time positions added to expand capacity for oversight and administration of the NISP.

Personnel

DCSA maintains its industrial security workforce at its headquarters and across four regions that support and conduct industrial security operations. From fiscal year 2021 to 2024, the total number of industrial security personnel remained relatively static (see table 2).

Table 2: Defense Counterintelligence and Security Agency (DCSA) Industrial Security (IS) Mission Personnel, Fiscal Years 2021 through 2025

Fiscal year	IS headquarters administration	IS headquarters operations	IS field	Total
2021	14	67	319	**400**
2022	14	88	310	**412**
2023	17	83	294	**394**
2024	20	90	293	**403**
2025	18	132	329	**479**

Source: DCSA information. | GAO-26-107861

Note: DCSA officials provided these personnel numbers and reported that they come from the Fourth Estate Management Tracking System.

In fiscal year 2025, DCSA increased the overall number of industrial security personnel by 76, or approximately 19 percent, over fiscal year 2024. Forty-two of the 76 new personnel were added to DCSA headquarters in part to support a statutory requirement to expand DCSA's mission to vet entities, according to officials.[28]

Training

DCSA provides training both internally to personnel conducting industrial security tasks and externally to military department components and

[27]According to DCSA officials, they have little discretion to shift appropriated personnel vetting funding to industrial security.

[28]Specifically, in 2019, section 847 of the National Defense Authorization Act for Fiscal Year 2020 required DOD to improve the process and procedures for the assessment and mitigation of risks related to DOD contractors and subcontractors under any foreign ownership, control, or influence (FOCI) with existing or prospective contracts in excess of $5 million, generally excluding awards for commercial products and services. Pub. L. No. 116-92, § 847 (2019) (included, as amended, as a note to 10 U.S.C. § 4819). According to DCSA officials, the agency's Office of Entity Vetting has expanded to address this new mission.

cleared contractors outside the agency. DCSA officials reported that the agency has dedicated approximately $29.2 million to $43.8 million in funding each year from fiscal year 2021 through 2025 for training across all of its mission areas (e.g., personnel vetting, industrial security)—training supported by the security training element.[29] According to DCSA officials, less than 10 percent of this funding is dedicated to solely supporting industrial security mission training. DCSA officials also said some portions of this funding support training across multiple DCSA missions. DCSA reported 677,748 completions of NISP-related training courses by government and contractor personnel in fiscal year 2025, which represents approximately 12 percent of all course completions.

Government

DCSA provides industrial security training within the agency and to entities inside the military and across the federal government. DCSA reported that there were 339,612 completions of NISP-related courses by military service members and government personnel in fiscal year 2025. These included courses in insider threat, cybersecurity, and counterintelligence awareness, as well as training on the sources and handling of classified information, among others. Specifically, DCSA provided training focus on the following:

- *DCSA internal training*. According to DCSA documentation and officials, the agency established a Security Academy in October 2024 to ensure the mission readiness of DCSA personnel, including providing entry-level training to new ISRs through a school-house academy and an assigned field office advisor. As part of this training, ISRs now go through a three-phase process known as the Industrial Security Essentials Curriculum, which includes prerequisites, instructor-led training, and field application phases. According to DCSA, this mandatory training is designed to be foundational for the agency's ISRs to provide them with knowledge of NISP requirements and internal processes ISRs are expected to carry out.
- *Other federal and military training*. DCSA provides an online curriculum to security specialists across the federal government training them on the basic industrial security requirements of the NISPOM. In addition, DCSA provides non-security government personnel, such as military department contracting officers and their

[29]The source of the training expenditures data is DCSA's Center for the Development of Security Excellence. According to officials, this expenditure data was pulled from the Defense Agencies Initiative portal.

representatives, with an online curriculum so they have basic knowledge required to understand the industrial security program according to DCSA officials.

Industry

DCSA provides training to federal contractors. DCSA reported that there were 338,136 completions of NISP-related courses by contractor personnel. The curriculum is offered for facility security officers at both facilities that possess and those that do not possess on-site classified material to help them understand their roles and responsibilities. In addition, the NISPOM states that foreign investment can play an important role in maintaining the vitality of the U.S. industrial base, and that it is the intent of the U.S. government to allow foreign investment consistent with U.S. national security concerns.[30] Accordingly, DCSA also provides baseline training for director, voting trustees, and other leaders of federal contractors who play an important role in the effective implementation of foreign ownership, control, or influence (FOCI) mitigation agreements.[31] This online curriculum is intended to ensure that these industry leaders understand FOCI documentation and terms and the roles and responsibilities of the Government Security Committee, the U.S. government, and industry personnel involved in the FOCI process.[32] In fiscal year 2025, contractor personnel completed training in courses such as management of controlled unclassified information, operations security awareness, the identification and safeguarding of personally

[30]32 C.F.R. § 117.11 (2026)

[31]According to the NISPOM, DCSA or another oversight agency will consider an entity to be under FOCI when (1) a foreign interest has the power to direct or decide issues affecting the entity's management or operations in a manner that could either (a) result in unauthorized access to classified information, or (b) adversely affect performance of a classified contract or agreement; or (2) the foreign government is currently exercising, or could prospectively exercise, that power, whether directly or indirectly, such as (a) through ownership of the U.S. entity's securities, by contractual arrangements, or other means; or (b) by the ability to control or influence the election or appointment of one or more members to the entity's governing board. To obtain a facility clearance under the NISP, an entity under FOCI must have its FOCI factors favorably resolved by DCSA or another oversight agency, such as through mitigation or negation agreements. The details of such agreements vary based on several factors identified in the NISPOM. *See* 32 C.F.R. § 117.11 (2026).

[32]Each company that participates in the NISP and is under FOCI is required to form a Government Security Committee. According to DCSA, the committee's role is to ensure that the company maintains policies and procedures to safeguard classified information and export-controlled information in the possession of the company and that violations of those policies and procedures are promptly investigated and reported to the appropriate authority in a timely manner.

identifiable information, and the handling of sensitive compartmentalized information.

DCSA Personnel Identify Security Issues While Performing the Industrial Security Mission

DCSA is required to conduct periodic security reviews of contractor-owned facilities to ensure compliance with the NISP. Security reviews are a mix of in-person and remote reviews. Agency personnel conduct these reviews to identify and track any security issues—both security violations and vulnerabilities—involving cleared facilities. For example, in fiscal year 2023, DCSA reported that they were responsible for conducting security reviews at 9,611 contractor-owned facilities.[33]

DCSA officials conducting security reviews rate a contractor's security posture at the conclusion of each security review, and this security rating provides a description of the contractor's effectiveness in protecting classified information.[34] After the security review, DCSA provides each facility a timeline for addressing any security vulnerabilities and administrative findings dependent on the security rating issued.[35] DCSA officials provided information on the number of completed industrial security reviews from fiscal year 2021 through 2025 (see table 3).

[33]In fiscal year 2023, DCSA had 12,519 cleared contractor-owned facilities under its purview in the NISP. Of those, based on the baseline inspection frequency identified in volume 1 of DOD Manual 5220.32, one-third required a security review be completed every 12 months, while two-thirds required a security review every 18 months. The baseline inspection frequency for a given facility is based primarily on whether the facility is authorized to possess classified material and whether the facility is under FOCI; thus, according to DCSA data, 9,611 facilities required a security review in that fiscal year.

[34]The five possible ratings that can come out of an industrial security review are superior, commendable, satisfactory, marginal, and unsatisfactory.

[35]Security reviews that receive a rating of satisfactory or better will result in a follow-up written correspondence between DCSA and the contractor within 15 days for any cited vulnerabilities and within 30 days for administrative findings to identify how the contractor has addressed or mitigated any identified concerns and to determine if those actions are sufficient. For security reviews that receive ratings of marginal or unsatisfactory, officials are expected to review written responses on a contractor's mitigation efforts. Officials are also expected to complete a formal compliance review within 30 days of receiving an unsatisfactory rating and 120 days of receiving a marginal rating.

Table 3: Industrial Security Reviews Completed by DCSA, Fiscal Years 2021–2025

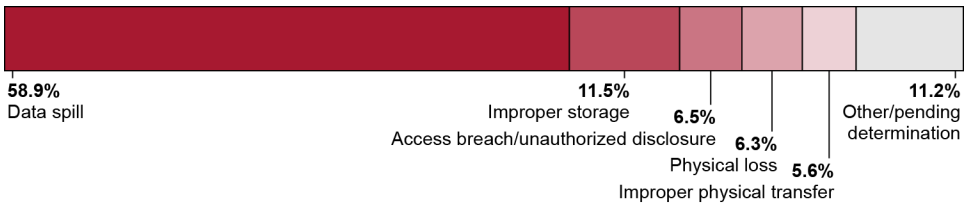
Fiscal year	Number of completed security reviews
2021	49[a]
2022	2,775[a]
2023	3,618
2024	4,692
2025	4,634

Source: Defense Counterintelligence and Security Agency (DCSA) information. | GAO-26-107861

[a]DCSA officials noted that the relatively smaller number of industrial security reviews the agency completed in fiscal years 2021 and 2022 was due to the COVID-19 pandemic. In lieu of security reviews, the agency conducted other remote monitoring activities as workarounds, referred to as continuous monitoring activities, according to officials. Additionally, the number of security reviews above includes those remote security reviews conducted by the National Access Elsewhere Security Oversight Center.

Security violations. DCSA documented 815 security violations that were open sometime during fiscal year 2025. Security violations are incidents where a contractor fails to comply with the NISPOM's policies and procedures that could reasonably result in the loss or compromise of classified information.[36] DCSA provides mechanisms to allow industrial security officials within DCSA or at other government or contractor levels to report any security violations as they are identified. Most security violations are reported by contractors and are related to data spills (i.e., classified information appearing, or "spilling," on an unclassified system) (see fig. 3).

Figure 3: Defense Counterintelligence and Security Agency (DCSA) Documented 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. 32 C.F.R. § 117.3 (2026). DCSA documented 815 security violations in fiscal year 2025 and categorized them as depicted above. For example, data spills are when classified information appears, or "spills," onto an unclassified system.

[36]32 C.F.R. §117.3 (2026).

DCSA officials work with contractors to investigate and mitigate, or close out, their security violations. As of September 2025, 576 security violations, or about 70 percent of the 815 security violations that were open sometime during fiscal year 2025, were closed. For additional information on the timeliness of addressing security violations at the end of fiscal year 2025, see appendix II.

Open security vulnerabilities. DCSA identified 1,032 open vulnerabilities as of September 2025. An open vulnerability is an identified weakness in a contractor's security program that indicates non-compliance with NISPOM requirements and that could be exploited to gain unauthorized access to classified information or information systems accredited to process classified information.[37] ISRs and ISSPs identify these vulnerabilities during their security reviews, and the top five categories comprise about 82 percent of them (see table 4).[38]

Table 4: DCSA Identified Industrial Security Open Vulnerabilities, Fiscal Year 2025

Category[a]	Number of open vulnerabilities[b]	Percentage of total open vulnerabilities
Procedures[c]	231	22.4%
Security Training and Briefings[d]	204	19.8%
Determination of Access to Classified Information[e]	162	15.7%
Reporting Requirements[f]	137	13.3%
Information System Security[g]	111	10.8%
All other categories[a]	187	18.1%

Source: GAO analysis of Defense Counterintelligence and Security Agency (DCSA) data. | GAO-26-107861

[a]DCSA aligns the categories for open vulnerabilities presented in the table with areas of the National Industrial Security Program Operating Manual (NISPOM). Five of these categories make up approximately 82 percent of all open vulnerabilities as of September 29, 2025. The remaining 18 percent of open vulnerabilities were spread across 10 other vulnerability categories, including "Safeguarding Classified Information," "International Security Requirements," and "Subcontracting."

[b]Vulnerabilities are identified weaknesses in a contractor's industrial security program that indicate noncompliance with the requirements of the NISPOM that could be exploited to gain unauthorized access to classified information or information systems accredited to process classified information. DOD Manual 5220.32, *National Industrial Security Program: Industrial Security Procedures for Government Activities*, vol. 1 (Aug.1, 2018) (incorporating change 2, effective Dec. 10, 2021).

[37]DOD Manual 5220.32, vol. 1.

[38]DCSA aligns the categories for open vulnerabilities with areas of the NISPOM. The remaining 18 percent of open vulnerabilities were spread across 10 other vulnerability categories such as Safeguarding Classified Information, International Security Requirements, and Subcontracting, among others.

[c]The Procedures category includes vulnerabilities found in contractors' security review procedures, standard practices and procedures, contractor security officials' procedures, and insider threat program procedures, among others.

[d]The Security Trainings and Briefings category includes vulnerabilities found with insider threat briefings, refresher training, initial security trainings, and facility security officer training, among others.

[e]The Determination of Access to Classified Information category includes vulnerabilities found with contractors providing employees with a valid need-to-know access to classified information, maintaining accurate records on employees' access to classified information, investigative requirements, and execution of classified-related non-disclosure agreements, among others.

[f]The Reporting Requirements category, as indicated in the NISPOM, includes vulnerabilities found with reporting certain events that may have an effect on an entity's or an employee's eligibility to access classified information, the establishment of internal procedures to ensure employees eligible to access classified information are aware of their respective security responsibilities, reports submitted to DCSA on contractors' adverse information or suspicious contactors, and submission of individual culpability reports, among others.

[g]The Information System Security category includes vulnerabilities found with contractors' information system security programs such as plans and procedures to assess and contain classified information from data spills, information sharing procedures, continuous monitoring program, and risk management framework, among others.

After identifying these vulnerabilities in a contractor's industrial security program, DCSA personnel then are responsible for following up with cleared contractors on both security violations and vulnerabilities. For example, agency officials check to see that contractors have addressed identified vulnerabilities, such as reporting their employees' foreign travel. As of September 2025, DCSA officials reported that 78 percent of open security vulnerabilities have been open for 90 days or less. See appendix II for more details on the timeliness of mitigating open vulnerabilities.

DCSA Has Various Steps to Help Manage Risk in the NISP but Has Gaps in Risk Assessments and Responses

DCSA Has Completed Various Steps to Manage Risk in the NISP

DCSA has completed some efforts and has others underway that identify, assess and prioritize, and mitigate risk to classified information in the NISP. Table 5 highlights in more detail selected DCSA efforts for its industrial security mission.

Table 5: Selected Defense Counterintelligence and Security Agency (DCSA) Efforts to Manage Risk in the National Industrial Security Program (NISP)

Risk management effort	Summary of effort	Risk management phase(s)
Industrial Security Mission Guidance (2024)	DCSA issues annual guidance to its industrial security mission elements where it identifies the primary risks with determining which security reviews should be accelerated or deferred. The agency identified the following, among others, as key risks: (a) length between security reviews (e.g., secret facilities going over 3 years without a security review), (b) facilities with high priority technologies targeted by foreign adversaries, and (c) facilities with foreign ownership, control, or influence going over 18 months without a security review.	Risk identification
NISP resource request's development of investment options (2023)	DCSA identified limited resources as a significant risk, enabling oversight of only 25-30 percent of the cleared industrial base that it said presented significant risk in the form of undetected security violations and vulnerabilities. The agency proposed three funding options—100, 70, and 30 percent investment options—to the Under Secretary of Defense for Intelligence and Security to respond to this risk of limited resources through increases in the workforce and other actions. We discuss this in more detail later in the report.	Risk identification
National Industrial Security Program: State of the NISP (2024)	In an agency overview of the NISP, DCSA identified insufficient human capital and technological tools as presenting high risks for undocumented adversary actions—creating opportunities for adversaries to operate undetected against existing classified industrial sites. The agency noted that the current ratio of field operators to number of facilities and systems is untenable.	Risk identification
Safeguard tool	Safeguard is a decision support tool that, according to agency documentation, gives DCSA's leadership a common operating picture of risk and communicates these risks within the industrial security base to various stakeholders. The model prioritizes security reviews by quantifying risk at the facility level—taking 17 risk indicators and establishing a risk score for each facility, according to documentation.	Risk assessment and prioritization
Industrial Security Manpower Assessment (2023)	DCSA assessed risk in its current workforce numbers. According to the document, the difference between the requirements of the industrial security mission and staffing numbers result in the agency accepting risk in the NISP. The assessment analyzed current authorized billets and workload requirements and offered quantitative estimates of additional billets required to effectively increase its oversight of facilities from the current 40 percent to 100 percent coverage.	Risk assessment
Undiscovered security vulnerabilities analysis	DCSA officials noted that, for every year that an industrial security review is delayed, they have found 1.5 to 2.5 times more security vulnerabilities. Risk compounds over time, according to officials. An agency figure showed that an increased amount of time between security reviews leads to a larger number of critical and acute vulnerabilities in a cleared facility.	Risk assessment
National Access Elsewhere Security Oversight Center (NAESOC)(2019)	NAESOC—overseeing approximately 5,000 cleared facilities comprising 40 percent of the NISP that are categorized as "non-possessing" or "access elsewhere"—is a risk management initiative intended to allow field operators to focus their efforts on more complex facilities that possess classified information or IT systems at their own facilities.[a] The center seeks to provide a reduction in facilities assigned to each operator.	Risk response

Risk management effort	Summary of effort	Risk management phase(s)
Cross-Directorate Joint Task Force for Remote Security Reviews (2025)	In fiscal year 2026 DCSA is implementing a task force to accelerate the agency's mission of conducting security reviews. The force will be managed and overseen by NAESOC, according to agency documentation. The task force aims to conduct 800 to 1,200 remote security reviews in fiscal year 2026 on eligible, "access elsewhere" facilities, thus complementing the conduct of in-person security reviews.[a] The aim, according to agency documentation, is to minimize risk across facilities.	Risk response
Industrial Security Essentials Curriculum (2024)	DCSA redesigned the mandatory foundational training for Industrial Security Representatives, called the Industrial Security Essentials Curriculum. The curriculum is specifically designed to provide these officials with the fundamental knowledge of NISP requirements and internal processes and procedures. According to officials, one goal of the new training is to provide consistency across the agency, mitigating in part the risk of inconsistent implementation of the NISP.	Risk response

Source: GAO analysis of DOD information. | GAO-26-107861

[a]"Non-possessing" or "access elsewhere" facilities are a specific type of facility whereby access to classified content or IT systems with classified content takes place at designated government sites or other cleared contractor locations.

We conducted focus groups with officials responsible for overseeing and conducting core operational activities for industrial security, particularly security reviews, in DCSA's four regions: Mid-Atlantic, Eastern, Central, and Western. Participants of focus groups we conducted confirmed many of the risks identified in industrial security-related documents, tools, and efforts reported by DCSA headquarters officials, as shown in table 5, as well as other risks. For example, participants in 10 of 12 focus groups reported that long intervals or delays between security reviews increase risk of program non-compliance and security vulnerabilities. Apart from the focus groups, DCSA officials stated that for every year that an industrial security review is delayed they have found 1.5 to 2.5 times more security vulnerabilities. Participants in 10 of 12 focus groups also reported that critical technologies are used as a key method to prioritize risk. (See appendix III for a more detailed list of focus group themes relating to risk management in the industrial security mission area.)

DCSA Has Gaps in How It Assesses and Responds to Risks in the Program

Although the agency has taken several steps to manage risk to its industrial security mission, as noted previously, we identified some gaps in how DCSA assesses and responds to risks in the NISP.

Risk Assessments

Examples of DCSA Focus Group Perspectives on Analytic Capabilities

"...I think more so it [NISS toolkit] is a logistical tool rather than an analytical product…"

"…ability to do reports would be nice and a little more user-friendly intuitive reports than the toolkit…"

"…we really need to be able to automate some of this [trend reporting] better…"

Source: Selected GAO focus groups with Defense Counterintelligence and Security Agency (DCSA) regional personnel. I GAO-26-107861

We found that while DCSA has taken steps to analyze risks at the national level, opportunities exist for identifying and developing analytic capabilities at the regional level. Participants in nine of the 12 focus groups we conducted reported that analytic capabilities and trend analysis for operators generally could be enhanced—such as with more automation—or communicated in a timelier manner. For example, DCSA headquarters disseminates a biweekly toolkit that pulls data from the system of record, NISS, and can be used to identify security-related findings and activities.

However, participants in seven focus groups reported that they found the toolkit's capabilities limited.[39] Specifically, these participants stated that the toolkit is not seen as an analytic product, is not user-friendly, or lacks automation. For example, a more desirable toolkit would auto-generate trend reports based on fields that regional officials select. Similarly, DCSA headquarters officials stated that they do not report on trends (i.e., there is no annual report compiling trends), but they brief industry on common non-compliance issues.

According to DOD Instruction 5010.40, the risk management process should be applied both top-down and bottom-up across all levels of the department; the bottom-up approach includes enabling tools and involves aggregating and analyzing risks to a DOD component's strategic goals and performance objectives.[40] Such tools could include analytic capabilities or other means to aggregate, assess, or identify trends in risks affecting a mission area. Additionally, federal internal control standards state that risks should be analyzed to estimate their significance, providing a basis for responding to the risks.[41] Further,

[39]The toolkit is an excel spreadsheet with numerous tabs—including tabs on active facilities, security violations, and open vulnerabilities—capturing industrial security mission data across all four regions.

[40]DOD Instruction 5010.40, *DOD Enterprise Risk Management and Risk Management and Internal Control Program* (Dec. 11, 2024). The instruction also defines risk assessment as a methodical approach to apply risk rating criteria to evaluate the overall exposure to identified risks associated with achieving strategic goals and performance objectives and risk prioritization as a systematic approach to determine the most critical risks to strategic goals and performance objectives at the DOD and DOD component levels.

[41]GAO, *Standards for Internal Control in the Federal Government,* GAO-25-107721 (Washington, D.C.: May 2025).

management estimates the significance of a risk by considering the likelihood of occurrence of risks to their mission objectives.

Officials are not able to fully assess their risks because DCSA has not identified and developed analytic capabilities and related trend analysis to better support field operators' assessments of risk at the regional level.[42] For example, participants in nine focus groups, DCSA headquarters, and military department headquarters officials responsible for industrial security reported that their current IT system, NISS, has a limited ability to query data.[43] Such a query function, and associated automated analytics, could support the identification and assessment of their most significant risks—and potentially identify the likelihood of occurrence of these risks to their mission objectives.

DCSA officials reported that their national biweekly toolkit has findings from facility security reviews, which can be filtered by region. However, as noted previously, participants in seven focus groups reported that this toolkit's analytic capabilities are limited and need improvements. Further, facilities in individual regions have different attributes, according to DCSA officials, so analysis within regional portfolios may generate trends that differ substantially from a nationwide perspective. For example, officials in the Mid-Atlantic region reported that each region is different and thus faces different challenges; they noted that their region has about 45 percent of the agency's facilities under FOCI, even though they are only one of four regions.

While DCSA has efforts to assess risk at the national level, identifying and developing enhanced analytic tools for use at the regional level could help position field operators to identify trends unique to their regions and target efforts at highest risk. A bottom-up approach leveraging useful analytic capabilities could more easily aggregate and analyze risks at the

[42]DCSA, *Capability Needs Statement (CNS) for Industrial Security*, version 1.5 (July 15, 2025) describes the agency's required capabilities for a modernization of systems to support the industrial security mission, NISS Increment 2 (NI2), but these modernizations have not been implemented to date. In a document annex, the agency expresses the intent to, "*implement analytical tools* to discover, understand, monitor, and manage risk across the defense industrial base, using platform services, building case management, all-source data operations, and artificial intelligence-enhanced data aggregation analysis on the latest secure architecture." Deploying these projected capabilities could meet the need for operators' access to analytic capabilities and trend analysis that would support their assessment and prioritization of risk at the regional level. However, these capabilities do not necessarily need to be provided through the NI2 deployment.

[43]A later section of this report will discuss in more detail the limitations of NISS.

regional level—in addition to the national level—and thus identify the most significant regional trends affecting the agency's overall performance objectives. Such tools are particularly critical in an environment of constrained resources as they can support the assessment and prioritization of risks.

Risk Responses

DCSA also has not fully responded to identified risks to its industrial security mission. We identified three key challenges facing DCSA in responding to their risks. First, in 2023, DCSA officials identified their limited resources as a significant risk, noting that DCSA was "resourced to conduct required NISP oversight of only about 25-30 percent of the cleared industrial base" at the time.[44] DCSA offered a package of proposals to USD (I&S) to respond to and mitigate this risk, in part through workforce increases.[45] Specifically, DCSA proposed three investment options—100, 70, and 30 percent—to reduce risk, and projected additional security violations, security vulnerabilities, and undetected threats that could be identified based on the varying options.[46] For example, the 100 percent investment option—DCSA's recommended proposal—aimed to identify nearly all of the projected security violations and vulnerabilities while adding 230 ISRs, 164 ISSPs, 25 field office chiefs, and 17 ISSP Team Leads across the Future Years Defense Program. The proposal noted the number of facilities required by policy to be reviewed in fiscal year 2023 and offered estimates on the number of unidentified security violations and vulnerabilities—based on risk projections—that could be potentially identified at varying investment levels, if more of the required security reviews could be done.

In September 2025, OUSD(I&S) officials reported they had not implemented any of the agency's proposed investment options. These officials stated that DCSA's memorandum with investment options showed limited policy requirements or linkage to the industrial security mission. Officials also told us there was a lack of data or requirements to take further action. As a result, DCSA officials told us that they have not

[44]DCSA Director Memorandum, *National Industrial Security Program Resource Request* (June 15, 2023).

[45]USD (I&S) exercises authority, direction and control over DCSA; oversees policy and management of the NISP; and directs, administers, and oversees the NISP to ensure that the program is efficient and consistent. DOD Directive 5143.01, *Under Secretary of Defense for Intelligence and Security (USD(I&S))* (Oct. 24, 2014) (incorporating change 2, effective Apr. 6, 2020); DOD Manual 5220.32, vol. 1.

[46]DCSA Director Memorandum, *National Industrial Security Program Resource Request* (June 15, 2023).

been able to hire additional personnel—ISRs, ISSPs, or others identified in the proposal options—to conduct core operational activities relating to industrial security across the regions.[47] DCSA headquarters officials emphasized that resourcing has been an "enduring challenge," contributing in part to the agency completing around one-third of their required industrial security reviews in fiscal year 2023, according to an agency report.[48]

Second, DCSA's regional operators in all our focus groups reported that the implementation of the National Access Elsewhere Security Oversight Center (NAESOC)—an initiative that aimed to mitigate risk partly through the reduction of workload on regional officials—has been ineffective. The NAESOC was established in 2019 to advise and assist up to 4,500 of approximately 8,000 "access-elsewhere" facilities, according to agency officials (i.e., facilities with a lower risk level that do not possess classified information or classified IT systems). Later in 2024, DCSA officials reported that they gave the center the mission of coordinating a national approach to remote security reviews on these non-possessing facilities while conducting these reviews itself without additional resources. In June 2025, DCSA officials reported that the NAESOC was staffed with 11 civilians and 47 contractors.

According to DCSA officials, NAESOC is intended to allow regional operators to focus their efforts on more complex facilities that possess classified information or IT systems at their own facilities. Therefore, the center oversees cleared facilities that do not possess classified information onsite and have no FOCI or classified IT systems—approximately 5,000 cleared facilities comprising 40 percent of the NISP, according to an agency overview of the industrial security mission area.[49]

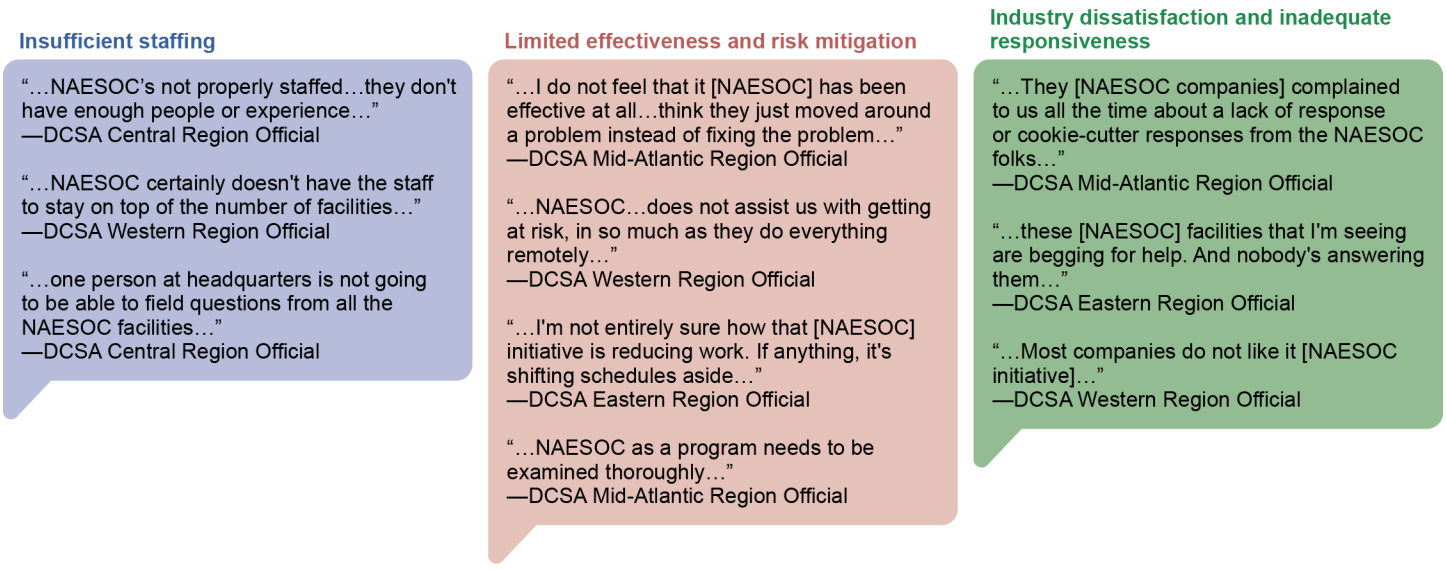
[47]As shown in table 2, the number of regional, or field, industrial security personnel (e.g., ISRs, ISSPs) remained static from fiscal year 2023 through 2024. Additionally, when comparing the number of regional industrial security personnel from fiscal year 2021 against their number in fiscal year 2025—numbers reported in September 2025—the increase was about 3 percent.

[48]DCSA, *National Industrial Security Program: State of the NISP* (January 2024).

[49]DCSA, *National Industrial Security Program: State of the NISP* (January 2024). In addition to this criterion, according to DCSA officials, the number of cleared facilities within NAESOC is also based on other criteria—e.g., facility does not provide support to critical programs or technology; the facility has had a security review within the last 12 months—so the number of facilities in NAESOC can vary.

However, we found that DCSA has not comprehensively assessed various aspects of NAESOC. Participants in all 12 focus groups expressed negative reviews of the NAESOC. Specifically, the participants in focus groups reported on the center's insufficient staffing, limited effectiveness and risk mitigation, and industry dissatisfaction and inadequate responsiveness. See figure 4 for selected comments illustrating these themes. (See appendix III for a complete list of risk management-related themes.)

Figure 4: Selected Defense Counterintelligence and Security Agency (DCSA) Regional Officials' Perspectives on the National Access Elsewhere Security Oversight Center (NAESOC)



Source: GAO interview responses. | GAO-26-107861

Note: We conducted 12 focus groups with DCSA officials responsible for overseeing and conducting industrial security-related tasks across the agency's four regions: Mid-Atlantic, Eastern, Central, and Western. Officials' testimonial comments above were selected to represent three predominant themes related to the NAESOC.

NAESOC senior officials reinforced these challenges highlighted by DCSA regional officials above and spoke about other challenges. For example, NAESOC leaders reported that they are understaffed, with resources being a challenge. These officials stated that they experienced an increase in scope without resource alignment, noting that the center gets additional missions assigned annually without accompanying resources or formal project plans. Further, NAESOC officials highlighted that the center measures outputs—such as continuous monitoring

alerts—but it is difficult to measure performance outcomes.[50] This situation challenges NAESOC's ability to measure success or show impact on the industrial security mission, according to officials.

Third, officials reported that there is an organizational divide in how NAESOC operates between two DCSA directorates, Industrial Security and Field Operations. According to the NAESOC officials, partly because the center falls under the Industrial Security directorate, NAESOC does not receive the same level of administrative or dedicated IT support at the Field Operations directorate, even though the center performs field mission work.[51]

According to DOD Instruction 5010.40, for identified risks to its strategic plans, a DOD component like DCSA should determine underlying root causes, develop and implement specific risk response action plans, and establish clear accountabilities to prevent overall risk from exceeding DOD's risk appetite levels.[52] In this context, risk response is a deliberate approach to consider, implement, and document appropriate actions to accept, avoid, mitigate, or share risk in alignment with risk appetite. DOD components—as part of risk management—are also to conduct regular assessments to ensure effective risk response.[53] Additionally, according to lessons learned in government reorganizations—for which the creation and operation of NAESOC is an example—an agency should establish clear outcome-oriented goals and performance measures.[54] In these reorganizations, an agency should establish a dedicated implementation

[50]According to an agency overview of the NAESOC, Continuous Monitoring is a program within NAESOC that uses an enhanced risk-management approach to facilitate early detection of a cleared facility's security risk in near real-time using multiple automated data streams, such as commercial and government sources; the process generates alerts that are sent to the regions for further investigation.

[51]Similarly, in a 2025 agency document laying out risks to the NAESOC, the center's lack of integration with the field is listed as a significant risk to its mission. It stated that "if NAESOC does not have information sharing channels in place with the Field Operations [directorate] due to organizational structure, then mission execution is dysfunctional and drives inefficiencies and risk is not appropriately addressed."

[52]DOD Instruction 5010.40. The instruction defines risk appetite as the amount of risk, on a broad level, an organization is willing to accept in pursuit of its objectives. Risk appetite helps senior leadership understand and define the level of risk on a broad level that DOD is willing to accept in pursuit of its strategic goals and performance objectives.

[53]DOD Instruction 5010.40. Federal internal control standards also state that management may need to periodically assess their risk response actions.

[54]GAO, *Government Reorganization: Key Questions to Assess Agency Reform Efforts*, GAO-18-427 (Washington, D.C., June 13, 2018).

team that has the capacity, including staffing and resources, to manage reform.[55]

DCSA has not fully responded to risks to its industrial security mission because USD(I&S) has not taken deliberate steps to accept, mitigate, or share the risks raised by DCSA regarding a limited workforce for industrial security. In other words, USD(I&S) has not implemented a risk response plan with specific actions to address DCSA-identified risks. Such actions could include, as appropriate, accepting the risk of conducting fewer security reviews and changing the periodicity of reviews to reflect a higher risk appetite, or taking steps to mitigate or avoid such risks.

According to OUSD(I&S) officials, they are considering both changing the periodicity of required security reviews and shifting policy in such a way that military departments would be responsible for conducting more of the industrial security work. Officials stated that these considerations are part of an effort to update DOD Manual 5220.32 on industrial security.[56] These deliberate responses to risk could implicitly accept the DCSA-identified risk of its current workforce levels—by adjusting the overall risk appetite in this mission area—or explicitly share more of the risk with organizations outside DCSA (e.g., the military departments), respectively. However, as of January 2026, these considerations and any specific policy changes had yet to be coordinated across the department, and the update to DOD's industrial security manual will likely not be issued until sometime in 2026, according to OUSD(I&S) officials. Thus, it is unclear whether the actions under consideration will be eventually implemented, as well as what form they will take and whether they would appropriately address the risks as identified by DCSA.

Further, DCSA is unable to fully respond to risk because it has not comprehensively assessed the NAESOC risk response effort, including identifying its resourcing and personnel needs, outcome-oriented performance goals, and evaluating its organizational alignment with other

[55]GAO-18-427.

[56]Under DOD Manual 5220.32, volume 1, DCSA currently conducts security reviews every 12 or 18 months depending on the facility and risk management considerations. However, according to officials, the USD(I&S) could choose to lengthen the periodicity requirements for certain facilities, such as the non-possessing ones, as part of its update of this manual. Additionally, OUSD(I&S) officials noted that an updated manual could specify and place more industrial security responsibilities on the military departments for security review and assessment activities.

directorates, according to officials. DCSA has planned an after-action review to assess the effectiveness of its cross-directorate joint task force (see table 5) and its strategies to execute remote security reviews in October 2026. The agency has also initiated a separate pilot effort called “Operation Torch” that proposes to hand off more of the tasks associated with security reviews to contractor personnel. DCSA plans on conducting an after-action review of this pilot in the summer of 2026. Taken together, these two planned after-action reports could form the core of a more comprehensive assessment of the NAESOC risk response effort, including its long-term personnel needs, performance goals, and organizational alignment with other directorates (e.g., field versus headquarters). With limited details on the scope of these after-action reviews, however, it is unclear if they will comprehensively assess the NAESOC effort, including the aspects identified above related to outcome-oriented performance goals and organizational alignment.

NAESOC and DCSA leadership noted that they are bringing in additional agency personnel in fiscal year 2026 to the center to address more of their workload. Specifically, a concept of operations for the joint task force shows the center will receive eight detailees from the regions, who will work for the task force—overseen by NAESOC—primarily to complete remote security reviews. However, without an assessment of the NAESOC risk response effort, DCSA would not be positioned to determine if the eight detailees would address its needs. According to agency documentation, the center will see an increase in its workload of remote security reviews from 100 in fiscal year 2025 to between 800 and 1,200 in fiscal year 2026. Further, the planned increase in personnel does not directly address other NAESOC challenges, such as the absence of outcome-oriented performance goals or a perceived lack of organizational alignment with the Field Operations directorate.

If OUSD(I&S) implemented a risk response plan with deliberate steps to accept, share, or mitigate the DCSA-assessed risk of a limited workforce for industrial security, it could move forward with addressing this risk, and help define DOD’s overall risk appetite in this mission area. OUSD(I&S)—in taking such steps—could also clearly communicate and document its risk decisions as it oversees the policy and management of the NISP.

Additionally, if DCSA comprehensively assessed the NAESOC initiative, it could provide more detailed insights into NAESOC’s resourcing and personnel needs, outcome-oriented performance goals, and the center’s organizational alignment with the Field Operations directorate and regional offices, among other things. Such an assessment could

potentially identify opportunities to enhance coordination between DCSA's regional offices and NAESOC and could also lead to potential changes in NAESOC that may improve industry satisfaction with the center and overall risk mitigation.

DCSA Plans to Replace Its National Industrial Security System but Has Not Fully Engaged Stakeholders to Address Challenges

DCSA Identified Challenges with the National Industrial Security System

DCSA has identified a series of capability challenges and needed improvements within NISS, its current industrial security system of record. These include a need for improvements in automation, encrypted communications, data integration, system interoperability, metrics and dashboards, search and analytic tools, and record management capabilities related to its oversight activities and actions for companies in the NISP. Officials from DCSA headquarters, regional officials in the focus groups, and military department officials responsible for industrial security highlighted numerous specific challenges with NISS as follows in table 6. (See appendix IV for a more detailed list of NISS challenges identified through our interviews.)

Table 6: Selected Challenges with the National Industrial Security System (NISS) Identified by the Defense Counterintelligence and Security Agency (DCSA) and Military Department Officials

NISS challenge	Selected DCSA and military department officials' comments
Slow system performance	NISS often shows lag time, which sometimes results in officials' failure to save changes or duplication of work.
Frequent system downtime	NISS has significant periods of unavailability.
Limited ability to query system data	Some searches in NISS require labor-intensive searching through multiple records.
Limited interoperability with other necessary systems	NISS does not automatically update from other related systems. For example, the lack of interoperability with the Enterprise Mission Assurance Support Service results in data reliability issues and additional work for DCSA officials.[a] NISS also lacks interoperability with other key systems used by industrial security personnel, including the National Industrial Security Program (NISP) Contract Classification System and the Defense Information System for Security.

NISS challenge	Selected DCSA and military department officials' comments
Lack of trend reporting capabilities	NISS does not have the ability to identify trends over time based on system data. DCSA officials must generate trend reporting and other analytic products from the system by exporting the data and using workarounds.
Limited visibility by military departments into facility compliance	Military departments have limited access to NISS data, hampering visibility into cleared facilities for which DCSA is responsible for ensuring NISP compliance (i.e., while facilities perform on military department classified contracts, departments have challenges seeing the status of NISP compliance).
Lack of user-friendliness	Navigation through NISS is often difficult. For example, the system lacks a "back button," and officials reported needing to frequently duplicate work or to manually enter data.

Source: GAO analysis of DOD industrial security interviews and focus groups. | GAO-26-107861

[a]According to DCSA officials, DCSA cybersecurity specialists rely on the Enterprise Mission Assurance Support Service to capture and assess contractor classified information systems. However, these specialists must usually manually enter such information into NISS, due to the lack of a reliable interface between the two systems.

Industry representatives we interviewed from the NISP Policy Advisory Committee also reported that NISS often has been unavailable, and that the process for submitting updated company information within NISS is often cumbersome. Specifically, these industry officials stated that updating facility changes—such as changes in ownership required by the NISPOM to be reported—within NISS can take a year to approve, and facilities can only submit one change at a time, even though they may face multiple changes in a year. DCSA participants in three of 12 focus groups also brought up the challenges of industry partners working with NISS, citing the need for industry personnel to manually reenter data into NISS from pre-existing documents.

DCSA Had Limited Stakeholder Input Before Beginning Development of a Replacement Information System

In response to challenges with NISS, DCSA began developing a replacement system, known as NISS Increment 2 (NI2), in April 2024. Among other things, NI2 is intended to deliver a multi-disciplinary, common risk picture across the defense industrial base and provide expanded access to systems, analytic tools, and data to DCSA government customers.[57] NI2 capabilities are projected to include:

- a role-based case management application that provides automation, records management, encrypted communications, transparency, data integration, metrics and dashboards;
- an on-demand knowledge base with global search, visual analytics, and reports for general users; and

[57]DCSA, *Capability Needs Statement (CNS) for Industrial Security*, version 1.5 (July 15, 2025).

- an expanded capability for administrators to customize dashboards and widgets, reports, and visual analytics.

DCSA officials stated they expect to develop NI2 in three modules, or capability groups, focused on: NI2 architecture and a module focused on assessing FOCI risks to DOD contracts (or capability group 1);[58] updating DCSA's NISP Contract Classification System (capability group 2);[59] and replacing the core elements of NISS, including facility clearance information and NISP compliance data (capability group 3). According to DCSA officials, the agency plans to spend approximately $163 million in developing NI2. NI2's first capability group is projected to begin operating in early 2026, with NI2's last capability group to be deployed sometime in fiscal year 2028, according to DCSA officials.

DCSA is developing NI2 using a modern iterative software development methodology known as Agile.[60] Agile emphasizes the early and continuous delivery of working software by engaging stakeholders in collaboration early in the program and continuously adapting to changing requirements.[61] DCSA has written a user agreement for NI2, wherein the agency has identified roles and responsibilities for user representatives

[58]Section 847 of the National Defense Authorization Act for Fiscal Year 2020 requires DOD to improve the process and procedures for the assessment and mitigation of risks related to DOD contractors and subcontractors under any FOCI with existing or prospective contracts in excess of $5 million, generally excluding awards for commercial products and services. Pub. L. No. 116-92, § 847 (2019) (included, as amended, as a note to 10 U.S.C. § 4819). The first module of NI2 is to address this requirement, which also applies to contracts that do not require a facility clearance, and as such, is not directly linked to the NISP.

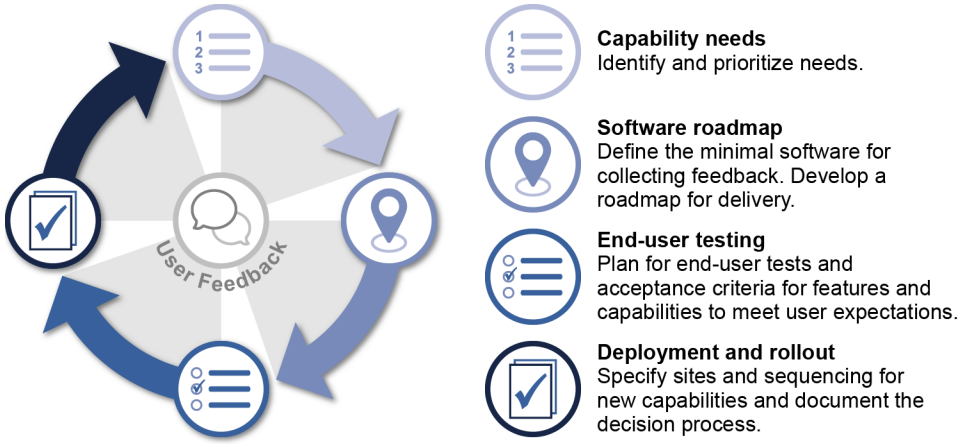
[59]The NISP Contract Classification System is a DOD system intended to improve upon the processing of DD Form 254, "Contract Security Classification Specification." DD Form 254 is the principal authorized means for providing security classification guidance to a contractor requiring access to classified information.

[60]GAO has reviewed challenges in Agile development of another DCSA program, National Background Investigation Services (NBIS). See GAO, *Personnel Vetting: Sustained Leadership is Critical to DOD's New Approach to Its Background Investigation System*, GAO-25-108721 (Washington, D.C.: Sept. 16, 2025); GAO, *Personnel Vetting: DOD Needs to Improve Management of the National Background Investigation Services Program*, GAO-24-107616 (Washington, D.C.: June 26, 2024).

[61]For more information on Agile, please see the following: GAO, *Agile Assessment Guide: Best Practices for Adoption and Implementation*, GAO-24-105506 (Washington, D.C.: Nov. 28, 2023 (reissued with revisions Dec. 15, 2023)); and Office of the Under Secretary of Defense for Acquisition and Sustainment, *Agile Software Acquisition Guidebook: Best Practices & Lessons Learned from the FY18 NDAA Section 873/874 Agile Pilot Program*, version 1.0 (Feb. 27, 2020).

as part of the development process.[62] Among other things, the NI2 user agreement states that two or more users from each community should contribute to the development of the Capability Needs Statement. Additionally, DOD's February 2020 Agile Software Acquisition Guidebook states that users help to identify and prioritize overall capability needs, and to map out a coherent approach to delivering the major capabilities over time.[63] Figure 5 shows the role of user involvement and feedback throughout the software development process, according to DOD guidance, beginning with contributions to identifying needs.

Figure 5: User Feedback Within DOD's Iterative Agile Software Development Process



Source: GAO analysis of Department of Defense information; GAO (icons). | GAO-26-107861

[62]DCSA, *DCSA Industrial Security DCSA PMO Industrial Security Systems and Services User Agreement* (Mar. 28, 2025). Such a user agreement is required by DOD guidance. *See* DOD Instruction 5000.87, *Operation of the Software Acquisition Pathway* (Oct. 2, 2020).

[63]Office of the Under Secretary of Defense for Acquisition and Sustainment, *Agile Software Acquisition Guidebook: Best Practices & Lessons Learned from the FY18 NDAA Section 873/874 Agile Pilot Program*, version 1.0 (Feb. 27, 2020).The GAO Agile Assessment Guide, which provides leading practices relating to Agile adoption, also states that Agile is reliant on frequent and ongoing collaboration with a wide range of stakeholders, to include the users of a system. Users should be included early and often, and an Agile program should elicit general requirements from users as part of early engagement. See GAO, *Agile Assessment Guide: Best Practices for Adoption and Implementation*, GAO-24-105506 (Washington, D.C.: Nov. 28, 2023 (reissued with revisions Dec 15, 2023)).

However, we found that, although DCSA has begun engaging other DOD components for feedback and testing on the initial NI2 module (capability group 1, discussed above), the agency has not engaged with other users and stakeholders in developing the requirements for all NI2 capability groups.[64] Specifically, we found—and DCSA officials confirmed—that the agency had not collected user input to inform the NI2 Capability Needs Statement, which lays out requirements for the program.

Additionally, in our interviews with selected stakeholders outside of DCSA headquarters, they reported the following:

- **DCSA regional officials**. Participants in the 12 focus groups we conducted in spring 2025 reported that they were either unaware of a replacement for NISS; or that they were aware of a replacement but did not know of any agency efforts to collect input from them for its development.[65]
- **Military department officials**. Officials responsible for overseeing industrial security in three military departments reported a mixed awareness of NI2 development in the last quarter of 2024. To the extent they were aware of NI2, officials expressed a need for more and better engagement from DCSA regarding NI2.[66]
- **Defense industry representatives**. Industry representatives we interviewed reported that industry had not been consulted or engaged on NI2 when we spoke to them in March 2025. These representatives

[64]The first capability group focuses primarily on the initial vetting of company facilities for FOCI risks before they enter the NISP and are subject to NISP compliance activities. According to DCSA officials, where DCSA has solicited feedback from stakeholders and users, the feedback focused on the NI2 module for assessing FOCI risks and was solicited after development work for the system had begun. Initially, DCSA identified users only from its headquarters Office of Entity Vetting, with the first set of users outside of DOD not identified until spring 2025, when DCSA first conducted demonstrations of capability group 1 for stakeholders. DCSA documented some participation by external DOD agencies in a tabletop exercise for NI2 in March 2025 and then appointed in April 2025 the first set of external or non-DCSA user representatives. Some external stakeholders have since participated in test events, starting in July 2025. However, DCSA has currently only collected input for the first capability group's demonstration and testing.

[65]As part of our focus groups with regional officials, we collected preliminary suggestions on desired capabilities and functions within a new system. See appendix IV.

[66]According to Air Force officials, later in January 2026, during DCSA's migration of the NISP Contract Classification System into NI2, Air Force stakeholders reported that there was no DCSA engagement during requirements development, which eliminated Air Force users' ability to provide input, and that limited DCSA communications in advance of system testing prevented their users from dedicating the necessary resources to testing.

knew very little about NI2 development and stated that DCSA had not taken industry requirements into consideration at that time.

DCSA has not continuously engaged with relevant stakeholders—including regional DCSA, military department, and industry officials—throughout the development process for NI2. In particular, DCSA did not engage with these stakeholders in requirements development by ensuring their inclusion in developing the Capability Needs Statement in 2025 and other stages prior to testing. DCSA officials stated that they are aware of the need to engage with relevant stakeholders as part of NI2 development and that they are in the early stages of that engagement for the next two capability groups. For example, agency officials highlighted in January 2026 that they have not started development of the third capability group so have not engaged users on this module. However, DCSA was to have already solicited input from relevant user communities during the development of the Capability Needs Statement for NI2—as outlined in the current user agreement—but the agency did not do this.

Participants in focus groups—reflecting on their previous experience with NISS development—highlighted their concern with the lack of timely input on their system. For example, participants in three focus groups described their experiences with DCSA seeking feedback for the development of NISS before its deployment in 2018. They stated that the agency collected this feedback shortly before the system was rolled out—which they considered too late—resulting in much of their input not being incorporated.

If DCSA does not collect and incorporate end user and stakeholder input when developing its requirements for, and during development of, NI2, it risks developing a replacement system that will continue to have challenges similar to those of NISS. Including such engagement in developing or updating the NI2 Capability Needs Statement would help ensure that the user needs and priorities are captured in requirements.[67] Additionally, early engagement with relevant stakeholders—including regional DCSA, military, and industry officials—would provide DCSA an opportunity to consider needs of end users for the next two capabilities that it may not have previously considered and allow them to play a greater role in identifying and prioritizing desired capabilities and features.

[67]According to DOD Instruction 5000.87, the program sponsor should periodically update a capability needs statement throughout development as required to reflect the current operational needs for the software solution.

Conclusions

Foreign entities attempt to illicitly obtain classified information and technology from U.S. industry thousands of times a year. DCSA has an organizational structure and detailed procedures to protect this information and technology as part of its industrial security mission. While the agency has some efforts to identify, assess, and mitigate risks to this mission, DCSA is still challenged to meet its industrial security requirements. Addressing its mission gaps by providing enhanced analytic tools at the regional level; implementing a risk response plan with specific actions to address the DCSA-identified risk of its limited workforce; assessing one of its core initiatives (NAESOC); and ensuring ongoing, comprehensive user feedback during NI2 development will help DCSA and OUSD(I&S) lay a stronger foundation for its industrial security mission and better protect core national security information and technologies.

Recommendations for Executive Action

We are making the following four recommendations to the Department of Defense:

The Secretary of Defense, through the Under Secretary of Defense for Intelligence and Security, should ensure that the Defense Counterintelligence and Security Agency identifies and develops enhanced analytic tools for field operators to better support their assessments of risk at the regional level. (Recommendation 1)

The Secretary of Defense should ensure that the Under Secretary of Defense for Intelligence and Security implements a risk response plan with specific actions to address the Defense Counterintelligence and Security Agency-identified risk of a limited workforce for industrial security. Such actions could include, as appropriate, changing the periodicity of security reviews to align with DOD's overall risk appetite in the mission area, sharing more industrial security responsibilities with the military departments, or other steps that DOD deems appropriate to address the risks to industrial security. (Recommendation 2)

The Secretary of Defense, through the Under Secretary of Defense for Intelligence and Security, should ensure that the Defense Counterintelligence and Security Agency comprehensively assesses the NAESOC risk response effort, including identifying its resourcing and personnel needs, establishing outcome-oriented performance goals, and evaluating its organizational alignment with other directorates. (Recommendation 3)

The Secretary of Defense, through the Under Secretary of Defense for Intelligence and Security, should ensure that the Defense Counterintelligence and Security Agency continuously engages with relevant stakeholders—including regional DCSA, military department, and industry officials—throughout the development process for NI2, to include requirements development and other stages prior to testing. In doing so, the department should revisit the Capability Needs Statement with relevant stakeholders to validate that it meets their needs, and update it, if necessary. (Recommendation 4)

Agency Comments and Our Evaluation

We provided a draft of this report to DOD. In its comments, reproduced in appendix V, DOD concurred with our four recommendations. As part of the department's response, DOD officials provided substantive details of actions it would take to address the first three recommendations. These actions, if implemented as described, should meet the intent of those recommendations.

DOD concurred with the fourth recommendation, but did not specify how the department will address it. We highlight that early engagement with relevant stakeholders—including regional DCSA, military, and industry officials—would provide DCSA an opportunity to consider the needs of end users for the remaining capabilities that it may not have previously considered and allow them to play a greater role in identifying and prioritizing desired capabilities and features.

We are sending copies of this report to the appropriate congressional committees, the Secretary of Defense, the Director of the Defense Counterintelligence and Security Agency, and other interested parties.

If you or your staff have any questions about this report, please contact me at kirschbaumj@gao.gov. Contact points for our Offices of Congressional Relations and Media Relations may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix VI.

//SIGNED//

Joseph W. Kirschbaum
Director, Defense Capabilities and Management

List of Committees

The Honorable Roger F. Wicker
Chairman
The Honorable Jack Reed
Ranking Member
Committee on Armed Services
United States Senate

The Honorable Mike Rogers
Chairman
The Honorable Adam Smith
Ranking Member
Committee on Armed Services
House of Representatives

Appendix I: Objectives, Scope, and Methodology

This report addresses (1) the funding, personnel, and training the Defense Counterintelligence and Security Agency (DCSA) dedicates to perform its industrial security mission, and the extent to which DCSA (2) has managed risks with the National Industrial Security Program's (NISP) core operational activities, and (3) is addressing challenges with the National Industrial Security System (NISS).

For all three objectives, we reviewed Department of Defense (DOD) issuances, policy, and processes for industrial security. We also interviewed officials from DCSA, military department components, the National Archives and Records Administration, and the NISP Policy Advisory Committee on issues and challenges relating to the NISP.[1] See the end of this appendix for a complete list of organizations interviewed. Further, we collected information for all three objectives from DCSA's regional officials responsible for NISP implementation by hosting a series of focus groups. Specifically, from April to May 2025, we conducted 12 focus groups across DCSA to obtain the perspectives of personnel responsible for overseeing and conducting industrial security-related tasks. We collected information in these groups on agency efforts to manage risk, on the NISS, and on training received.

To ensure we obtained perspectives from personnel in DCSA's four regions, Mid-Atlantic, Eastern, Central, and Western, we conducted the following 12 focus groups by personnel category, as the positions in the categories had differing responsibilities in managing or conducting tasks associated with industrial security: (1) four focus groups of Industrial Security Representatives (ISRs)—one group for each of the four regions, (2) four focus groups of Information Systems Security Professionals (ISSPs) and Counterintelligence Special Agents—one group for each of the four regions, and (3) four focus groups of managers—one group for

[1]Specifically, we discussed industrial security issues with the National Archives and Records Administration's Information Security Oversight Office. While the National Security Council provides overall policy direction for the NISP, the Director of the Information Security Oversight Office is responsible for implementing and monitoring the NISP, in consultation with the National Security Advisor. The Secretary of Defense is the Executive Agent for the NISP, and DCSA carries out most of DOD's NISP implementation activities. Additionally, we interviewed industry representatives from the NISP Policy Advisory Committee, which is composed of 16 members from government and eight members from industry with the Director of the Information Security Oversight Office serving as Chairman. The NISP Policy Advisory Committee advises the Director of the Information Security Oversight Office, as chairman, on all matters concerning the policies of the NISP, including recommended changes to those policies, and serves as a forum to discuss policy issues in dispute. Exec. Order No. 12,829, *National Industrial Security Program,* §§ 102, 103, *as amended*.

each of the four regions, including field office chiefs, ISSP Team Leads, and Counterintelligence Regional Operations Officers and Collection Managers.

To ensure an array of perspectives in each focus group, we hosted six to nine participants in nine groups; two other groups had five participants, and one group had four participants. To identify participants for each group, we obtained personnel data from DCSA that identified all the regions' field operators of different types. Eighty personnel, or 24 percent of their regional workforce, participated in the groups and included managers, ISRs, ISSPs, and Counterintelligence Special Agents. For the four regional ISR focus groups and the four regional ISSP and Counterintelligence Special Agent focus groups, we then randomly selected a mix of 10 personnel who were "more experienced" and "less experienced" based on their number of years at DCSA, using the median years of experience for the operator type in that region. For the four regional management focus groups, we extended invitations to all managers—as the total number of personnel was limited. Additional details on the methodology for each objective are included below.

To describe the amount of funding, the number of personnel, and the training DOD dedicates to its industrial security mission, we analyzed the corresponding data and information received for fiscal years 2021 through 2025 from DCSA. Specifically, DCSA provided annual industrial security funding and expenditure data, and data on the number of industrial security positions filled annually. DCSA also provided information on the type of training it provides internally to ISRs and ISSPs, and externally to other DOD stakeholders and external defense contractors who participate in the NISP.

Additionally, we reviewed DCSA's annual data on the number of security reviews completed. Further, we analyzed data from DCSA's "Bi-weekly Toolkit" pulled in September 2025 to determine the number and type of security violations and open vulnerabilities identified over the prior year, as well as the timeliness in addressing these violations and vulnerabilities. We then described security issues identified from DCSA's security reviews and other related efforts. We assessed the reliability of this data, as well as the expenditure, personnel, and training data above, by interviewing DCSA about the controls they have implemented to ensure accuracy and determined the data were sufficiently reliable for our purposes.

To assess the extent to which DCSA manages risks with the NISP's core operational activities, we first collected documentation on and interviewed DCSA headquarters officials to describe agency efforts to manage risks with its industrial security mission.[2] We organized these existing efforts and activities based on steps in the risk management framework, specifically the identification, assessment and prioritization, and response to risks.[3]

We then coordinated regional focus groups noted previously to collect perspectives on how the NISP is implemented at the operational level. We asked risk-related questions on the identification, assessment, and mitigation of risks, including:

- What are the risks if not all the security reviews can be completed?
- What techniques have you used to evaluate risks or estimate their severity?
- In your experience, what are the primary actions (or efforts) DCSA headquarters has taken to avoid or mitigate risks?

and collected their responses.

We analyzed transcripts of the focus group discussions to identify and compile risk management-related themes. One analyst coded the themes, and another analyst verified that the themes were coded correctly. We reported themes that at least one participant in half or more of the focus groups mentioned, along with comments supporting these themes. (See appendix III for the list of selected themes.) The themes related to the identification of, assessment and prioritization of, and mitigation and response to risks affecting the industrial security mission area. Lastly, we assessed DCSA headquarters and regional officials' efforts in this mission area—from documents collected and testimonial data—against DOD guidance on risk management and internal controls

[2]Examples of documentation we reviewed include DCSA, *National Industrial Security Program: State of the NISP* (January 2024); DCSA, *Industrial Security Mission Guidance* (Sept.18, 2024); and DCSA, *IS Manpower Assessment: Final Report* (June 15, 2023).

[3]DOD Instruction 5010.40, *DOD Enterprise Risk Management and Risk Management and Internal Control Program* (Dec. 11, 2024) provides procedures for implementing an integrated enterprise risk management framework.

to identify any gaps and potential ways to manage risk.[4] These principles include estimating the significance of a risk, taking deliberate steps to mitigate or accept risk, and periodically assessing the effectiveness of risk response actions.

To assess the extent to which the agency is addressing challenges with NISS, we first collected documentation on NISS (the current IT system) and interviewed DCSA headquarters officials to better understand current NISS capabilities and challenges. We additionally interviewed DOD officials from the departments of the Army, Navy, and Air Force, as well as industry representatives from the NISP Policy Advisory Committee, to obtain their experiences with NISS—to include any challenges. In addition to questions about NISS challenges, we interviewed officials about their organization's participation in the development of a NISS replacement. We leveraged the focus groups mentioned earlier to collect information from DCSA field personnel on these same issues, to include gathering information on

- the major benefits and challenges of using NISS;
- their awareness of a replacement system for NISS;
- their participation in—or awareness of—any efforts to solicit input or feedback for the replacement system;
- any key features or functions participants would like to see incorporated into the replacement.

Finally, we interviewed officials responsible for developing the replacement of NISS. We assessed through these interviews and documents whether DCSA has solicited initial feedback on this system and whether they have a mechanism in place to collect ongoing stakeholder feedback against leading practices in Agile software development, as well as requirements from the user agreement.[5]

[4]Specifically, we used DOD Instruction 5010.40, *DOD Enterprise Risk Management and Risk Management and Internal Control Program* (Dec. 11, 2024), specifically paragraph 5.4 on the risk management process, and GAO, *Standards for Internal Control in the Federal Government* (Washington, D.C.: May 2025) on risk assessment principle 7 on the identification, analysis, and response to risks.

[5]Office of the Under Secretary of Defense for Acquisition and Sustainment, *Agile Software Acquisition Guidebook: Best Practices & Lessons Learned from the FY18 NDAA Section 873/874 Agile Pilot Program*, version 1.0 (Feb. 27, 2020) and GAO, *Agile Assessment Guide: Best Practices for Adoption and Implementation*, GAO-24-105506 (Washington, D.C.: Nov. 28, 2023 (reissued with revisions Dec 15, 2023)).

Organizations with Whom GAO Conducted Interviews

In support of our work, we interviewed officials from the Office of the Under Secretary of Defense for Intelligence and Security (OUSD(I&S)), DCSA, the military departments, and the National Archives and Records Administration listed below.

- OUSD(I&S)
  - Office of the Director for Defense Intelligence (Counterintelligence, Law Enforcement, and Security), Director for Information and Acquisition Protection
- DCSA
  - Center for the Development of Security Excellence
  - DCSA Headquarters offices including:
    - Chief Financial Officer
    - Contracting and Procurement Office
    - Industrial Security Directorate
      - Entity Vetting
      - National Access Elsewhere Security Oversight Center
      - NISP Cybersecurity
      - NISP Mission Performance
      - NISP Operations
  - DCSA Field Operations
    - Mid-Atlantic region
    - Eastern region
    - Central region
    - Western region
- U.S. Air Force
  - Secretary of the Air Force
- U.S. Army
  - Army G2, Security Division
- U.S. Navy
  - Office of the Deputy Under Secretary of the Navy for Intelligence and Security

- National Archives and Records Administration
  - Information Security Oversight Office
  - NISP Policy Advisory Committee

We conducted this performance audit from October 2024 to April 2026 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.

Appendix II: Industrial Security Violations and Vulnerabilities

Defense Counterintelligence and Security Agency (DCSA) personnel follow up with and track cleared contractors on their reported security violations and open security vulnerabilities. Security violations can be identified through security reviews or can be reported by DCSA and government security officials or by cleared contractors. In addition, security vulnerabilities are typically identified in a contractor's industrial security program as part of a security review.

Security violations. Most security violations in fiscal year 2025 were reported by contractors. As of September 2025, 576 security violations, or about 70 percent of the 815 security violations that were open sometime during fiscal year 2025, were closed. The average time to investigate and close these security violations from the time they were initially reported was about 67 days. For additional information on the timeliness of addressing security violations closed in fiscal year 2025, see table 7.

Table 7: Number of Days to Close Security Violations as Recorded by DCSA, Year-End Fiscal Year 2025

Days to close	Number of reported violations closed	Percentage of total violations closed
0 to 30	139	24.1%
31 to 60	205	35.6%
61 to 90	101	17.5%
91 to 199	111	19.3%
200 to 299	16	2.8%
300 to 399	2	0.3%
400 to 499	0	0.0%
500 to 999	2	0.3%
1,000+	0	0.0%

Source: GAO analysis of Defense Counterintelligence and Security Agency (DCSA) data. | GAO-26-107861

Notes: Security violations that have not been closed comprised about 30 percent, or 239, of all 815 security violations identified during fiscal year 2025. Security violations that were not closed at the end of fiscal year 2025 had been open for approximately 101 days on average from the time they were initially reported. 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. 32 C.F.R. § 117.3 (2026).

Security vulnerabilities. As of September 2025, DCSA had 1,032 identified vulnerabilities that remained open after the completion of a security review across all active contractor-owned facilities in the National Industrial Security Program. Of those, 310 (30 percent) had been open or unmitigated for less than 30 days after a security review, and 328 (31.8

percent) of the open vulnerabilities had been unmitigated for between 31 and 60 days following the security review. For additional details on the amount of time open vulnerabilities were in an unmitigated status at the end of fiscal year 2025, see table 8.

Table 8: Number of Days Industrial Security Vulnerabilities Remained Open Upon Completion of a Security Review as Recorded by DCSA, Year-End Fiscal Year 2025

Days open	Number of open vulnerabilities	Percentage of total open vulnerabilities
0 to 30	310	30.0%
31 to 60	328	31.8%
61 to 90	169	16.4%
91 to 199	172	16.7%
200 to 299	33	3.2%
300 to 399	11	1.1%
400 to 499	5	0.5%
500 to 999	3	0.3%
1,000+	1	0.1%

Source: GAO analysis of Defense Counterintelligence and Security Agency (DCSA) data. | GAO-26-107861

Notes: DCSA personnel track the number of days cleared contractors take to mitigate open security vulnerabilities related to industrial security, as shown above. Any vulnerability is an identified weakness in a contractor's security program that indicates non-compliance with National Industrial Security Program Operating Manual requirements that could be exploited to gain unauthorized access to classified information or information systems accredited to process classified information. *See* Department of Defense Manual 5220.32, *National Industrial Security Program: Industrial Security Procedures for Government Activities*, vol. 1 (Aug.1, 2018) (incorporating change 2, effective Dec. 10, 2021).

Appendix III: GAO Focus Group Analysis of Risk Management Themes

In table 9, we compile 13 selected risk management-related themes that were mentioned in at least half of the 12 focus groups, along with comments supporting the theme. Seven of the themes were reported by nine or more of the groups. The themes relate to the identification of, assessment and prioritization of, and mitigation and response to risks affecting the industrial security mission area.

Table 9: Selected Themes on Risk Management in the National Industrial Security Program (NISP), as Reported by Focus Groups

Risk management theme ***(Number of focus groups where theme was reported)***	**Example comments**
An increased number of officials could help mitigate risk in the program. Similarly, limited workforce numbers hinder the agency from meeting program requirements. **(12 focus groups reported)**	*"…if we had more ISRs, ISSPs, and Counterintelligence Special Agents, we would be able to go to more facilities every year and that would help reduce the risk…"* *"…the biggest issue to mitigate risk is really we need more people…"* *"…DCSA as a whole just based on personnel in the field… we're probably only accomplishing right around 33% of the overall NISP facilities. And that's strictly to do with just manpower…"* *"…we've been suffering from this manpower shortage…that kind of really stymies us from really being able to be on task with risk…"*
The effectiveness of the NAESOC initiative is limited based on several challenges, including insufficient center staffing, slow responsiveness to contractors, poor security compliance at NAESOC-aligned facilities, and limited risk mitigation. **(12 focus groups reported)**	*"…NAESOC's not properly staffed…they don't have enough people or experience…"* *"…they [NAESOC contractors] complained to us all the time about a lack of response or cookie-cutter responses from the NAESOC folks…"* *"…we're finding every one of them [NAESOC facilities] is a mess…. we're not allowed to send them back to the NAESOC until we clean them up…"* *"…NAESOC…does not assist us with getting at risk, in so much as they do everything remotely…"* *"…I do not feel that it [NAESOC] has been effective at all…think they just moved around a problem instead of fixing the problem…"*
Regional officials generally prefer—if given a binary choice—to add more personnel instead of developing a better IT system to mitigate risk across the industrial security mission. **(11 focus groups reported)**	*"…I'd prefer more people… people definitely would have to come first…"* *"…if you had to choose... I would have to go with people—more people…more people means more reviews…"* *"…I would always choose more ISSPs…more ISSPs because we definitely need the bodies that could go out there and look at the systems and identify risk—more so than a system we need resources…"* *"…the true problem that we have right now is boots on the ground… other than that I'd have to say manpower…you've got to have boots on ground…"*

Risk management theme *(Number of focus groups where theme was reported)*	**Example comments**
Long intervals or delays between security reviews increases risk of program non-compliance and security vulnerabilities. **(10 focus groups reported)**	*"…if we're not able to get out to a company in 3 years, I think we run a higher risk of when we finally do get out there…"* *"…essentially the more time we're away from a cleared defense contractor, the more vulnerabilities there are…"* *"…the longer we go without security reviews there, the longer there is a potential for things that the contractor did wrong, to go unmitigated…"* *"…you generally tend to see that risk and vulnerabilities increase for the longer a period of time that a facility doesn't have a security review…"*
The critical technology list or critical technologies in general is used as a key method to prioritize risk. **(10 focus groups reported)**	*"…we do have a method…based on critical technology…a list based on those facilities that have critical technologies. And so with those facilities, we are required to go out and see them…"* *"…there's a [technology] priority list that comes out…lot of things go into play when we decide what's a priority…what technology are they working on?..."* *"…technology priority list is based off of classified technology priorities…there's critical technologies. There's multiple layers that go into that technology prioritization…"* *"…when prioritizing… another helpful thing is to also understand to the greatest extent possible the critical technologies and infrastructure that are being supported by a contractor…"*
Trend analysis could be enhanced—such as with more automation—or communicated in a more timely manner. **(9 focus groups reported)**	*"…so if there are trends that are available to us, like an increase in security violations…from a push down from headquarters, from the region level [trend analysis] certainly could be better…"* *"…NISS exists…but it's very difficult to pull any kind of trend data out of it…"* *"…I don't have an accounting of that where I'm keeping track of my administrative findings and what the statistics are overall…"* *"…we really need to be able to automate some of this [trend reporting] better…"* *"…our headquarters have done that [trend data collection] on occasion, but nothing consistent where we're doing it regularly…"*
Business plans incorporate several factors—including foreign ownership, control, and influence; facility clearance; time since last assessment; and critical technologies—used to identify and prioritize risk. **(9 focus groups reported)**	*"…what's called a business plan… when we assess risk there, we take input…complexity of facilities that have information systems…foreign partners…"* *"…there's the primary metrics of age risk…or it's a prioritized technology trend…that's created at the beginning of the year through a business plan…"* *"…we go through our business plans and we have a plan in place of how many reviews that need to be conducted that year…So, it's just a lot of [risk] factors…"* *"…the field office chief is on the hook for drafting up a business plan for the field office… supposed to prioritize for the year for our entire field office… whether it's the whatever critical technology…"*

Risk management theme ***(Number of focus groups where theme was reported)***	**Example comments**
Onsite reviews of facilities are critical in identifying areas of non-compliance or deviation from the NISP. **(8 focus groups reported)**	*"…imperative that we have people visit the sites. That is crucial. We find 90% of our deviations [from visits], 90%..."* *"…the lack of being able to physically go out to these sites to conduct on-site validation… some things you just can't verify without going there and seeing in person…"* *"…during the COVID period, we didn't go on site. And when we started going back on site…we were discovering a great amount of items that hadn't been completed—from patching to doing updates…"* *"…if we don't get out there, usually you might see an increase in security violations…"*
The bi-weekly toolkit pulled from NISS data can be used to identify findings and activities, but its analytic capabilities are limited and could be improved. **(7 focus groups reported)**	*"…so it's the NISS Toolkit. It's ran bi-weekly…basically it shows all your actions that you put into NISS. So, I do find it helpful…it could be more helpful…"* *"…the national toolkit drops biweekly. And it is essentially a tracker for all of our oversight activities…it is a logistical tool rather than an analytical product…[biweekly toolkit] doesn't inherently analyze…"* *"…NISS comes up with the [biweekly] toolkit every 2 weeks with about 50 columns of gobbledygook where you might be able to start breaking it down that applies to the entire nation. That's not what I need…"* *"…so, we do have…national toolkit that's produced, but it would be nice if NI2 would just produce that based on fields that we select…"*
The relative quality, expertise, and dedication of the facility's security staff is a key risk factor—with the lack of dedicated, knowledgeable staff increasing risk. **(7 focus groups reported)**	*"…the level of knowledge of the security staff at the company…could have been a really great security program a year ago, just absolutely tanked because of personnel [facility security staff] changes…"* *"…the risk is going to be…also based on what is the past performance of the company…if the people who are at the company that had good past performance are still there…"* *"…the company owner/Facility Security Officer just stood up and said that "I don't have time for this. I'm an engineer"…we'll get to it when we get to it and therefore, of course for those, the risk gets higher…"* *"…you tend to get individuals who are not necessarily have the experience…they may not know the right things to do. They may not do certain things they're supposed to do…that is an additional risk…"*
Insider threat programs are not being implemented effectively in many cases. **(6 focus groups reported)**	*"…with the insider threat program…what I'm seeing now is a lot of programs have documentation, but really no implementation plan. So, there's a shortfall…"* *"…contractors often do not know how to do insider threat programs…"* *"…at a facility the other day and they're like, it's 5 of us. I'm like, "what's your insider threat program?" And they're like, "Well, we look at each other and that's it"…"* *"…they barely have any type of insider threat [program] other than the annual required training and maybe an annual meeting. So, it's just, it's "hit or miss"…"*

Risk management theme *(Number of focus groups where theme was reported)*	**Example comments**
Inadequate or incomplete company self-inspections generally indicate likely security issues or findings. **(6 focus groups reported)**	*"…we typically see if they don't conduct a thorough self-inspection that they're going to have [security] findings based on the things that they didn't cover well…"*
	"…all of us have seen self-inspections that we know have just been "pencil whipped" and there's no way you didn't have any [security] issues given the size and complexity of your facility…"
	"…when people do their self-assessment [facility self-inspection], a lot of times it comes out to be insufficient because they either pencil whip the self-assessment or just have inexperienced people…"
	"…you never know if the self-inspection was actually a thorough self-inspection or if it was one of these where they just kind of "pencil whip" it…if they've done a proper self-inspection, they would have caught it…"
Ongoing communications with facilities outside the required security reviews helps to reduce risk. **(6 focus groups reported)**	*"…keeping good communication with the facility outside of an inspection [security review], I think that helps lower the risk…"*
	"…the vast majority of the visits I do to industry are not security reviews… engagements like the "advise and assist," the on-site validations, those are where we are truly managing risk…"
	"…the more time that we're away from communications with them [facilities], actually communicating threats to them, the more chance we have for vulnerabilities…"
	"…my larger complex companies, I work very closely with them, and we have a plan in place where I meet with them monthly, at least a phone call…because we know risks might come in…"

Legend:

DCSA: Defense Counterintelligence and Security Agency

ISR: Industrial Security Representative

ISSP: Information Systems Security Professional

NAESOC: National Access Elsewhere Security Oversight Center

NI2: National Industrial Security System, Increment 2

NISS: National Industrial Security System

Source: GAO analysis of DOD focus groups. | GAO-26-107861

Note: Comments included in the right column from focus group participants support the theme in the left column, and the comments were selected to generally represent the theme across focus group participants reporting similar comments. For conciseness, not all comments are included for each selected theme. The number of focus groups with participants reporting each theme reflects the minimum number—i.e., at least x focus groups—of groups that may have agreed with a theme, because the specific theme may not have been discussed during all groups.

Appendix IV: National Industrial Security System Challenges and Additional Functionality Requested

DOD and defense industry officials who use the National Industrial Security System (NISS)—the industrial security system of record—during their normal operations cited numerous challenges in using the system. We conducted focus groups with DCSA officials across the agency's four regions—Mid-Atlantic, Eastern, Central, and Western—for a total of 12 separate groups. The table below includes a summary of challenges cited by these groups, as well as challenges cited in interviews with DCSA headquarters officials and external stakeholder groups (e.g., military departments, industry).

Table 10: Challenges with the National Industrial Security System (NISS) Reported by Defense Counterintelligence and Security Agency (DCSA), Military Department, and Selected Industry Officials

NISS challenge	Examples of NISS challenges
Slow system performance	NISS is slow, sometimes spinning and failing when attempting to save.
Frequent system downtime	NISS has significant periods of unavailability.
Poor data quality, accuracy, or availability	NISS data is often inaccurate or unavailable to support the work of industrial security representatives, in part because industry is not required to input or update all the data.
Limited ability to query NISS data	Some searches in NISS can require labor-intensive searching through multiple records.
Limited interoperability with other necessary systems	NISS cannot automatically update from other related systems, such as the Defense Information System for Security or the Enterprise Mission Assurance Support Service. This limited interoperability significantly increases—doubles or triples—the work of Information Systems Security Professionals because of the lack of a connection between the systems.
Lack of trend reporting capabilities	NISS lacks the ability to identify trends over time. Officials can only generate trend reports and other analytic products from NISS by exporting the data and using workarounds.
Lack of automated (or bulk) data entry	Companies must manually enter data in the system rather than importing the data through a single file, such as a spreadsheet.
Poor workflow management	NISS does not track workflow very well, requiring significant duplication of effort.
Limited visibility by military departments into facility compliance	Military department access to NISS data—on companies for which their department holds classified contracts—is limited except through workarounds. For example, department officials experience challenges in viewing which contractor facilities at their installations have been cleared for storage of classified information.
Missing system notifications	NISS often fails to notify officials when they have messages in the system.
Lack of capability to transfer data to classified systems	Counterintelligence officials are unable to move NISS data to classified systems, limiting the utility of that data.
System unsuitability for industry	Industry is challenged to process change condition packages through NISS as the system only allows the submission of one change condition at a time, which can take a long time to approve. However, companies often experience multiple changes a year.

NISS challenge	Examples of NISS challenges
Lack of user-friendliness	NISS reduces effectiveness by being overly time-consuming. Documenting activities in NISS can take longer than the task being documented. System navigation is also difficult (e.g., lack of a back button).
Limited visibility into classified shipments	Permissions in NISS do not enable agency officials to view the shipment of classified hardware from one facility to another (e.g., visibility to monitor whether the receiving facility has permission to accept the classified shipment).

Source: GAO analysis of industrial security interviews and focus groups. | GAO-26-107861

Note: NISS is the industrial security system of record. We conducted 12 focus groups with DCSA officials across the agency's four regions—Mid-Atlantic, Eastern, Central, and Western. The table includes selected challenges cited by these groups, as well as NISS challenges cited in interviews with DCSA headquarters officials and in agency documents. Given the large number of NISS challenges cited across different reporting groups, we did not quantify the number of groups reporting any given challenge.

Additionally, we asked the 12 focus groups specifically about the functions or capabilities they wanted in the system, NI2, that is to replace NISS. We have compiled their responses below.

1. **Data sharing and interoperability with other systems**. Participants from seven focus groups reported that they want NISS Increment 2 (NI2) to be able to communicate with, access, and process data from other key systems (e.g., through Application Programming Interfaces) that field staff use to oversee industrial security.[1] Systems specifically mentioned in the focus groups include:
    a. Enterprise Mission Assurance Support Service
    b. National Industrial Security Program Contract Classification System
    c. Defense Information System for Security
    d. USAspending.gov
    e. System for Award Management (SAM.gov)
2. **Greater automation**. Participants from seven focus groups reported that they want NI2 to automate more of their work, to include generating documents, managing tasks and workflow, and distributing automated messages.

[1]An Application Programming Interface sets up machine-to-machine communication, which can allow users to obtain real-time data updates.

3. **Improved user friendliness**. Participants from six focus groups reported that they want NI2 to have a better interface; better system reliability and responsiveness; improvements in navigation (e.g., a "back button"); better notifications; and improvements that reduce redundant data entry (i.e., reduce the need to enter the same data in more than one location in the system).
4. **Customized reporting features**. Participants from six focus groups reported that they want NI2 to generate customized reports and metrics that they could run for their own work.
5. **Additional tools for analysis**. Participants from six focus groups reported that they want NI2 to provide additional tools and capabilities to support their analytic work, including improvements in search capability, the addition of artificial intelligence, and the linkage of data associated with a cleared facility (e.g., contracts and work on certain technologies).
6. **Improved capability to perform database functions**. Participants from three focus groups reported that they want NI2 to provide improvements to database functions, such as better import, export, organization, and filtering of data.
7. **Compatibility/interoperability with existing work equipment**. Participants from three focus groups reported that they want NI2 to interoperate with current field office capabilities, such as being available when working at a facility they are reviewing.
8. **Improved data quality, controls, and validation**. Participants from two focus groups reported that they want NI2 to provide improved validation of data in the system (e.g., verifying corporate ownership and government contracts).
9. **Inclusion of past corporate history**. Participants from two focus groups reported that they want NI2 to provide the history of a facility, such as previous facility clearances or past vulnerabilities.
10. **Additional opportunities to capture work done at/for a facility**. Participants from one focus group reported that they want NI2 to provide DCSA field personnel with more opportunities to detail the actions they take at a facility.

Appendix V: Comments from the Department of Defense

OFICE OF THE UNDER SECRETARY OF WAR
5000 DEFENSE PENTAGON
WASHINGTON, DC 20301-5000

INTELLIGENCE
AND SECURITY

APR 0 1 2026

Mr. Joseph Kirschbaum
Director, Defense Capabilities and Management
U.S. Government Accountability Office
441 G Street, NW
Washington DC 20548

Dear Mr. Kirschbaum:

This letter serves as the Department of War (DoW) response to the Government Accountability Office (GAO) Draft Report GAO-26-107861SU, titled "Industrial Security: Improved Risk Management and Stakeholder Engagement Needed to Help DOD Address Mission Gaps," dated March 3, 2026, GAO Code 107861.

Substantive responses to the recommendations are enclosed. For further information, please contact Jamie E. Long, who may be reached at jamie.e.long2.civ@mail.mil or (703) 697-4693.

Tara L. Jones
Acting Director for Defense Intelligence
Counterintelligence, Law Enforcement,
& Security

Enclosure:
As stated

GAO DRAFT REPORT DATED MARCH 3, 2026
GAO-26-107861SU (GAO CODE 107861)

"INDUSTRIAL SECURITY: Improved Risk Management and Stakeholder Engagement Needed To Help DoD Address Mission Gaps"

DEPARTMENT OF WAR COMMENTS
TO THE GAO RECOMMENDATIONS

RECOMMENDATION 1: The Secretary of Defense, through the Under Secretary of Defense for Intelligence and Security, should ensure that the Defense Counterintelligence and Security Agency identifies and develops enhanced analytic tools for field operators to better support their assessments of risk at the regional level.

DoW RESPONSE: Concur, with comments. DCSA Portfolio Acquisition Executive (PAE) and Industrial Security team within DCSA, will immediately initiate a formal requirements elicitation process across all regional offices to define functional capabilities for localized risk assessment. This initiative will standardize the definition of "analytic tools" and identify any capability gaps not addressed by the Capability Needs Statement (CNS), ensuring that front-line operational needs are translated directly into technical requirements. DCSA will take the following steps: 1) Internal alignment and scoping to align internal stakeholders on the project's objectives and standardize the definition of "analytic tools." 2) Discovery and initial engagement with all regional offices to gather information on operational needs and existing capability gaps. 3) Requirements validation and deep dive for a detailed analysis to validate the initial findings and translate the operational needs into specific technical requirements. 4) Synthesis and roadmap for validated requirements to guide the acquisition and development strategy.

Upon the scheduled completion of this documentation by September 26, 2026, DCSA's, PAE will execute a comparative analysis and market research to determine the optimal acquisition strategy, whether through internal development or external procurement. The end state of this integrated effort is to equip all stakeholders and field operators with the advanced technical infrastructure necessary to optimize mission-critical support.

RECOMMENDATION 2: The Secretary of Defense should ensure that the Under Secretary of Defense for Intelligence and Security implements a risk response plan with specific actions to address the Defense Counterintelligence and Security Agency-identified risk of a limited workforce for industrial security. Such actions could include, as appropriate, changing the periodicity of security reviews to align with DOD's overall risk appetite in the mission area, sharing more industrial security responsibilities with other military agencies, or other steps that DOD deems appropriate to address the risks to industrial security.

DoW RESPONSE: Concur, with comments. The Office of the Under Secretary of War for Intelligence and Security will direct and oversee a comprehensive mission analysis by the DCSA to address risks associated with its industrial security mission, with a defined timeline. This analysis will address risks associated with its industrial security mission by evaluating and modeling various risk-mitigation strategies. Informed by the Fast-tracking Acquisition Security

1

Transformation (FAST) Study conducted by MITRE, these strategies will include, but are not limited to: 1) Adjusting the periodicity of security reviews based on threat-based and risk-based principles; 2) Increasing capabilities for cleared industry to perform on classified contracts by establishing Classified Infrastructure as a Service (CIaaS) a service; 3) Implementing technological efficiencies to automate and reduce administrative tasks, thereby optimizing availability of personnel to focus on identified risks; 4) Modernizing the National Industrial Security Program: Industrial Security Procedures for Government Activities (DoWM 5220.32, Vol. 1) to align with a risk-based security posture and reduce administrative burdens that strain the current mission; 5) Evaluating the outcomes of the ongoing OUSW(I&S) chartered congressionally mandated RAND study on managing foreign investment disclosures and impact on FOCI framework. This evaluation will inform the establishment of a consistent system for managing foreign investment risk while reducing duplicative efforts and allocating resources more effectively.

The initial findings and a proposed implementation roadmap for this multi-phased plan are scheduled to be presented to the Office of the Secretary of War by December 31, 2026. This initiative is designed to ensure DCSA can dynamically allocate its resources to counter the most significant threats to the industrial base while maintaining its commitment to all mission partners.

RECOMMENDATION 3: The Secretary of Defense, through the Under Secretary of Defense for Intelligence and Security, should ensure that the Defense Counterintelligence and Security Agency comprehensively assess the NAESOC risk response effort, including identifying its resourcing and personnel needs, establishing outcome-oriented performance goals, and evaluating its organizational alignment with other directorates.

DoW RESPONSE: Concur, with comments. DCSA, in coordination with OUSW(I&S), will take action to ensure the NAESOC risk response effort is comprehensively assessed. This will be accomplished through two distinct but complementary lines of effort:

1) Integrated Organizational Assessment and Realignment. OUSW(I&S) will provide oversight for a comprehensive assessment of NAESOC, executed by the DCSA. This assessment will be conducted as an integral part of DCSA's ongoing initiative to enhance mission effectiveness and synergy. This integrated approach will determine NAESOC's optimal organizational alignment and establish clear, outcome-oriented performance goals. Crucially, these goals will be directly tied to Industrial Security's core mission of providing effective oversight of the National Industrial Security Program (NISP). DCSA will initiate this review before the end of the fiscal year and report its findings and implementation plan within six months.

2) Enhancement of the Continuous Monitoring Program. In parallel, and in direct support of the National Defense Strategy, OUSW(I&S) will oversee DCSA's efforts to further advance the capabilities of the Continuous Monitoring Program (CMP). This separate line of effort is focused on improving the tools, analytics, and processes used to vet and continuously monitor covered entities and cleared entities in the NISP. By strengthening the CMP, the Department will enhance its ability to proactively identify and mitigate FOCI risk and other threats, ensuring the integrity of our trusted industry partners and the protection of national security information.

This dual approach ensures the Department is not only optimizing its organizational structures but also advancing the critical programmatic capabilities required to meet current and future threats.

RECOMMENDATION 4: The Secretary of Defense, through the Under Secretary of Defense for Intelligence and Security, should ensure that the Defense Counterintelligence and Security Agency continuously engage with relevant stakeholders – including regional DCSA, military department, and industry officials – throughout the development process for NI2, to include requirements development and other stages prior to testing. In doing so, the Department should revisit the Capability Needs Statement with relevant stakeholders to validate that it meets their needs, and update it, if necessary.

DoW RESPONSE: Concur.

Appendix VI: GAO Contact and Staff Acknowledgments

GAO Contact

Joseph W. Kirschbaum, kirschbaumj@gao.gov

Staff Acknowledgments

In addition to the contact named above, Jennifer Andreone (Assistant Director), Robert Breitbeil (Analyst-in-Charge), Caroline Christopher, Michele Fejfar, Christopher Gezon, Kaelin Kuhn, Richard Powelson, Carter Stevens, Richard Winsor, Lillian Moyano Yob, and Ed Yuen made key contributions to this report.

Related GAO Products

Personnel Vetting: Sustained Leadership Is Critical to DOD's New Approach to Its Background Investigation System. GAO-25-108721. Washington, D.C.: September 16, 2025.

Federal Contracting: Timely Actions Needed to Address Risks Posed by Consultants Working for China. GAO-24-106932. Washington, D.C.: September 19, 2024.

Personnel Vetting: DOD Needs to Improve Management of the National Background Investigation Services Program. GAO-24-107616. Washington, D.C.: June 26, 2024.

Government Reorganization: Key Questions to Assess Agency Reform Efforts. GAO-18-427. Washington, D.C.: June 13, 2018.

Protecting Classified Information: Defense Security Service Should Address Challenges as New Approach Is Piloted. GAO-18-407. Washington, D.C.: May 14, 2018.

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 X, LinkedIn, Instagram, and YouTube.
Subscribe to our 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

Media Relations

Sarah Kaczmarek, Managing Director, Media@gao.gov

Congressional Relations

David A. Powner, Acting Managing Director, CongRel@gao.gov

General Inquiries

https://www.gao.gov/about/contact-us