



Report to the Subcommittee on
Emerging Threats and Capabilities,
Committee on Armed Services,
House of Representatives

May 2018

PROTECTING CLASSIFIED INFORMATION

Defense Security
Service Should
Address Challenges
as New Approach Is
Piloted

GAO Highlights

Highlights of [GAO-18-407](#), a report to the Subcommittee on Emerging Threats and Capabilities, Committee on Armed Services, House of Representatives

Why GAO Did This Study

Industrial security addresses the information systems, personnel, and physical security of facilities and their cleared employees who have access to or handle classified information. The National Industrial Security Program was established in 1993 to safeguard federal government classified information that may be or has been released to contractors, among others. GAO last reported on this program in 2005 and the Department of Defense has since implemented 13 of the 16 related recommendations.

GAO was asked to examine how DSS administers the program. This report assesses to what extent DSS: 1) changed how it administers the program since GAO's last report; and 2) addressed challenges as it pilots a new approach to monitoring contractors with access to classified information.

GAO reviewed guidance and regulations since 2005, including the program's operating manual. GAO analyzed data from DSS's electronic databases and also selected a non-generalizable sample of contractor facilities based on clearance level, geographic location, and type of agreement to address foreign influence. We also reviewed documents and interviewed relevant government and contractor officials.

What GAO Recommends

GAO recommends DSS determine how it will collaborate with stakeholders, including identifying roles and responsibilities and related resources, as it pilots a new approach. DSS concurred with the recommendation.

View [GAO-18-407](#). For more information, contact Marie A. Mak at (202) 512-4841 or MakM@gao.gov.

May 2018

PROTECTING CLASSIFIED INFORMATION

Defense Security Service Should Address Challenges as New Approach Is Piloted

What GAO Found

The Defense Security Service (DSS) has upgraded its capabilities but also faces challenges in administering the National Industrial Security Program, which applies to all executive branch departments and agencies, and was established to safeguard federal government classified information that current or prospective contractors may access. Since we last reported on this program in 2005, DSS has:

- streamlined facility clearance and monitoring processes, and
- strengthened the process for identifying contractors with potential foreign influence.

However, under its current approach, DSS officials indicated that they face resource constraints, such as an inability to manage workloads and complete training necessary to stay informed on current threats and technologies. In its most recent report to Congress, DSS stated that it was unable to conduct security reviews at about 60 percent of cleared facilities in fiscal year 2016. Further, DSS recently declared that the United States is facing the most significant foreign intelligence threat it has ever encountered. As a result, in 2017, DSS announced plans to transition to a new monitoring approach to address emerging threats at facilities in the program. For a comparison of the current and new approaches, see below.

Comparison of the Defense Security Service's (DSS) Current and New Approaches for Monitoring Cleared Facilities

| Current Monitoring Approach | New Approach – DSS in Transition |
|---|---|
| Schedules security reviews on a 90-day work plan starting with specific facilities, such as those with mitigation agreements for foreign influence or classified information systems. | Will use national intelligence and Department of Defense's list of critical technologies and programs to prioritize security reviews at facilities based on their assets and the threats to those assets. |
| Conducts security reviews that focus on a contractor's adherence with National Industrial Security Program Operating Manual requirements. | Will conduct security reviews to develop customized security plans and assess implementation of such plans to ensure contractors protect assets. |

Source: GAO analysis of DSS documentation and interviews with DSS officials. | [GAO-18-407](#)

DSS has not addressed immediate challenges that are critical to piloting this new approach. For example, GAO found it is unclear how DSS will determine what resources it needs as it has not identified roles and responsibilities. Moreover, DSS has not established how it will collaborate with stakeholders—government contracting activities, the government intelligence community, other government agencies, and contractors—under the new approach. Federal Internal Control Standards establish the importance of coordinating with stakeholders, including clearly defining roles and responsibilities. In addition, GAO's leading practices for interagency collaboration state that it is important for organizations to identify the resources necessary to accomplish objectives. Until DSS identifies roles and responsibilities and determines how it will collaborate with stakeholders for the piloting effort, it will be difficult to assess whether the new approach is effective in protecting classified information.

Contents

| | | |
|--------------|---|----|
| Letter | | 1 |
| | Background | 4 |
| | DSS Upgraded Capabilities for the National Industrial Security Program but Faces Challenges Monitoring Contractors | 13 |
| | DSS Has Not Determined How It Will Collaborate with Stakeholders As It Pilots a New Approach | 20 |
| | Conclusions | 26 |
| | Recommendation for Executive Action | 27 |
| | Agency Comments and Our Evaluation | 27 |
| Appendix I | Methods for Mitigating Foreign Influence | 28 |
| Appendix II | Status of Prior GAO Recommendations Related to the National Industrial Security Program | 30 |
| Appendix III | Comments from the Department of Defense | 33 |
| Appendix IV | GAO Contact and Staff Acknowledgments | 35 |
| Tables | | |
| | Table 1: Comparison of the Defense Security Service's (DSS) Current and New Approaches for Monitoring Cleared Facilities | 21 |
| | Table 2: Types of Plans to Mitigate Foreign Influence | 29 |
| | Table 3: Summary of Prior GAO Recommendations Related to the National Industrial Security Program and Actions to Address Them | 31 |
| Figures | | |
| | Figure 1: Overview of Defense Security Service's (DSS) Facility Clearance Process in the National Industrial Security Program | 8 |

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

11

Abbreviations

DSS Defense Security Service

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



May 14, 2018

The Honorable Elise Stefanik
Chairwoman
The Honorable Jim Langevin
Ranking Member
The Honorable Joe Wilson
Member
Subcommittee on Emerging Threats and Capabilities
Committee on Armed Services
House of Representatives

Protecting classified information from compromise and exploitation is essential for the U.S. government to maintain its technological advantage over potential adversaries. In recent years, there have been high profile leaks of classified information by contractors, and there are heightened concerns about foreign adversaries' ability to access classified information and evade detection. Industrial security addresses the information systems, personnel, and physical security of facilities and their cleared employees who have access to or handle classified information. In 1993, the National Industrial Security Program, which applies to all executive branch departments and agencies, was established to safeguard federal government classified information that may be or has been released to current, prospective, or former contractors, among others, and is administered by the Defense Security Service (DSS) within the Department of Defense.¹ DSS determines the eligibility of contractors to access classified information, known as the facility security clearance process, and contractors may have one or multiple facilities that participate in the program.² Once a contractor is cleared and enters the program, DSS is responsible for ensuring that

¹Executive Order No. 12829, 58 Fed. Reg. 3479 (Jan. 6, 1993), as amended by Executive Order No. 12885, 58 Fed. Reg. 65863 (Dec. 14, 1993).

²In January 2017, the Information Security Oversight Office within the National Archives and Records Administration proposed to replace "facility security clearance" with "entity eligibility determination." The rule proposed to define "entity eligibility determination" as, "an assessment by the cognizant security agency as to whether an entity is eligible for access to classified information of a certain level (and all lower levels)." Eligibility determinations may be broad or limited to specific contracts, sponsoring agencies, or circumstances. A favorable determination results in eligibility to access classified information under the cognizance of the responsible cognizant security agency to the level approved." 82 Fed. Reg. 3219, 3221, 3223 (Jan. 11, 2017).

cleared contractors meet the requirements to safeguard classified information through periodic security reviews.

You requested that we examine how the Department of Defense, through DSS, administers the National Industrial Security Program to protect classified information. This report assesses to what extent DSS: 1) changed how it administers the program since our last report in 2005; and 2) addressed challenges as it pilots a new approach to monitoring contractors with access to classified information.

To determine the extent to which DSS changed how it administers the National Industrial Security Program, we reviewed relevant guidance and regulations including changes made since we last reported in 2005, such as DSS's Industrial Security Operating Manual. We also reviewed the National Industrial Security Program Operating Manual (operating manual), which describes the requirements for contractors to safeguard classified information under the program.³ We also viewed demonstrations of DSS's various electronic systems, including the Industrial Security Facilities Database. To learn about changes to how DSS processes facility security clearances, we selected a non-generalizable sample of 13 contractor facilities based on 3 criteria: security clearance level, geographic location, and type of mitigation agreements. Mitigation agreements that address foreign ownership, control, or influence are intended to prevent situations in which a foreign interest has the power to decide matters affecting a contractor's operations and that could result in unauthorized access to U.S. classified information or adversely affect the performance of classified contracts.⁴ For the purposes of this report, we will use "foreign influence" when

³Department of Defense, "DOD 5220.22-M National Industrial Security Program Operating Manual (incorporating Change 2, May 18, 2016)" (Washington, D.C.: Feb. 2006).

⁴The National Industrial Security Program Operating Manual prescribes the requirements, restrictions, and safeguards that contractors are to follow to prevent the unauthorized disclosure of classified information. Several factors relating to the company, the foreign interest, and the government of the foreign interest must be considered to determine whether a company is under foreign ownership, control, or influence, including whether the foreign interests are substantial (i.e. a minority position is deemed substantial if it consists of greater than 5 percent of the ownership interests or greater than 10 percent of the voting interest.) A U.S. company determined to be under foreign ownership, control, or influence is ineligible for a facility clearance unless and until security measures have been put in place to negate or mitigate foreign ownership, control, or influence. For more information about different types of mitigation agreements, see appendix I.

referring to contractors with foreign ownership, control, or influence.⁵ Our sample included at least two contractor facilities from each of DSS's four regions (Capital, North, South, and West) with active secret or top secret clearances (as of June 29, 2017) that were operating with mitigation agreements to address foreign influence.

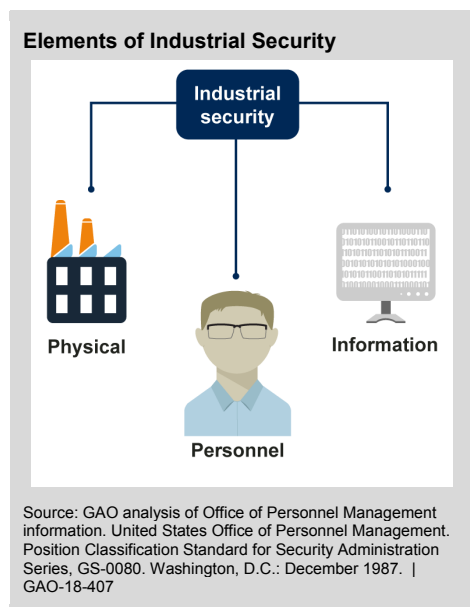
We reviewed documents from DSS's facility clearance process, including the agency's analysis of potential foreign influence along with mitigation agreements and supplemental plans. We conducted site visits at all four regional offices and met with industrial security representatives, regional leadership staff, counterintelligence special agents, and information system security professionals who worked with these facilities. We also analyzed data from DSS's Industrial Security Facilities Database, including the number of clearances granted to facilities with contractor mitigation agreements from fiscal year 2007 through 2016. We took steps to assess the reliability of the data, including comparing selected data fields against DSS documentation and conducting interviews with DSS officials. We determined that the data were sufficiently reliable to understand how many facility clearances DSS processed for facilities with and without contractor mitigation agreements during this period.

To assess the extent to which DSS has addressed challenges as it pilots a new approach to monitoring contractors with access to classified information, we reviewed documents, analyzed DSS data, and conducted interviews with officials involved in DSS's monitoring process. We reviewed documents related to DSS's current process, such as security reviews, and DSS's new approach (*DSS in Transition*), including documents distributed to cleared contractors. We also conducted interviews with officials from DSS headquarters, including those involved with *DSS in Transition*, DSS field offices, government contracting activities, cleared contractor facilities, and defense industrial trade associations.

⁵A U.S. company is considered under foreign ownership, control, or influence whenever a foreign interest has the power, direct or indirect, whether or not exercised, and whether or not exercisable through the ownership of the U.S. company's securities, by contractual arrangements or other means, to direct or decide matters affecting the management or operations of that company in a manner which may result in unauthorized access to classified information or may adversely affect the performance of classified contracts. National Industrial Security Program Operating Manual, 2006, Department of Defense 5220.22-M, incorporating Change 2, May 18, 2016, 2-300(a).

We conducted this performance audit from February 2017 to May 2018 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



The goal of federal government industrial security is to ensure that contractors' security programs detect, deter, and counter the threat posed by adversaries seeking classified information. The National Industrial Security Program was established by executive order in 1993 to replace industrial security programs operated separately by various federal agencies and ensure that contractors, among others, were adequately protecting classified information.⁶ For the purposes of this report, we will use "contractor" to refer to any party that the program applies to, including contractors, grantees, licensees, certificate holders, and their respective employees.⁷

⁶Executive Order No. 12829, 58 Fed. Reg. 3479 (Jan. 6, 1993), as amended by Executive Order No. 12885, 58 Fed. Reg. 65863 (Dec. 14, 1993).

⁷In its January 2017 proposed rule, the Information Security Oversight Office within the National Archives and Records Administration proposed to add a definition for "entity." The proposed rule defined "entity," in part as, "a generic and comprehensive term which may include sole proprietorships, partnerships, corporations, limited liability companies, societies, associations, institutions, contractors, licensees, grantees, certificate holders, and other organizations usually established and operating to carry out a commercial, industrial, educational, or other legitimate business, enterprise, or undertaking, or parts of these organizations." 82 Fed. Reg. 3219, 3223 (Jan. 11, 2017). Currently, DSS tracks facilities by their Commercial and Government Entity code, also commonly referred as CAGE code.

DSS Responsibilities

DSS is responsible for administering the National Industrial Security Program on behalf of the Department of Defense and, by mutual agreement, 32 other federal departments and agencies.⁸ Headquartered in Quantico, Virginia, and with staff in 26 field offices across four regions, DSS provides oversight, advice, and assistance to more than 12,000 U.S. facilities that are cleared for access to classified information under the program.⁹ Facilities can range in size and be located anywhere in the United States, and include manufacturing plants, laboratories, and universities. In addition, they can also include contractor personnel who travel to U.S. government sites to access classified information but do not store any classified information at their facility. There are multiple reasons why a contractor may need access to classified government information. For example, a factory may produce parts for a major weapons system using a production process that is classified, or a contractor may have employees who deliver their technical expertise in a classified environment at a military installation.

⁸Department of Defense Instruction 5220.22, "National Industrial Security Program (NISP)." The Department of Defense has entered into agreements with the following 32 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, and the Treasury; 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 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; and U.S. Trade Representative.

⁹Under Executive Order No. 12829, as amended, the Director of National Intelligence, the Secretary of Energy, and the Nuclear Regulatory Commission retain authority over access to information under their respective programs. As such, they may monitor contractor facilities with access to such information or assign some of that responsibility to the Department of Defense. The Department of Defense, through DSS, serves as the cognizant security office for the Department of Homeland Security based on an agreement between the two agencies for the National Industrial Security Program. The agreement does not include the Classified Critical Infrastructure Protection Program at the Department of Homeland Security.

National Industrial Security Program Operating Manual

As part of the facility clearance process, DSS is responsible for ensuring that cleared contractors safeguard classified information under the program by meeting requirements, which are outlined in the National Industrial Security Program Operating Manual.¹⁰ The Secretary of Defense, 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, issues and maintains the operating manual. The operating manual addresses the contractors' key responsibilities such as reporting incidents of suspected loss of classified information.¹¹ The Information Security Oversight Office of the National Archives and Records Administration, an agency separate from the Department of Defense, monitors the National Industrial Security Program and issues implementing directives for agencies. The Information Security Oversight Office also chairs the program's policy advisory council, which is comprised of government and industry representatives who recommend changes to industrial security policy. The Department of Defense, including DSS, has periodically issued information for contractors in the program, such as industrial security letters, to clarify the operating manual.

The operating manual states that a contractor or prospective contractor is eligible for a facility clearance if it has a need for access to classified information in connection with a legitimate U.S. government contracting requirement. A facility clearance is an administrative determination that, from a national security standpoint, a contractor or prospective contractor is eligible to access classified information at a specified level. A contractor's employees cannot begin accessing classified information until the facility clearance has been granted, even if that results in delayed performance of a contract.

¹⁰The National Industrial Security Program Operating Manual was updated in May 2016 to establish and maintain an insider threat program to detect, deter, and mitigate insider threats.

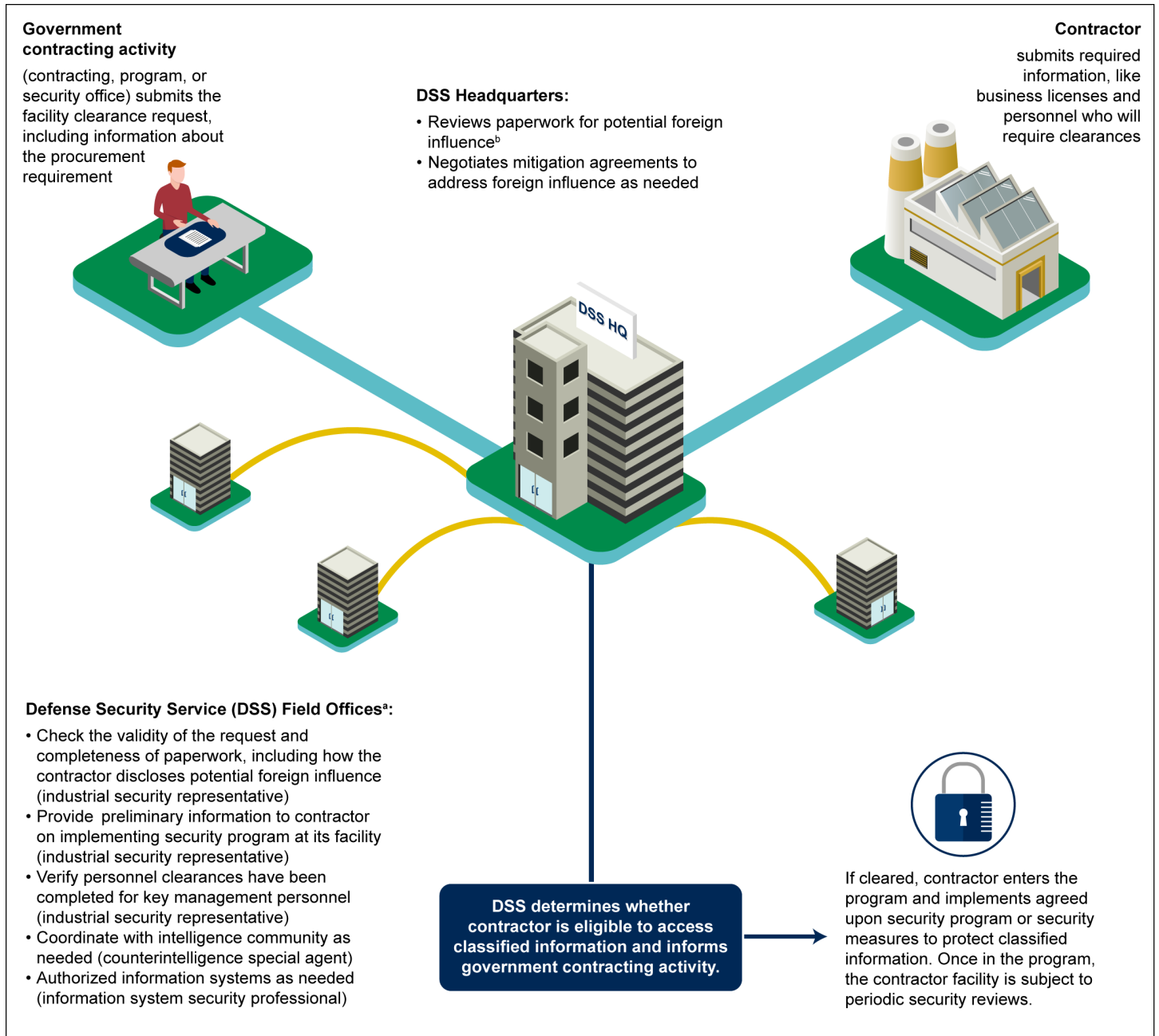
¹¹The responsibilities of agencies participating in the National Industrial Security Program are listed in 32 C.F.R. § 2004.

Facility Clearance Process

According to the operating manual, in order for a contractor or prospective contractor to enter the program, it may be sponsored by an already cleared contractor or the government contracting activity. DSS requires information about the contract, subcontract, or solicitation that necessitates a clearance, such as level of safeguarding required and a brief description of the procurement.¹² Within the government contracting activity, the information may be provided by the contracting office, program office, or security office. DSS begins its facility clearance process once it receives the information and assigns the case to an industrial security representative at a local DSS field office. The industrial security representative serves as the primary point of contact for the sponsored facility during the clearance process and once the contractor is eligible to access classified information. Across DSS field offices and headquarters, multiple people are involved in the facility clearance process, including those who specialize in information systems or others who have experience with analyzing contractors for indicators of foreign influence. See figure 1 for more details about how DSS processes a facility clearance.

¹²The information is submitted via the Department of Defense Contract Security Classification Specification Form (DD-254).

Figure 1: Overview of Defense Security Service's (DSS) Facility Clearance Process in the National Industrial Security Program



Source: GAO analysis of Defense Security Service facility clearance processes and interviews with DSS officials. | GAO-18-407

^aDSS is headquartered in Quantico, VA, with 26 field offices across four regions.

^bMitigation agreements that address foreign ownership, control, or influence (“foreign influence”) are intended to prevent situations in which a foreign interest has the power to decide matters affecting a

contractor's operations and that could result in unauthorized access to U.S. classified information or adversely affect the performance of classified contracts. For the purposes of our report, a contractor under "foreign influence" means it is under foreign ownership, control, or influence, as described in section 2-300(a) of the National Industrial Security Program Operating Manual.

As shown in the figure above, DSS also reviews the contractor's ownership and business structure to assess whether foreign interests indicate a contractor is under foreign influence, which could lead to disclosure of classified information to foreign nationals. Contractors are required to answer questions about whether there is foreign involvement in their ownership, board composition, debt, source of revenues, and any other situations where foreign nationals might be in a position to influence their operations.¹³ If DSS determines that there is a risk for foreign influence, the contractor is ineligible for a facility clearance unless, and until, security measures are put in place, such as negotiating a mitigation agreement with DSS. As of June 2017, approximately 630 of the over 12,000 cleared facilities in the program have mitigation agreements in place to address foreign influence.

As part of the facility clearance process, certain personnel, such as the facility security officer, must receive personnel clearances to the level of the facility clearance. In the personnel clearance process, specialists at DSS headquarters grant interim clearances to U.S. citizens based on national security standards and information from background investigations conducted by the Office of Personnel Management, if there is no adverse information of material significance.¹⁴ Before the facility clearance can be granted, a DSS industrial security representative verifies that the key management personnel have received their permanent clearance.

¹³This information is submitted in the Certificate Pertaining to Foreign Interests (Standard Form 328).

¹⁴Clearances may be at the Top Secret, Secret, or Confidential level. Upon the completion of the background investigation, Department of Defense Consolidated Adjudications Facility, separate from DSS, adjudicates the case and determines whether to grant the final clearance. Individuals cannot apply for a personnel security clearance on their own. Rather, the contractor determines whether an employee will require access to classified information in performance of tasks or services related to the fulfillment of a classified contract. Once the contractor makes this determination, the individual may be processed for a security clearance.

Contractor Responsibilities for Cleared Facilities

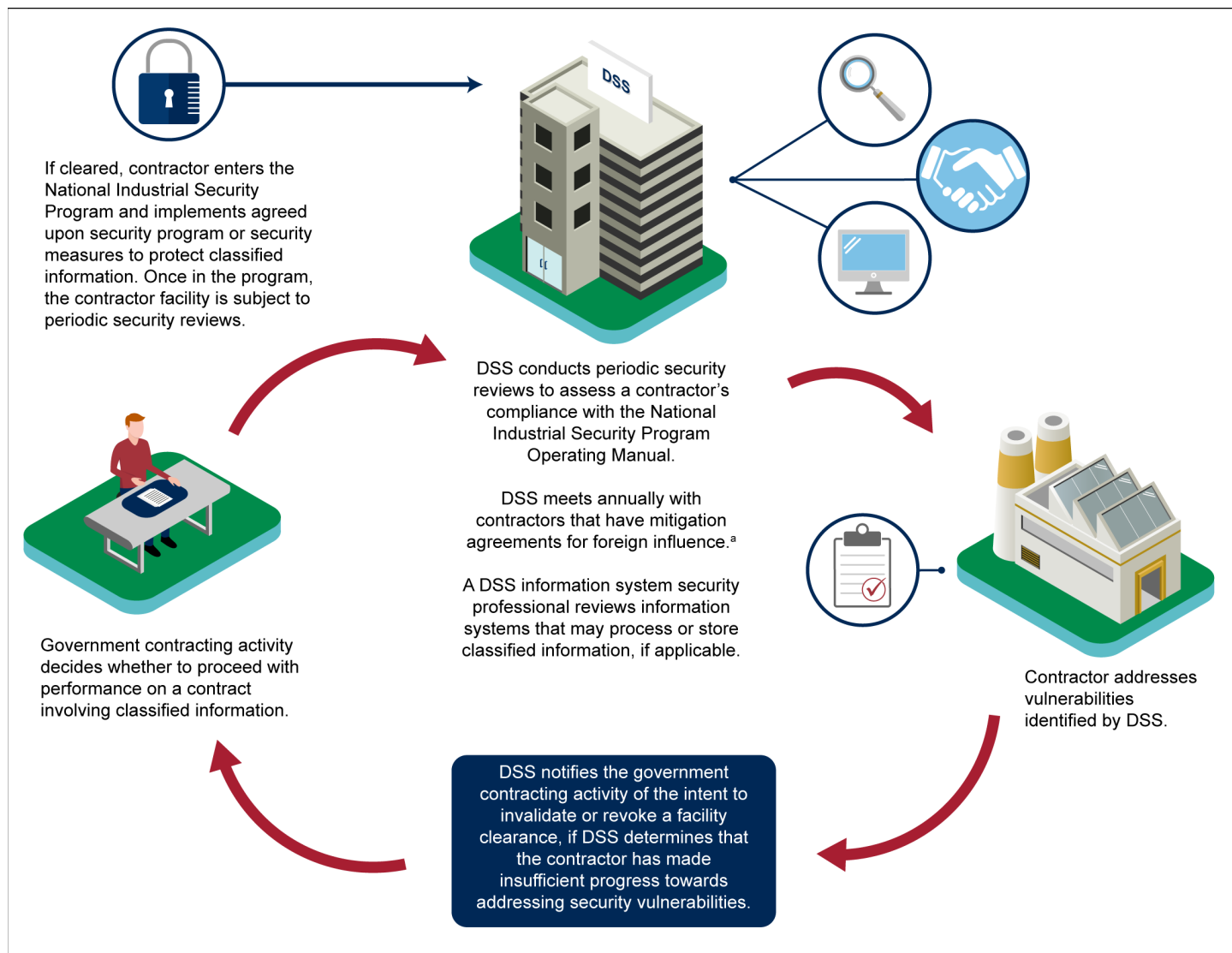
After DSS completes the facility clearance process and determines that a contractor is eligible to access classified information and grants the facility security clearance, the cleared contractor officially enters the National Industrial Security Program. Once in the program, contractors establish a security program at cleared facilities or implement security measures required by the Department of Defense security agreement, as well as any elements required by DSS. Depending on the facility, security measures may address a variety of industrial security issues. 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. In addition, contractors are required to implement insider threat programs, which are meant to prevent persons with approved access to classified information, such as contractor employees, from causing harm to national security through unauthorized disclosures. The insider threat programs may include activities such as training programs about reporting requirements or monitoring classified information systems.

DSS monitors cleared contractor facilities to determine their compliance with the program's requirements for protecting classified information by conducting periodic security reviews. DSS determines the frequency of these reviews, although they generally cannot take place more than once in a 12-month period, according to the operating manual. 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 DSS officials, such as information system security professionals who review a facility's information systems if they are needed to store or process classified information. Moreover, counterintelligence officials may also participate and provide threat information about the facility. Security reviews are generally led by staff located in DSS's 26 field offices across the country. A contractor's facility clearance may be subject to invalidation or revocation if DSS identifies certain vulnerabilities, among other things.¹⁵ See figure 2 for more

¹⁵Invalidation 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 that DSS can take before revoking a facility clearance.

information about DSS's process for monitoring contractor facilities in the program.

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



Source: GAO analysis of Defense Security Service (DSS) processes and interviews with DSS officials. | GAO-18-407

^aMitigation agreements that address foreign ownership, control, or influence ("foreign influence") are intended to prevent situations in which a foreign interest has the power to decide matters affecting a contractor's operations and that could result in unauthorized access to U.S. classified information or adversely affect the performance of classified contracts. For the purposes of our report, a contractor

under "foreign influence" means it is under foreign ownership, control, or influence, as described in section 2-300(a) of the National Industrial Security Program Operating Manual.

In addition to administering the facility clearance process and conducting security reviews at cleared facilities, DSS also collects information from cleared contractors about suspicious contacts, which may involve efforts by an individual to obtain illegal or unauthorized access to classified information, among other things. DSS aggregates this information to identify counterintelligence trends among cleared contractors and refers cases to the relevant agency for further investigation or action.¹⁶

We last issued reports about the National Industrial Security Program in 2004 and 2005. In 2004, we made eight recommendations for DSS to improve its processes for conducting security reviews, such as taking steps to quickly notify government contracting activities when classified information has been lost or compromised.¹⁷ The Department of Defense agreed with our recommendations. In 2005, we made eight recommendations about DSS's oversight of contractors under foreign influence.¹⁸ For example, we recommended that DSS collect and analyze data about foreign business transactions in order to improve its oversight of contractors under foreign influence. The Department of Defense partially agreed with our recommendations and subsequently took action to address them. As of April 2018, 13 of 16 of the recommendations have been implemented. For more detail on our prior recommendations, please see appendix II.

¹⁶DSS issues an annual publication that describes counterintelligence trends, "*Targeting U.S. Technologies: A Trend Analysis Report of Cleared Industry Reporting*".

¹⁷GAO, *Industrial Security: DOD Cannot Provide Adequate Assurances That Its Oversight Ensures the Protection of Classified Information*, [GAO-04-332](#) (Washington, D.C.: Mar. 4, 2004).

¹⁸GAO, *Industrial Security: DOD Cannot Ensure Its Oversight of Contractors under Foreign Influence is Sufficient*, [GAO-05-681](#) (Washington, D.C.: July 15, 2005). GAO also issued a testimony about the National Industrial Security Program that was based on findings reported in [GAO-04-332](#) and [GAO-05-681 – Department of Defense: Observations of the National Industrial Security Program](#), [GAO-08-695T](#) (Washington, D.C.: Apr. 16, 2008).

DSS Upgraded Capabilities for the National Industrial Security Program but Faces Challenges Monitoring Contractors

Since 2005, when we last reviewed how DSS administered the National Industrial Security Program, it has streamlined its facility clearance process in order to make it more efficient. DSS has also strengthened the process to analyze contractors for foreign influence and the Department of Defense issued a rule to clarify policies and procedures for mitigating foreign influence concerns. Despite upgrading its capabilities, DSS continues to face challenges in monitoring cleared contractors with access to classified information.

Streamlined Clearance Processes

In 2004 and 2005, we reported that DSS did not collect and analyze data on contractors operating in the National Industrial Security Program. For example, DSS was not able to analyze data to make informed resource decisions or track key changes that affect contractors operating under foreign influence. In our 2005 report, we recommended that DSS collect and analyze data about foreign business transactions, among other things. As a result, DSS streamlined its facility clearance process by developing two electronic systems for tracking the facility clearance requests and maintaining information on cleared facilities.

1. The Electronic Facility Clearance System is a web-based system that contractors or prospective contractors use to submit their required information, such as key management personnel and other staff who need to be cleared for access as well as business-related items like articles of incorporation, bylaws, and other supporting documentation.
2. The Industrial Security Facilities Database is another web-based system that serves as a repository for information about cleared facilities.

DSS field office and contractor officials we spoke with noted that the web-based systems help them do their job more efficiently. For example, DSS's industrial security representatives stated that these systems make the facility clearance and monitoring process more efficient because it is easier to track the status of documentation received. Industrial security representatives also track conditions that may require changes to their monitoring process through this database, such as a change in ownership or key management personnel. Industrial security representatives noted that being able to track this information electronically is helpful because the facility clearance and monitoring processes involve numerous officials within DSS, as well as other parties, such as the government contracting

activity and the contractor. For example, a government contracting activity can use the database to check whether a facility has been cleared to store classified information onsite before sending materials to them.

In 2017, DSS started the process of modernizing these systems by developing two new systems. DSS officials stated that these two new systems will provide additional automation that can be used in the facility clearance and monitoring processes. The new systems are:

- **National Industrial Security Program Contracts Classification System.** This system collects detailed information about classified contract(s) a facility will support during the initial clearance process as well as throughout the duration of the facility's clearance, to include the facility's assets (e.g. technology produced or expertise provided), and enables the government contracting activity to gain visibility into the subcontractors performing work for each classified contract.
- **National Industrial Security System.** This system will be the official repository for data on cleared facilities. DSS officials noted that the system will help identify foreign influence concerns, such as changes in a contractor's ownership, because they will be more centrally tracked.

Further, in 2017, DSS also issued a manual to reflect an updated process for assessing and authorizing cleared contractors' information systems that process classified information. DSS changed its process to align with the intelligence community, the Department of Defense, and other federal government agencies' standards.¹⁹ DSS previously reviewed systems on regular cycles and is shifting to reflect practices in the intelligence community that are based on assessed threats and target the information systems that pose the most significant risk of losing information. DSS information security system professionals told us that this new authorization process is helping them clarify and communicate the nature of security risks to the contractor. The updated process is intended to include the identification of cybersecurity concerns earlier than the prior

¹⁹Federal agencies have adopted the National Institute of Standards and Technology Risk Management Framework as a common set of guidelines for the assessment and authorization of Information Systems. In an effort to streamline and build reciprocity into the DSS processes, DSS is adopting these standards as well, so that all cleared contractor information systems that process classified information as part of the National Industrial Security Program are authorized under the Risk Management Framework Assessment and Authority process.

approach and enables DSS's information system security professionals to adjust their monitoring to meet emerging cyber threats.

Centralized Support and Strengthened Its Process to Identify Foreign Influence

In response to recommendations we made in 2005, DSS has centralized its support related to identifying and mitigating foreign influence and strengthened its process, including issuing a rule to make the process of mitigation of foreign influence clearer to contractors. Since our last review of the program in 2005, DSS has centralized staff expertise in headquarters to improve the identification and mitigation of foreign influence concerns.²⁰ Whereas DSS used to rely primarily on field staff to negotiate and oversee individual facilities in their respective regions, it now has staff in headquarters, including specialists in law and other areas, who have an agency-wide view of threats and who understand the portfolio of contractors that may be at risk of foreign influence. DSS officials said that this is important because a contractor may have multiple cleared facilities across several regions. They noted that an agency-wide view helps DSS identify trends across facilities that may be tied to a single contractor. The headquarters staff:

- negotiate and put in place mitigation agreements that require contractors under foreign influence to acknowledge and mitigate foreign influence risks, including the development of protective measures to reduce the risk of foreign interests gaining access to classified information;
- identify foreign influence within cleared contractors and provide written analysis to DSS field offices when foreign influence concerns are identified, such as when a foreign contractor acquires a majority or substantial minority position in a U.S. contractor with a cleared facility; and
- provide subject matter expertise in the areas of business, acquisition, intelligence, and international law to develop a comprehensive understanding of companies, their industries and technologies, as well as the regulatory environments in foreign countries.

DSS officials acknowledged that the establishment of a headquarters division in 2008 focused on analyzing foreign influence and issuing related publications was in response to recommendations we made in 2005. DSS's field office industrial security representatives said that the

²⁰[GAO-05-681](#), [GAO-08-695T](#).

written products and specialized foreign influence analysis prepared and disseminated by DSS headquarters has resulted in more timely identification and mitigation of these issues. Examples include:

- *NISP in the News*, an internal weekly publication that provides a summary of business transactions that may result in the need for a mitigation agreement to address foreign influence. Industrial security representatives we spoke with said this publication helps them identify and proactively address issues with their contractors.²¹ DSS officials told us the publication is helpful because it can result in more timely identification and initiate the process for negotiating a mitigation agreement, particularly in cases where a foreign company acquires a facility previously owned by a U.S. contractor. Copies of *NISP in the News* that we reviewed also included information that may affect contractors that are not under a mitigation agreement for foreign influence, such as changes in key management personnel. We previously reported that DSS had challenges identifying these transactions or facility security officers would neglect to report them, which led to delays in putting protective measures in place to prevent unauthorized access to classified information.²²
- Assessments of new contractors that have been sponsored for clearances, which are used to identify and mitigate foreign influence. DSS industrial security representatives stated that this analysis used to be performed in the field but now they can use time previously spent preparing analysis of foreign influence to work with contractors to implement security measures. Further, the assessments help them work more effectively with contractors because they draw upon expertise across different disciplines. For example, 7 of the 13 facility case files we reviewed contained a summary of analysis conducted by specialists in DSS headquarters. The summaries also noted that the specialists reviewed classified and unclassified information on the

²¹*NISP in the News* is the title of an internal DSS publication. According to the operating manual, contractors are required to report change conditions to DSS. Examples of change conditions include, but are not limited to, change of ownership, change of operating name, change in key management personnel, or actions to terminate business.

²²[GAO-05-681](#).

contractor, including counterintelligence information and other U.S. government information, as applicable.²³

In April 2014, the Department of Defense issued a rule about policies and procedures for mitigating foreign ownership, control, or influence.²⁴ This rule was issued in order to ensure maximum uniformity and effectiveness in the Department of Defense implementation of the National Industrial Security Program. The rule detailed specific mitigation approaches for addressing concerns about foreign ownership, control, or influence, which we cover in detail in appendix I. The rule clarified the role of DSS, the government contracting activity, and the contractor during the process when DSS determines that the contractor needs to mitigate potential foreign ownership, control, or influence. The rule also documented policies and procedures regarding how decisions will be made on the appropriate method to mitigate foreign ownership, control, or influence. These include the timing of agency and contractor actions involved in mitigation of foreign ownership, control, or influence and how to proceed in cases where the contractor had not worked out a mitigation agreement with DSS before changed conditions (e.g. indebtedness, ownership, or foreign intelligence threat) occurred, among other things. The rule further stated that DSS, in consultation with the government contracting activity, has discretion to modify or reject the contractor's outlined action plan to mitigate foreign ownership, control, or influence.

²³In one summary, DSS's documentation indicated that the contractor had a case with the Committee on Foreign Investment in the United States, an interagency committee chaired by the Treasury Department that conducts reviews of proposed mergers, acquisitions, or takeovers of a U.S. business by a foreign person. The review is a voluntary process and affords an opportunity to foreign persons and U.S. businesses entering into certain transactions to submit the transaction for review by the committee to assess the impact of the transaction on U.S. national security. GAO issued a related report, *Committee on Foreign Investment in the United States: Treasury Should Coordinate Assessment of Resources Needed to Address Increased Workload*, [GAO-18-249](#) (Washington, D.C.: Feb. 14, 2018).

²⁴On April 9, 2014, the Department of Defense issued an interim final rule, codified at 32 C.F.R. § 117, 79 Fed. Reg. 19,467 (Apr. 9, 2014). The interim final rule clarified and codified policies for ensuring classified information will be properly safeguarded for government contractors that are subject to foreign ownership, control, or influence, and for using security mechanisms to mitigate or negate this foreign ownership, control, or influence. On April 17, 2014, the Department of Defense also published the Department of Defense Manual 5220.22, Volume 3, "National Industrial Security Program: Procedure for Government Activities Relating to Foreign Ownership, Control, or Influence (FOCI)."

Challenges Remain

Despite upgrading its capabilities, DSS officials indicated that they face resource constraints, such as an inability to manage workloads and complete training necessary to stay informed on current threats and technologies. DSS's current resource challenges include:

- **Managing staff workloads.** DSS field officials acknowledged that they have historically faced workload challenges. DSS officials said that their limited staff carry heavy workloads and, according to DSS's most recent biennial report to Congress, were unable to conduct security reviews at about 60 percent of cleared facilities in fiscal year 2016. In addition to their official security reviews, industrial security representatives also conduct informal "advise and assist" efforts when facility officials inquire about a range of security issues, from preparing employees for overseas travel to providing training on reporting suspicious contacts. In fiscal year 2016, industrial security representatives conducted about 22,000 "advise and assist" efforts. DSS officials attribute the heavy workload to the current staffing levels of their field offices and frequent turnover among the industrial security representatives.

DSS officials noted that both hiring and retention are difficult and that these challenges are exacerbated by the fact that it is a relatively small agency with field offices with limited staff. For example, an average field office oversees about 470 facilities and has about 8 industrial security representatives on staff. As a result, if a person leaves, it adds strain to the remaining staff. Most of the contractors' facility security officers we spoke with noted that DSS field officials have heavy workloads that could affect their ability to respond to threats at cleared facilities. Further, DSS indicated that it has limited resources to analyze, process, and distribute counterintelligence to the cleared facilities. For example, DSS received more than 46,000 reports from cleared contractors about suspicious contacts in fiscal year 2016, which was an almost 18 percent increase over the prior year. In comparison, during the same time period, DSS's counterintelligence directorate, which analyzes suspicious contact reports, grew by 7 percent. In addition, DSS's ability to distribute counterintelligence is limited by the geographic distribution of over 12,000 cleared facilities and each facility's capability to receive or store classified communication.

- **Developing foreign influence mitigation agreements.** Multiple DSS industrial security representatives and contractors' facility security officers stated that mitigation agreements to address the risk of foreign influence, including supplemental plans, have become more

detailed and the process to develop and implement them has required additional time and resources. For example, DSS may require a contractor to develop an electronic communications plan, which must include details about which networks will be protected from access by a foreign parent contractor, including monitoring, maintaining, and establishing separate email servers, as appropriate.²⁵ DSS reported in its 2015 biennial report to Congress that the average amount of time to approve and implement a foreign influence mitigation plan was 93 days.²⁶ The length of time to approve and implement a foreign influence mitigation plan more than doubled to 204 days, according to the 2017 biennial report.²⁷ DSS officials stated that this increase is due, in part, to increased complexity of the agreements and the amount of coordination required between the government contracting activity, DSS, and the contractor. A DSS official also noted that over time, the agency has incorporated more information in its analysis and sometimes needs more time to review all the information that may be relevant.

- **Attending relevant trainings.** DSS officials in three of four regions noted that staffing challenges affect their ability to take training, even though industrial security matters continue to become more sophisticated. Information system security professionals said they face challenges in learning technology that continues to evolve. For example, they cited the multiple software products such as operating systems and configurations of information networks that are used in a facility's daily operations. In addition, they need to understand other technologies that can pose risks to industrial security, such as devices that are capable of transmitting data, like cellular phones, and therefore might need to be prohibited from areas where classified information is discussed. As a result, the lack of expertise in multiple technologies hampers their ability to identify vulnerabilities that might leave a facility at risk for loss of classified information. We have previously reported that training staff in new skills, such as cybersecurity, remains an ongoing challenge for the federal government. For example, in 2016, we found that chief information

²⁵For more information about the types of plans to mitigate foreign influence, please see appendix I.

²⁶U.S. Department of Defense, *Biennial Report to Congress on Improving Industrial Security*. (Washington, D.C.: February 2015).

²⁷U.S. Department of Defense, *Biennial Report to Congress on Improving Industrial Security*. (Washington, D.C.: August 2017).

officers throughout the government identified difficulties related to recruiting, hiring, and retaining qualified personnel, as well as ensuring they have the appropriate skills and expertise.²⁸

DSS Has Not Determined How It Will Collaborate with Stakeholders As It Pilots a New Approach

In 2017, DSS announced its plans to transition to a new approach to monitoring cleared facilities in order to address emerging threats to classified information. DSS faces challenges as it pilots its new approach—*DSS in Transition*. DSS has taken steps to begin addressing challenges, including scheduling training for its staff, but has not documented how it will collaborate with its stakeholders or identified the resources needed to monitor cleared facilities.

New Approach to Monitoring Cleared Facilities

In 2017, DSS announced that it would begin transitioning to an asset-and-threat-based monitoring approach. DSS has reported that the United States is facing the most significant foreign intelligence threat it has ever encountered and adversaries are attacking cleared facilities at unprecedented rates. In fact, adversaries are varying their methods and adjusting their priorities based on the targeted information they need. The new approach is expected to involve DSS working collaboratively with contractors and government contracting activities to design a customized security plan for each facility based on threats specific to its assets rather than using a standardized worksheet to perform security reviews. DSS officials said that customized security plans will be developed based on assets at the specific facilities. For example, a contractor providing information technology services may need the latest software to thwart cyberattacks while a contractor that engineers weapons systems may need additional secure storage facilities and work areas to ensure an adversary cannot physically extract classified information or technology. As a result, according to agency officials, these customized security plans represent a departure from a “one size fits all” or schedule-driven approach to overseeing contractors’ protection of classified information. According to DSS officials, this new approach, *DSS in Transition* will use the Department of Defense’s list of critical technologies and programs, along with counterintelligence, to prioritize facilities for security reviews

²⁸GAO, *Federal Chief Information Security Officers: Opportunities Exist to Improve Roles and Address Challenges to Authority*, GAO-16-686 (Washington, D.C.: Aug. 26, 2017).

based on their assets and the severity of the threats to them. See table 1 for more information about the monitoring approaches.

Table 1: Comparison of the Defense Security Service’s (DSS) Current and New Approaches for Monitoring Cleared Facilities

| Current Monitoring Approach | New Approach (as of GAO review March 2018) – <i>DSS in Transition</i> |
|---|---|
| Scheduling | |
| Schedules security reviews on a 90-day work plan starting with specific facilities, such as those with mitigation agreements for foreign influence or classified information systems. | Will use national intelligence and Department of Defense’s list of critical technologies and programs to prioritize security reviews at facilities based on their assets and threats to those assets. |
| Ensures security reviews of facilities with foreign influence are scheduled 30 to 60 days before required annual meeting. | Will look to contractors and government to identify assets at facilities. |
| | Will schedule security reviews based on plans designed for each facility’s customized security plan. |
| Monitoring | |
| Conducts security reviews that focus on a contractor’s adherence with National Industrial Security Program Operating Manual requirements. | Will conduct security reviews to develop customized security plans and assess implementation of such plans to ensure contractors protect assets. |
| Results in a security rating based on contractor’s compliance with the operating manual. | Expected to result in framework to develop a customized security plan for the threats facing each facility. |

Source: GAO analysis of DSS documentation and interviews with DSS officials. | GAO-18-407

After announcing *DSS in Transition* in 2017, DSS began taking steps to develop its methodology for the new approach, including prioritization of facilities and developing procedures for executing customized security plans. In a January 2018 letter to industry, DSS stated that it plans to pilot the new approach by working with one facility in each of its four regions to develop a customized security plan and use the lessons learned to refine the process. While it is piloting the approach at four facilities, DSS notified contractors not participating in the pilot that DSS would partner with selected facilities to identify and document their critical assets. Industry, including contractors and prospective contractors that are interested in U.S. government contract awards in the future, are awaiting more details on how DSS plans to implement *DSS in Transition*, including who would be responsible for the costs of additional security requirements, according to a March 2018 statement from the industry spokesperson of the National Industrial Security Program Policy Advisory Committee.

Collaboration Needed with Stakeholders As It Pilots the New Approach

Although DSS began piloting *DSS in Transition* in January 2018, it has not determined how it will collaborate with government contracting activities, the intelligence community, other federal agencies, and contractors. In particular, DSS has not identified its stakeholders' roles and responsibilities in terms of who needs to communicate and coordinate with whom and when, which is necessary to successfully implement the new approach. For example, DSS needs to establish agreed-upon criteria for what information a government contracting activity would need to provide to DSS in order to develop a customized security plan for a facility. GAO's Federal Internal Control Standards establish the need to coordinate with stakeholders and clearly define roles and responsibilities, among other things.²⁹ In addition, our leading practices for interagency collaboration state that successful collaborative working relationships require organizations to agree on roles and responsibilities and identify the resources necessary to accomplish objectives.³⁰ For example, GAO found it is unclear how DSS will determine what resources it needs as it has not identified the necessary roles and responsibilities. DSS has taken steps to begin addressing these challenges by establishing an office dedicated to documenting processes and procedures for how *DSS in Transition* will be implemented, providing a concept of operations, and scheduling training for its staff. However, to monitor cleared facilities, DSS needs information from the various National Industrial Security Program stakeholders, including:

- **Government contracting activity.** DSS officials stated that, under the new approach to monitoring cleared facilities, they will need to better communicate and coordinate with the government contracting activity. For example, in some circumstances, DSS officials will have to collaborate with government contracting activities to determine when a security plan is no longer sufficient as threats and mitigation methods evolve. DSS officials stated that communication and coordination with government contracting activities has been a challenge because industrial security is often considered an added duty on top of their contract management responsibilities. Further, DSS officials indicated that staff turnover at government contracting activities and the lack of clear roles and responsibilities have led to

²⁹See GAO, *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington, D.C.: Sept. 10, 2014).

³⁰See GAO, *Managing for Results: Key Considerations for Implementing Interagency Collaboration Mechanisms*, [GAO-12-1022](#) (Washington, D.C.: Sept. 27, 2012).

delays in resolving a facility's vulnerabilities. According to DSS officials, it is difficult to determine whether they have the correct point of contact at the government contracting activity to discuss vulnerabilities at a facility, which, if left unaddressed, can leave classified information at risk for loss. There are no formal agreements about how a case should be elevated and resolved if DSS identifies vulnerabilities and is unable to elicit a response from the government contracting activity about further action, according to DSS officials. In addition, DSS officials stated that they will need to work with the government contracting activity to assess the risk of security vulnerabilities that involve subcontractors working on contracts containing classified information. In the past, a government contracting activity might not know the identities of subcontractors if they were sponsored by a cleared contractor. Given the adversaries' ability to vary its methods to target information it needs, the government needs to know who—regardless of subcontracting tier—is accessing classified information.

- **Government intelligence community.** We found DSS has not established how it will collaborate with the intelligence community, including formalizing roles and responsibilities for its new approach. A DSS counterintelligence official told us that DSS currently relies on a combination of its own counterintelligence staff and informal coordination with other agencies, such as the Federal Bureau of Investigation. Another DSS official stated that they have worked with the Federal Bureau of Investigation to deliver counterintelligence when a facility does not have the capacity to receive classified information electronically. According to DSS field officials, the current process is handled on a case-by-case basis, depending on the availability of resources. Although DSS's Counterintelligence Directorate recently became part of the intelligence community and will potentially have greater access to counterintelligence data, it will need to determine how to regularly communicate with the intelligence community to fully understand their products and share current threats and vulnerabilities with certain contractors under *DSS in Transition*.³¹
- **Other government agencies.** DSS relies on collaborating with other cognizant security agencies to develop a complete picture of the threats to contractors. In addition to the Department of Defense, there

³¹The Director of DSS was recently designated as the head of a Defense Intelligence Component, specifically only for the counterintelligence element of DSS that collects, analyzes, retains, and disseminates information in support of the organization's counterintelligence missions.

are four other federal agencies that have authority to inspect and monitor facilities to ensure the protection of classified information.³² DSS may only conduct security reviews for facilities performing contracts awarded by these agencies if the Department of Defense is the cognizant security agency for that facility. Contracts where another agency is the cognizant security agency may involve information coveted by adversaries, but DSS industrial security representatives have acknowledged that they may not know why the information is coveted or that it exists. Given the new approach to develop a complete picture of threats to a facility, DSS will need additional information from other cognizant security agencies that it may not have sought in the past. As a result, DSS needs to establish how best to collaborate with other agencies, such as identifying appropriate points of contacts and specific time frames to conduct outreach, to effectively implement DSS's new approach to monitor contractors.

- **Cleared contractors.** DSS officials said that *DSS in Transition* will require contractors to identify assets in a greater level of detail than what was previously expected of them. In order to develop a security plan unique to the facility, the contractor's facility security officers will need to understand these assets and why adversaries would want to target them in order to develop and implement specific security measures. Since DSS officials cannot be onsite every day, they have to rely on the contractor's facility security officer or other key management personnel at cleared facilities to identify and report potential problems.³³ However, DSS officials noted that convincing facility staff to spend more time on security-related matters may be difficult at facilities where one employee may serve as the contractor's facility security officer in addition to having other responsibilities. In addition, DSS officials stated that contractors' security costs are typically not profit-generators and realize that *DSS in Transition* may require the contractor to expend more time, money, and energy to

³²Executive Order No. 12829, as amended.

³³For certain mitigation agreements (Security Control Agreement, Special Security Agreement, Voting Trust, and Proxy Agreement) for foreign influence, the contractor may be required to establish a government security committee, which is a permanent committee of a contractor's Board of Directors. The members of the committee are required to ensure that the contractor maintains policies and procedures to safeguard classified and export-controlled information entrusted to it, and that violations of those policies and procedures are promptly investigated and reported to the appropriate authority when it has been determined that a violation has occurred.

address vulnerabilities or enact policies to safeguard against adversaries.

DSS recognizes the need to keep industry informed and its implementation plans for *DSS in Transition* need to address what level of communication and coordination is required. For example, DSS currently uses a rating system to indicate how well a contractor is meeting the requirements of the operating manual as a metric for how it is protecting classified information. As DSS moves toward developing customized security plans that are unique to each facility's threats and assets, it needs to formalize new approaches to communicate with contractors how well they are protecting classified information.

In addition to piloting *DSS in Transition*, DSS is reassuming responsibility for conducting background and security investigations for the Department of Defense, which could potentially magnify its workload challenges.³⁴ DSS previously held these responsibilities but they were transitioned to the Office of Personnel Management in 2005. The National Defense Authorization Act of Fiscal Year 2018 required DSS to reassume this background and security investigations mission by implementing a phased transition by October 1, 2020. This phased transition will overlap with DSS's piloting of *DSS in Transition* and may create disruptions as an agency of over 700 employees assumes responsibility for a background and security investigations mission that currently has more than 7,000 employees and contractors. In January 2018, we added personnel security clearances to our high-risk list, a list of federal areas in need of either broad-based transformation or specific reforms to prevent waste, fraud, and abuse. This issue is on the list because we identified: (1) a significant backlog of background investigations; (2) a lack of long-term goals for increasing federal and contractor-provided investigator capacity to address the backlog; and (3) delays in the timely processing of security clearances among other factors.³⁵ DSS officials have identified potential benefits and challenges with reassuming the background investigations mission, and, in August 2017, the Department of Defense submitted a

³⁴DSS will assume conducting personnel background investigations under the National Defense Authorization Act of Fiscal Year 2018, Pub. L. No. 115-91, § 925.

³⁵Our High-Risk program has served to identify and help resolve serious weaknesses in areas that involve substantial resources and provide critical services to the public. See GAO, *High-Risk Series: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others*, [GAO-17-317](#) (Washington, D.C.: Feb. 15, 2017) for our most recent report. We added personnel security clearances to the high-risk list on January 25, 2018.

plan for a 3-year phased transition to assume the background and security investigations mission. In March 2018, we reported that this transition could potentially affect the timely processing of personnel security clearances, the backlog, and other reform initiatives but the effect is unknown at this time.³⁶

Conclusions

Given the changing nature of threats to classified information, DSS needs to ensure that classified information is protected from unauthorized access. While DSS has upgraded its capabilities for identifying foreign influence, DSS officials acknowledged that adversaries continue to evolve, and classified information and technologies remain vulnerable to exploitation. In response, in 2017, DSS launched a new approach (*DSS in Transition*) to change how it oversees contractors with access to classified information. As DSS pilots the new approach, it will need to work with government contracting activities, the intelligence community, other agencies, and cleared contractors to determine their roles and responsibilities in protecting classified information at every facility in the program. Without the necessary information—that is gained through communicating and coordinating with stakeholders—to assess the threats to the nation’s most critical technologies and programs, DSS will be unable to provide appropriate oversight that addresses the most significant threats to industrial security. Also, DSS has not identified the resources necessary, including the number of personnel needed to implement its new approach, which will add pressure to an agency accepting a background and security investigations mission that has significant backlog and timeliness challenges. Until DSS identifies roles and responsibilities and determines how it will collaborate with stakeholders for the pilot, it will be difficult to assess whether the new approach is effective in protecting classified information.

³⁶GAO, *Personnel Security Clearances: Additional Actions Needed to Implement Key Reforms and Improve Timely Processing of Investigations*, [GAO-18-431T](#) (Washington, D.C.: Mar. 7, 2018).

Recommendation for Executive Action

We are making one recommendation to the Director of the Defense Security Service:

Determine how it will collaborate with stakeholders as it pilots a new approach to overseeing contractors with cleared facilities (*DSS in Transition*), including identifying roles and responsibilities and the related resources needed. (Recommendation 1)

Agency Comments and Our Evaluation

We provided a draft of this report for review and comment to DSS.

DSS provided written comments, which are reproduced in appendix III. In its comments, DSS concurred with the recommendation and summarized actions it is taking to pilot its new approach (*DSS in Transition*). DSS also provided technical comments, which we incorporated as appropriate.

We are sending copies of this report to the appropriate congressional committees, the Secretary of Defense, Director of DSS, and other interested parties. In addition, the report is available at no charge on the GAO website at <http://www.gao.gov>.

If you or your staff have any questions about this report, please contact me at (202) 512-4841 or makm@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix IV.



Marie A. Mak

Director, Contracting and National Security Acquisitions

Appendix I: Methods for Mitigating Foreign Influence

Since our July 2005 report, the Defense Security Service (DSS) has taken additional steps to address oversight of contractors with foreign influence. In April 2014, the Department of Defense issued a rule that clarified policies for oversight of contractors under foreign ownership, control, or influence.¹ The rule detailed specific mitigation approaches for addressing foreign ownership, control, or influence concerns. The rule provided detail regarding the terms of each of these types of foreign ownership, control, or influence mitigation agreements and the circumstances under which each may be appropriate. The types of mitigation specified in the rule are:

- *Board Resolution.* The board resolution may be used when a foreign entity does not own voting interests sufficient to elect a representative to the company's governing board.
- *Security Control Agreement.* The security control agreement is a tailored foreign ownership, control, or influence mitigation agreement, often used when a foreign interest does not effectively own or control a company or corporate family but the foreign interest is entitled to representation on the company's board.
- *Special Security Agreement.* The special security agreement may be used when a company is effectively owned or controlled by a foreign interest. Access to certain proscribed classified information by a company cleared under this agreement may require that the government contracting activity complete a National Interest Determination to determine that the release of proscribed information to the company is consistent with the national security interests of the United States.
- *Voting Trust Agreement and Proxy Agreement.* These foreign ownership, control, or influence mitigation agreements may be used when a foreign interest effectively owns or controls a company or corporate family. Under these agreements, the foreign owner relinquishes most rights associated with ownership of the company to cleared United States citizens approved by the U.S. government.²

DSS has clarified the types of supplemental plans that companies must submit to document specific steps that it will take to mitigate foreign

¹On April 9, 2014, the Department of Defense issued an interim final rule, codified at 32 C.F.R. § 117, 79 Fed. Reg. 19,467 (Apr. 9, 2014).

²In addition to these types of mitigation plans, DSS has the authority to customize foreign ownership, control, or influence mitigation plans, depending on the circumstances.

influence. Table 2 describes the types of plans and provides examples of how they mitigate foreign influence.

Table 2: Types of Plans to Mitigate Foreign Influence

| Foreign Influence Mitigation Plan | Description of Plan | Example of How Plan Mitigates Foreign Influence |
|-----------------------------------|--|---|
| Affiliated operations plan | Describes the shared business services the company plans to engage in, including the entity paying for the service, the benefits received, specific sub-categories of services received, procedures for providing the services and technologies used, the involvement of key management personnel in the shared administrative service, and risk and mitigation procedures, among other things. | An affiliated operations plan we reviewed documented the risk associated with shared legal services. To mitigate this risk, the plan stated that DSS may review all emails, phone calls, and visits between the facility and the parent company concerning shared legal services. |
| Technology control plan | Describes security measures necessary to foreclose the possible unauthorized access to classified or export-controlled information by employees or visitors who are not U.S. citizens or affiliates. The plan is a facility-specific requirement and establishes measures to assure that access by these employees or visitors and foreign affiliates is strictly limited to only specific information for which disclosure authorization has been obtained. | A technology control plan we reviewed stated that the facility must maintain documentation of its products and their jurisdiction, providing the name of the commodity, the export jurisdiction, classification information, who classified or categorized the product, and where the item is manufactured or exported. |
| Electronic communications plan | Documents policies and procedures assuring electronic communications between the parent company under foreign influence and its subsidiaries and affiliates do not disclose classified information or export-controlled information without proper authorization. | According to an electronic communications plan we reviewed, critical information technology resources are physically located in locked rooms. The plan states that physical access is restricted to authorized personnel using badge reader, key, or cipher lock. Access lists will be maintained by human resources or security personnel. |
| Facilities location plan | Required when a company is located or plans to relocate within the proximity of an affiliate that would reasonably inhibit the cleared company's ability to comply with the mitigation agreement and includes justification for close proximity with affiliates and how the colocation is monitored, among other things. | A facilities location plan we reviewed contained floor plans and building diagrams and documented mitigation procedures for each colocation. |

Source: GAO analysis of Defense Security Service (DSS) procedures and facility documentation. | GAO-18-407

Appendix II: Status of Prior GAO Recommendations Related to the National Industrial Security Program

In 2004 and 2005, GAO issued reports about the National Industrial Security Program and made 16 recommendations.¹ Prior to the start of our review, the Department of Defense, through the Defense Security Service (DSS), implemented two of the recommendations. Below is our assessment of whether DSS addressed the remaining 14 recommendations that had been previously recorded as “closed – not implemented”.

Table 3 provides a summary of those recommendations and the actions that DSS has taken in response to the recommendations. A number of the recommendations we made were aimed at clarifying policies related to contractors under foreign influence that were part of the National Industrial Security Program. The primary evidence to support our conclusions is cited in the last column.

In GAO-04-332, we made eight recommendations that were recorded as closed not implemented prior to the start of this review. Based on information obtained during this review, seven of the recommendations will be closed as implemented. The recommendation that remains closed as not implemented was outside of the scope of the current review.

In GAO-05-681, we made eight recommendations and two of the recommendations were closed as implemented prior to this review. Based on information obtained during this review, four of the remaining six recommendations will be closed as implemented. We were unable to close two of the six recommendations as implemented based on the information provided during this review.

¹GAO, *Industrial Security: DOD Cannot Provide Adequate Assurances That Its Oversight Ensures the Protection of Classified Information*, [GAO-04-332](#) (Washington, D.C.: Mar. 4, 2004); and *Industrial Security: DOD Cannot Ensure Its Oversight of Contractors under Foreign Influence is Sufficient*, [GAO-05-681](#) (Washington, D.C.: July 15, 2005).

**Appendix II: Status of Prior GAO
Recommendations Related to the
National Industrial Security Program**

Table 3: Summary of Prior GAO Recommendations Related to the National Industrial Security Program and Actions to Address Them

| Industrial Security: DOD Cannot Provide Adequate Assurances That Its Oversight Ensures the Protection of Classified Information (GAO-04-332) | |
|---|--|
| Recommendations | Status as of April 2018: Implemented |
| 1 | <p>Establish mechanisms that create accountability for knowing the identity of government customers so that industrial security representatives can readily notify those customers of any loss or compromise.</p> <p>In July 2017, Defense Security Service provided information from its facility database that included the contract number.</p> |
| 2 | <p>Explore the effects of establishing specific time-based criteria in the Industrial Security Operating Manual for representatives to make determinations and notify government customers.</p> <p>The May 2015 Industrial Security Operating Manual provides time frames for conducting initial screening interviews and notifying government customers of facility clearance determinations.</p> |
| 3 | <p>Revise the Industrial Security Operating Manual requirements to emphasize the need to apply the established determinations regarding the compromise or loss of classified information.</p> <p>The May 2015 Industrial Security Operating Manual establishes requirements related to making determinations regarding the compromise or loss of classified information.</p> |
| 4 | <p>Regularly analyze information (that needs to be analyzed to detect systemic vulnerabilities and identify trends regarding how contractor facilities protect classified information) to make informed management decisions about the use of resources for its oversight activities and make any needed changes to those activities or procedures to reduce the risk of information compromise.</p> <p>DSS analyzes and reports on resources in its biennial report to Congress. The last report was issued in August 2017.</p> |
| 5 | <p>Identify the information that needs to be analyzed to detect systemic vulnerabilities and identify trends regarding how contractor facilities protect classified information.</p> <p>DSS headquarters, including a division focused on issues of foreign ownership, control, or influence, collects and reports information on trends in how contractor facilities protect classified information in its biennial report to Congress. The headquarters division also publishes an internal publication based on monitoring of foreign business transactions and changed conditions at cleared facilities.</p> |
| 6 | <p>Establish results-oriented performance goals and measures that would enable DSS to assess the extent to which it is achieving its industrial security mission.</p> <p>DSS has developed a strategic plan that contains results-oriented performance goals and measures that are tied to its mission.</p> |
| 7 | <p>Revise the Industrial Security Operating Manual to require industrial security representatives to inform facilities of the official determinations regarding the loss or compromise of classified information.</p> <p>The May 2015 Industrial Security Operating Manual identifies a process for industrial security representatives to follow when informing facilities of the official determinations regarding the loss or compromise of classified information, including the stakeholders involved in the process and the timeframes and methods for communicating this information.</p> |

**Appendix II: Status of Prior GAO
Recommendations Related to the
National Industrial Security Program**

| Industrial Security: DOD Cannot Ensure Its Oversight of Contractors under Foreign Influence Is Sufficient (GAO-05-681) | | |
|---|--|---|
| Recommendations | Status as of April 2018: Implemented | |
| 1 | Develop a plan to systematically review and evaluate the effectiveness of the foreign ownership process. | DSS has developed a strategic plan to assess how it is performing its mission. DSS also reports performance metrics related to how it addresses foreign influence in its biennial report to Congress. |
| 2 | Collect and analyze data on contractors operating under all protective measures as well as changes in types and prevalence of foreign business transactions reported by contractors. | DSS has divisions in headquarters that collect and analyze data on foreign business transactions at contractor facilities. |
| 3 | Clarify when contractors need to report foreign business transactions to DSS. | The May 2015 Industrial Security Operating Manual clarifies the need to report foreign business transactions to DSS and how this should occur. |
| 4 | Determine how contractors should report and communicate dates of specific foreign business transactions to DSS. | |

Source: GAO analysis of Defense Security Service (DSS) documentation. | GAO-18-407

Appendix III: Comments from the Department of Defense



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

INTELLIGENCE

APR 25 2018

Ms. Marie Mak
Director, Contracting and National Security Acquisitions
U.S. Government Accountability Office
441 G Street, NW
Washington DC 20548

Dear Ms. Mak:

This is the Department of Defense (DoD) response to the Government Accountability Office (GAO) Draft Report GAO-18-407, "PROTECTING CLASSIFIED INFORMATION: Defense Security Service Should Address Challenges as New Approach is Piloted" dated March 30, 2018 (GAO Code 101654). As its single recommendation, GAO recommends that the Director of the Defense Security Service: "Determine how it will collaborate with stakeholders as it pilots a new approach to overseeing contractors with cleared facilities ("DSS in Transition"), including identifying roles and responsibilities and the related resources needed."

DoD concurs, with the following comments:

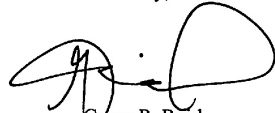
- The Defense Security Service's "DSS in Transition" initiative is a transformative, enterprise-wide effort requiring robust, ongoing collaboration with government and industry stakeholders in accordance with program management standards and Federal internal control principles. In March 2017, the Defense Security Service began collaborating with stakeholders and conducting senior-level industry focus groups to develop, test, and refine the new methodology through the summer of 2017.
- In May 2017, the Defense Security Service launched five integrated process teams aligned with the primary components of the new methodology. These teams included government and industry stakeholders in testing, refining, and validating the "DSS in Transition" methodology.
- In the second quarter of fiscal year 2018, the Director, Defense Security Service placed implementation management under the control of a program management office and established the "DSS in Transition" Implementation Program Review Board. The Board will manage a phased implementation plan in 2018 and continuing through 2019. Throughout the phased implementation plan, the Implementation Program Review Board will perform a detailed identification and analysis of stakeholders to determine needs, roles, responsibilities, and appropriate communication channels, including the National Industrial Security Program Policy Advisory Committee.
- The Defense Security Service is also conducting a mission needs analysis of the new oversight methodology to prepare for the phased transition from operational concept



development to program execution. Any gaps and refinements identified during each of these phases will be prioritized, resource requirements defined, and stakeholder roles and responsibilities documented. For the remainder of 2018 and in 2019, the Defense Security Service will continue to leverage existing industry and government forums, as well as stakeholder focus groups created specifically in support of methodology development.

DoD appreciates the credit given to the Defense Security Service for implementing recommendations from the prior GAO reports on the National Industrial Security Program. Technical comments on this GAO report were sent via email. My point of contact is Ms. Valerie Heil, who can be reached at Valerie.I.heil.civ@mail.mil or 703-692-3754.

Sincerely,

A handwritten signature in black ink, appearing to read 'Garry P. Reid', with a large, stylized flourish at the end.

Garry P. Reid
Director for Defense Intelligence
(Intelligence & Security)

Appendix IV: GAO Contact and Staff Acknowledgments

GAO Contact

Marie A. Mak, (202) 512-4841 or makm@gao.gov.

Staff Acknowledgments

In addition to the contact named above, Penny Berrier (Assistant Director), Lorraine Ettaro, Gina Flacco, Stephanie Gustafson, John Rastler, Sylvia Schatz, Roxanna Sun, Alyssa Weir, and Jocelyn Yin made key contributions to this report.

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 GAO's website (<https://www.gao.gov>). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to <https://www.gao.gov> and select "E-mail Updates."

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 [Facebook](#), [Flickr](#), [Twitter](#), and [YouTube](#).
Subscribe to our [RSS Feeds](#) or [E-mail 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:

Website: <https://www.gao.gov/fraudnet/fraudnet.htm>

Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Orice Williams Brown, Managing Director, WilliamsO@gao.gov, (202) 512-4400,
U.S. Government Accountability Office, 441 G Street NW, Room 7125,
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

James-Christian Blockwood, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548



Please Print on Recycled Paper.