United States General Accounting Office

GAO

Report to the Committee on Armed Services, U.S. Senate

March 2004

INDUSTRIAL SECURITY

DOD Cannot Provide Adequate Assurances That Its Oversight Ensures the Protection of Classified Information

GAO-04-332

March 2004

INDUSTRIAL SECURITY

DOD Cannot Provide Adequate Assurances That Its Oversight Ensures the Protection of Classified Information

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-04-332, a report to the Senate Committee on Armed Services

Why GAO Did This Study

Department of Defense (DOD) contractors perform numerous services that require access to classified information. With access comes the possibility of compromise, particularly as foreign entities increasingly seek U.S. military technologies. To ensure the protection of classified information, the National Industrial Security Program (NISP) establishes requirements that contractors must meet. In administering the NISP for DOD and 24 other government agencies, DOD's Defense Security Service (DSS) monitors whether 11,000-plus contractor facilities' security programs meet NISP requirements.

In response to a Senate report accompanying the National Defense Authorization Act for Fiscal Year 2004, GAO assessed DSS's oversight and examined DSS's actions after possible compromises of classified information.

What GAO Recommends

GAO recommends that DSS improve its oversight of contractors. GAO also recommends that DSS take steps to ensure that determinations for possible information compromises be properly made and that government agencies be quickly notified when their classified information has been lost or compromised. DOD concurred with GAO's recommendations.

www.gao.gov/cgi-bin/getrpt?GAO-04-332.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Katherine Schinasi at (202) 512-4841 or schinasik@gao.gov.

What GAO Found

DSS cannot provide adequate assurances to government agencies that its oversight of contractor facilities reduces the risk of information compromise. DSS is unable to provide this assurance because its performance goals and measures do not relate directly to the protection of classified information. While DSS maintains files on contractor facilities' security programs and their security violations, it does not analyze this information. Further, the manner in which this information is maintained—geographically dispersed paper-based files—does not lend itself to analysis. By not analyzing information on security violations and how well classified information is being protected across all facilities, DSS cannot identify systemic vulnerabilities and make corrective changes to reduce the risk of information compromise.

When a contractor facility reports a violation and the possible compromise of classified information, DSS does not always follow established procedures. After receiving a report of a possible information compromise, DSS is required to determine whether compromise occurred and to notify the affected government agency so it can assess any damage and take actions to mitigate the effects of the suspected compromise, compromise, or loss. However, DSS failed to make determinations in many of the 93 violations GAO reviewed and made inappropriate determinations in others:

- In 39 of the 93 violations, DSS made no determinations regarding compromise.
- For 30 of the remaining 54 violations, DSS's determinations were not consistent with established criteria.

As a result, government agencies are not being kept informed of possible compromises of their information.

In addition, weeks or months can pass before government agencies are notified by DSS of possible information compromises because of difficulties in identifying the affected agencies. In 11 out of 16 instances GAO reviewed, it took DSS more than 30 days to notify the affected agency that its information had been lost or compromised. DSS relies on contractor facilities to identify the affected government agencies, but some facilities cannot readily provide DSS with this information because they are subcontractors that have to obtain the identity of the government agency from the prime contractors. In one case, 5 months passed before a subcontractor facility could provide DSS with the identity of the government agency whose information was suspected of being compromised. Such delays limit the government agencies' opportunity to assess and mitigate any damage from loss or compromise.

Contents

Abbreviations

DOD	Department of Defense
DSS	Defense Security Service
GAO	General Accounting Office
NISP	National Industrial Security Program
NISPOM	National Industrial Security Program Operating Manual

GAO
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, DC 20548

March 3, 2004

The Honorable John W. Warner
Chairman
The Honorable Carl Levin
Ranking Member
Committee on Armed Services
United States Senate

Contractors for the Department of Defense (DOD) perform a multitude of services, ranging from designing advanced weapons used by U.S. forces around the world to providing translation services for prisoner interrogations at Guantanamo Bay, Cuba. Because a large portion of their work is vital to national security, contractors often require access to classified information. However, with contractor access comes the possibility that classified information will be compromised and national security will be harmed. Over the last several years, there have been several reported incidents of contractors handling classified information carelessly, losing it, and even providing it to unauthorized persons. These incidents have occurred at a time when foreign entities are increasing their attempts to obtain information from U.S. industry on militarily critical technologies, such as encryption devices or target recognition components for missiles. Further, the risk of compromise has grown with the increased use of the Internet to transfer information almost anywhere in the world.

Given the risk of information compromise, contractors are required to have security programs that provide DOD and other agencies with assurances that classified information will be appropriately safeguarded. The National Industrial Security Program (NISP) establishes requirements that contractors' programs must meet and a process for ensuring that contractors adhere to the requirements. DOD's Defense Security Service (DSS) administers the NISP on behalf of DOD and 24 other federal agencies. DSS grants clearances to contractor facilities so they can access and, in some cases, store classified information. DSS then monitors over 11,000 facilities' security programs to ensure that they meet NISP

requirements and to assure government customers[1] that their classified information is appropriately safeguarded.

In a report accompanying the National Defense Authorization Act for Fiscal Year 2004, the Senate Committee on Armed Services directed us to review the NISP and DOD's oversight of contractors' programs to protect sensitive information and technology. In response, we assessed (1) DSS's oversight of contractor facilities' implementation of the NISP and (2) DSS's adherence to required procedures after a security violation and possible compromise of classified information.[2] Details on the scope and methodology of our review can be found in appendix I.

Results in Brief

DSS cannot provide adequate assurances to government customers that its oversight of contractors reduces the risk of classified information being compromised. DSS cannot provide this assurance because its performance measures do not enable it to evaluate whether its oversight ensures the protection of classified information. Instead of focusing on the overall results of its oversight, DSS measures performance in terms of processes, such as the number of security reviews completed on time. DSS also evaluates the completeness of reports on security reviews conducted at contractor facilities, but does not evaluate its performance in terms of the results of these reviews and how well contractors are protecting classified information. DSS does not analyze the information it maintains on contractors' protection of classified information nor does the manner in which DSS maintains this information lend itself to such analysis. This lack of analysis limits DSS's ability to detect trends in the protection of classified information across facilities, to determine sources of security vulnerabilities, and to identify those contractors with the greatest risk of compromise. Therefore, DSS cannot determine where systemic vulnerabilities exist and make corrective changes to reduce the risk of information compromise.

[1]Throughout this report, "government customer" refers to the government contracting activity within a federal agency that awarded a contract requiring access to classified information.

[2]As agreed with committee staff, our review was limited to DSS's oversight of contractor facilities' protection of Confidential, Secret, and Top Secret information as defined in Executive Order no. 12958, as amended, and did not include DSS's oversight of special access programs at contractor facilities. Special access programs are established to provide protection for particularly sensitive classified information beyond that normally required for Top Secret, Secret, or Confidential information.

DSS has not always followed required procedures when contractors have reported security violations and possible compromises of classified information. After receiving a report of possible information compromise, DSS is required to determine whether compromise occurred and notify the affected government customer so it can assess the extent of damage and take actions to minimize the effects of suspected compromise, compromise, or loss. However, for 39 of the 93 reported violations we reviewed,[3] DSS made no determinations. For 30 of the remaining 54 violations, DSS's determinations were not consistent with the established criteria. As a result, government customers have not been kept informed of possible compromises of their information and DOD and other agencies cannot be sure that appropriate actions have been taken. In addition, DSS has frequently been unable to quickly notify government customers about a suspected compromise, compromise, or loss because of difficulties in identifying the affected customers. For 11 of the 16 instances we identified in which DSS notified the government customer of a violation, DSS's notification took more than 30 days. Some contractors could not readily provide DSS with information on the government customers because they were subcontractors that had to obtain the government customers' identification from prime contractors. In one case, a subcontractor took 5 months to identify the government customer so DSS could notify the affected customer that its information was suspected of being compromised.

In this report, we are making three recommendations to DOD to improve the oversight of contractors. We make four additional recommendations to DOD to ensure that appropriate determinations are made regarding possible information compromises and that government customers are quickly notified of such situations. We also make a recommendation to improve contractors' understanding of violation-reporting requirements. In commenting on a draft of this report, DOD agreed to implement these recommendations. However, DOD disagreed with our conclusions that DSS cannot provide adequate assurances that its oversight of contractors ensures the protection of classified information and that there are weaknesses in DSS's processes related to possible information compromises.

[3]The 93 violations we reviewed were reported by the 13 facilities selected for our case study. The selected facilities reported the 93 violations between January 1, 2001, and the time of our file reviews at DSS offices throughout the country. As explained in appendix I, the 13 facilities were selected on the basis of size, clearance level, and geographic location.

Background

Industrial security integrates information, personnel, and physical security to protect classified information entrusted to contractors. The goal is to ensure that contractors' security programs detect and deter espionage and counter the threat posed by adversaries seeking classified information. According to DSS, attempts by foreign agents to obtain information from contractors have increased over the last several years and are expected to increase further. The NISP is the governmentwide program to assure federal agencies that contractors adequately protect classified information. The NISP was established by executive order in 1993[4] to replace industrial security programs operated by various federal agencies. Under the national program, contractor facilities must be cleared prior to accessing classified information and must implement certain safeguards to maintain their clearance. DOD is responsible for clearing facilities and monitoring contractors' protection of classified information.[5] DOD, with concurrence from the Department of Energy, Nuclear Regulatory Commission, and Central Intelligence Agency, issued the National Industrial Security Program Operating Manual (NISPOM) in 1995.[6] The NISPOM prescribes the requirements, restrictions, and safeguards that contractors are to follow to prevent the unauthorized disclosure—or compromise—of classified information.

DSS administers the NISP on behalf of DOD and 24 other agencies through its Industrial Security Program.[7] DSS's Industrial Security Program, which

[4]Executive Order no. 12829, signed January 6, 1993, established the NISP for the protection of information classified under Executive Order no. 12958, as amended.

[5]Under Executive Order no. 12829, the Director of Central 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 DOD.

[6]The NISPOM (DOD 5220.22-M) was subsequently amended in 1997 and 2000.

[7]DOD has entered into agreements with the following 24 departments and agencies for the purpose of providing industrial security services: the Departments of Agriculture, Commerce, Education, Health and Human Services; Homeland Security, the Interior, Justice, Labor, State, Transportation, and the Treasury; Environmental Protection Agency; Federal Reserve System; General Accounting Office; General Services Administration; National Aeronautics and Space Administration; Nuclear Regulatory Commission; Small Business Administration; U.S. Agency for International Development; National Science Foundation; U.S. Arms Control and Disarmament Agency; U.S. Information Agency; U.S. International Trade Commission; and U.S. Trade Representative.

is one of DSS's three core mission areas,[8] oversees more than 11,000 contractor facilities to assure U.S. government customers that their classified information is protected. By clearing a facility, DSS has determined that the contractor facility is eligible to access classified information at the same or lower classification level as the clearance granted—Confidential, Secret, or Top Secret. Under the NISP, a facility is a grouping of buildings related by function and location that form an operating entity. Facilities include manufacturing plants, laboratories, offices, and universities. They range in size from small offices that are owned and operated by one person to huge manufacturing complexes that are one of many owned by a large corporation. According to DSS, about half of the cleared facilities have been approved by DSS to store classified information on site, while the other facilities access classified information at a government site or at another facility approved for storage.

DSS's industrial security representatives serve as the primary points of contact with cleared facilities and are responsible for ensuring that contractors have security programs that comply with the NISPOM. The 240 industrial security representatives are assigned to 23 field offices spread throughout the country, where field office chiefs supervise their work. Representatives' oversight involves educating facility personnel on security requirements, accrediting information systems that process classified information, approving classified storage containers, and assisting contractors with security violation investigations. DSS representatives also conduct periodic security reviews to assess whether contractor facilities are adhering to NISPOM requirements and to identify actual and potential security vulnerabilities. Security reviews are scheduled annually for facilities that store classified information and every 18 months for facilities that do not have classified information on site. In overseeing and assisting contractors, the representatives are to follow the procedures contained in the Industrial Security Operating Manual, which DSS issued to guide its personnel in administering the NISP. For example, the manual specifies how representatives should conduct security reviews to evaluate the quality of a facility's security program and how contractor facilities' reports of security violations should be handled.

[8]DSS's other core mission areas are the Personnel Security Investigations Program and the Security Education, Training, and Awareness Program. However, the Personnel Security Investigations Program will be transferred to the Office of Personnel Management under the authority provided in the National Defense Authorization Act for Fiscal Year 2004 (Pub. L. No. 108-136, § 906).

DSS Does Not Evaluate the Effectiveness of Its Oversight

DSS relies on performance goals and measures that do not provide it a basis for assuring government customers that its oversight of contractor facilities mitigates the risk of information compromise. Instead of focusing on the overall results of its oversight and the protection of classified information, DSS evaluates its performance in terms of indicators, such as the number of security reviews completed on time. Further, while industrial security representatives maintain paper files on the quality of contractor security programs and the types of security violations that result in compromises of classified information, DSS does not analyze this information, and the manner in which it is maintained does not lend itself to such analysis. Without this analysis, DSS is limited in its ability to detect trends in the protection of classified information across facilities, to determine sources of security vulnerabilities, and to identify those facilities with the greatest risk of compromise.

DSS's Performance Goals and Measures Do Not Indicate If Mission Is Being Achieved

Although DSS has reported that it has met or exceeded many of its performance goals, DSS has no basis for determining whether it is fulfilling its overall industrial security mission. DSS's industrial security mission, as stated in its current Fiscal Year 2000-2005 strategic plan, is to (1) ensure that all contractor facilities overseen by DSS properly protect classified information in their possession and (2) assure government customers that facilities are eligible to receive classified information and have systems in place to protect the classified information. However, DSS currently does not have performance goals and measures that would indicate whether DSS is fulfilling this mission.

DSS assesses its industrial security program based on the:

- percentage of security reviews completed,
- percentage of security reviews that covered all pertinent areas of contractors' security programs,
- length of time needed to clear contractor facilities for access to classified information, and
- length of time needed to clear contractor personnel for access to classified information.[9]

[9]DSS will only process an application for a personnel clearance if the facility at which the employee works has been cleared.

Such indicators are important. For example, according to DSS officials, the indicator pertaining to the completion of security reviews provides government customers assurances that industrial security representatives are monitoring their contractors. The timeliness of clearances also matters because the facility and its personnel cannot access classified information in support of a government contract until DSS has cleared them. For each of the indicators, DSS established specific performance goals. While DSS did not meet all of its goals related to the timeliness of contractor facility and personnel clearances, it met or exceeded the goals related to security reviews. For example, DSS's goal is to conduct annual security reviews of 98 percent of the facilities that store classified information on site. In fiscal year 2002, the most recent year for which data are available, DSS reported meeting this goal.

DSS also reported that it exceeded the goal of having 75 percent of its security reviews cover all pertinent areas within contractor facilities' security programs. Based on a review of selected security review reports, DSS determined that 86 percent of its security reviews conducted in fiscal year 2002 covered all pertinent areas and accurately reflected the contractor facilities' overall security posture. However, DSS measured its achievement of this goal based on field office chiefs' selection and review of about 550 of the approximately 9,000 reports completed by industrial security representatives. This review does not focus on the quality of the facilities' security programs or the representatives' review of those programs. Instead, it is used to determine the completeness of the reports.

These current goals and measures alone do not enable DSS to determine whether its oversight is effectively ensuring that contractors protect classified information. There are no goals related to how well facilities are protecting classified information, which would provide an indication as to whether DSS is achieving its mission. For example, while DSS evaluates the completeness of security review reports submitted by industrial security representatives, it does not evaluate its performance in terms of the ratings[10] and number of findings[11] that result from security reviews. Nor

[10]After a security review, an industrial security representative is to rate that facility's security program in terms of how well it meets NISPOM requirements and ensures the protection of classified information. There are currently four rating categories—ranging from unable to safeguard classified information to exceeding the basic requirements of the NISPOM.

[11]DSS defines a finding as the failure to comply with the NISPOM. Findings are either administrative or serious. Findings are deemed serious if they could lead to the loss or compromise of classified information.

does DSS evaluate its performance in terms of the frequency of security violations and information compromises occurring at contractor facilities. By not assessing its performance based on factors such as facility compliance with NISPOM requirements, DSS cannot determine whether its oversight efforts are contributing to an increase or decrease in facilities' compliance and the protection of classified information.

DSS's Lack of Analysis Limits Its Ability to Determine If Its Oversight Reduces the Risk of Information Compromise

DSS maintains records on how well contractor facilities protect classified information but does not analyze these records. There are no programwide analyses of violations reported by facilities or results of DSS's reviews of facilities. Further, the manner in which DSS maintains records on facilities' security programs—geographically dispersed paper-based files—does not lend itself to analysis. Industrial security representatives maintain a file folder on each facility they oversee. According to DSS officials, the information contained in these file folders represents the official record on each contractor facility. The folders are the primary means for documenting information on facilities' security programs and representatives' interactions with those facilities. The folders contain, in paper copy form, information such as the facility's clearance level, identity of the facility owner, results of the last two security reviews, and facility's reports on security violations.[12] Folders are kept with their respective industrial security representatives throughout the country.

An analysis of the types of security violations reported by facilities, their causes, or corrective actions taken would require a manual review of each file folder. According to DSS officials, DSS has not conducted such an analysis in recent years nor has it made any other attempt to identify the most common violations of the NISPOM or their causes. As a result, DSS does not know whether certain types of violations are increasing or

[12]In addition to the file folders, DSS has a Facilities Database that contains information on facilities' security programs. However, industrial security representatives are not required to document all oversight activities in the database nor has DSS assessed the database's reliability. The database is primarily used to assign facilities to representatives and track the number of security reviews completed. DSS also analyzes information on attempts to collect information from U.S. industry to determine the threat posed by foreign agents. Information on these attempts, such as the types of information sought, methods used to attempt access, and countries targeting the information, is entered into a database maintained by DSS's Counterintelligence Office. The office uses this database to identify trends in foreign information collection efforts, which are reported in the annual "Technology Collection Trends in the U.S. Defense Industry" report and disseminated to industrial security representatives and contractor facility security officials.

decreasing or why such changes may be occurring. For example, DSS officials told us that anecdotal evidence indicates that there are an increasing number of security violations involving unsecured e-mail transmission of classified information. However, DSS has no basis for knowing what percentage of facilities have had such violations or how significant any increase has been.

By not analyzing the information contained in the file folders, DSS is unable to identify patterns of security violations across all facilities based on factors such as the type of work conducted at the facility, the facility's government customer, or the facility's corporate affiliation. Officials at several contractor facilities informed us that their security procedures are developed and managed at the corporate level and, therefore, all facilities owned by the corporation follow the same procedures. As a result, security problems at one facility may indicate a more general, corporatewide vulnerability. For example, an industrial security representative attributed a series of violations at a facility owned by a large corporation to that facility's inadequate security education program. However, facility security officials told us that their education program was developed at the corporate level, rather than by that facility. Because DSS does not track violations and their causes across facilities, there was no way to readily determine whether use of the corporate security education program resulted in violations at other facilities.

DSS recently created a new database to track the number of security violations reported by facilities.[13] Industrial security representatives are required to enter into the database which facility reported the violation, which field office is responsible for the facility, and the industrial security representative's determination regarding whether information was compromised. According to DSS officials, DSS will use the new database to calculate the number of security violations nationwide and by region and to track the amount of time representatives take to make a determination after receiving facilities' violation reports. However, because of the limited data it will contain, the database cannot be used to identify common types and causes of security violations reported by facilities.

[13]This Web-based database, which is known as the Industrial Security Reporting System, became operational in July 2003.

DSS also does not analyze information on the quality of facility security programs, such as ratings and the number and types of findings from DSS's security reviews. While DSS officials expressed interest in eventually analyzing security review ratings and findings, they told us the new database currently lacks this capability. DSS has not manually reviewed the file folders and analyzed security review ratings to determine, for example, whether the number of facilities meeting NISPOM requirements is increasing or if security programs for facilities owned by one corporation have consistently lower ratings than those owned by another corporation. DSS also has not analyzed the security review findings to identify the number and most common types of findings. As a result, DSS cannot identify patterns of security review findings across all cleared facilities on the basis of the type of work they perform, their size, or corporate ownership.

DSS Does Not Always Comply with NISP Requirements after a Possible Compromise of Information

Industrial security representatives often failed to determine whether security violations by facilities resulted in the loss, compromise, or suspected compromise of classified information or made determinations that were not in accordance with approved criteria. Such determinations are important because if classified information is lost, compromised, or suspected of being compromised, the affected government customer must be notified so it can evaluate the extent of damage to national security and take steps to mitigate that damage. Even when representatives made an appropriate determination, they often took several weeks and even months to notify the government customer because of difficulties in identifying the customer. As a result, the customer's opportunity to take necessary corrective action was delayed.

Industrial Security Representatives Failed to Make Appropriate Determinations for Many Reported Security Violations

The NISPOM requires a facility to investigate all security violations. If classified information is suspected of being compromised or lost, the facility must provide its DSS industrial security representative with information on the circumstances of the incident and corrective actions taken to prevent future occurrences. The industrial security representative is to then review this information and, using the criteria specified in DSS's Industrial Security Operating Manual, make one of four final determinations: no compromise, suspected compromise, compromise, or loss. Table 1 outlines the criteria for each determination.

Table 1: Criteria for DSS's Compromise Determinations

No compromise	This conclusion is reserved for inquiries in which classified information may have been vulnerable to compromise but the circumstances of the situation led the industrial security representative to reasonably conclude that either no unauthorized individual had access to the information, or that, based on the facts of the inquiry, the possibility of access was extremely remote.
Suspected compromise	To reach this conclusion, the industrial security representative must be able to identify the classified information involved and, usually, the unauthorized individual(s) who may have gained access to the information. In this case, proving that there was unauthorized access to the information may not be possible, but the facts in the case lead the industrial security representative to reasonably conclude that unauthorized access probably occurred. For example, the storage of classified information in an unlocked desk drawer of an unlocked office or open space for several months in a facility where an unauthorized person had or was likely to have had access should be considered a suspected compromise.
Compromise	An unauthorized disclosure of classified information. To reach the conclusion that material was compromised, the industrial security representative must be able to identify the classified information involved and the unauthorized individual(s) to whom the information was disclosed.
Loss	Classified information is presumed lost if the material cannot be located within a reasonable time or if the material is out of the custodian's control, including transmission of the information by an unsecured communication method to which an unauthorized person reasonably could have had access (e.g., Internet, telephone, unsecured facsimile).

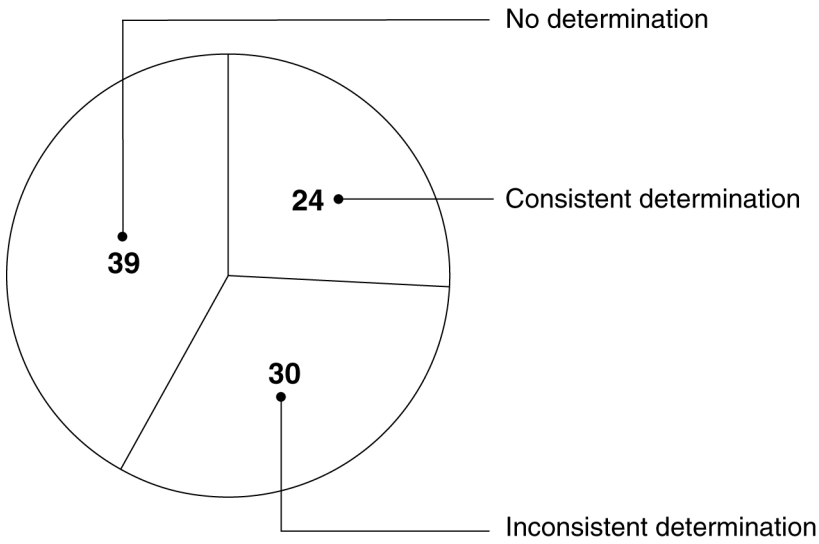
Source: Industrial Security Operating Manual.

If a determination other than no compromise is made, the Industrial Security Operating Manual directs the representative to inform the government customer about the violation so a damage assessment can be conducted. However, as shown in figure 1, for 39 of the 93 security violations that we reviewed, industrial security representatives made no determinations regarding the compromise or loss of classified information.[14] For example, in two cases where the same facility reported the improper transmission of classified information via e-mail, DSS made no determinations even though the facility reported the possibility of compromise in both cases. In eight cases at another facility, employees

[14]Of the 39 violations, 7 were reported to DSS in 2001, 13 in 2002, and 19 in 2003. The 2003 violations were reported to DSS at least 2 months prior to our review of how DSS responded to these violations.

repeatedly failed to secure a safe room to ensure the protection of classified information. DSS made no determinations in any of the eight cases. In the absence of a determination, the industrial security representatives did not notify the government customers of these violations. The government customers, unaware of the violations, could not take steps to assess and mitigate any damage that may have resulted.

Figure 1: DSS's Determinations for 93 Reported Violations



Source: DSS's facility file folders (data); GAO (analysis).

Note: Of the 24 cases where DSS made consistent determinations, it determined no compromise in 10 cases, loss of information in 9 cases, compromise of information in 3 cases, and suspected compromise in 2 cases.

For 54 of the 93 violations we reviewed, representatives made determinations regarding the compromise or loss of information, but the majority were not consistent with the criteria contained in DSS's Industrial Security Operating Manual. As figure 1 further illustrates, representatives made 24 determinations regarding compromise or loss that were consistent with the criteria contained in the manual. However, representatives made 30 inappropriate determinations, such as "compromise cannot be precluded" or "compromise cannot be determined." Neither of these is consistent with the determinations in the manual—no compromise, suspected compromise, compromise, or loss. For example, in nine cases, the same facility reported that classified material was left unsecured, and the facility did not rule out compromise. In each of these cases, the industrial security representative did not rule

out compromise but used an alternative determination. Senior DSS officials informed us that industrial security representatives should not make determinations other than the four established in the Industrial Security Operating Manual because the four have specific meanings based on accepted criteria. By not following the manual, representatives have introduced variability in their determinations and, therefore, their decisions of whether to notify the government customer of a violation.

Among the 30 reported violations for which inappropriate determinations were made, industrial security representatives notified the affected government customers in 5 cases so the customers could assess and mitigate any resulting damage. These cases included three violations involving classified material that was left unsecured at the same facility. For the remaining 25 reported violations, the customers were not made aware of the violations even when the violations were similar to those reported to other customers.

The failure of representatives to always make determinations consistent with the Industrial Security Operating Manual is at least partially attributable to inadequate oversight. The Standards and Quality Branch is the unit within DSS responsible for ensuring that industrial security representatives properly administer the NISP. Branch officials regularly test and review field office chiefs and representatives on NISP requirements, particularly those related to granting clearances and conducting security reviews. According to DSS officials, the results of these tests and reviews are used to design training courses that address weaknesses in job skills. However, the Standards and Quality Branch does not test or review how representatives respond to reported violations and make determinations regarding compromise. As a result, DSS does not know the extent to which representatives understand and are consistently applying Industrial Security Operating Manual requirements related to violations and, therefore, cannot make necessary revisions to training and guidance.

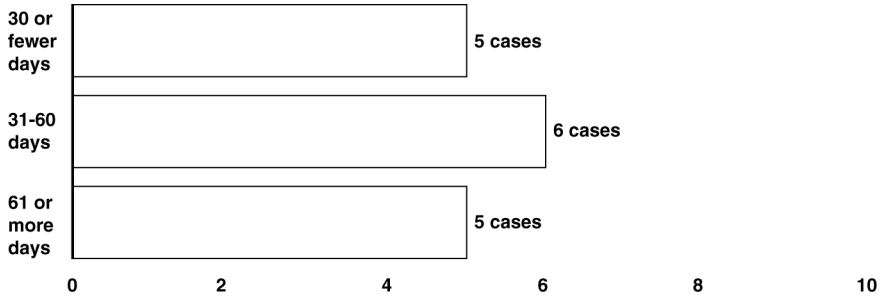
In addition, field office chiefs are responsible for supervising and ensuring the quality of industrial security representatives' day-to-day oversight of contractors. However, there is no specific requirement in the Industrial Security Operating Manual for field office chiefs to review their industrial security representatives' determinations regarding reported security violations. We found no evidence that chiefs reviewed the cases in which the representatives either did not make determinations or made determinations that were inconsistent with the manual. Further, chiefs may not fully understand the manual's criteria for determinations. For

example, one field office chief we met with tracked the industrial security representatives' processing of reported security violations by using a categorization sheet containing the inappropriate determination "compromise not precluded."

DSS Is Not Always Able to Quickly Notify Government Customers about Violations

While the Industrial Security Operating Manual does not specify a time requirement for notifying government customers when classified information has been lost or compromised, DSS is frequently unable to notify customers quickly because of difficulties in identifying the affected customers. DSS notified government customers regarding 16 of the 54 reported violations for which representatives made determinations. Figure 2 shows that for 11 of these 16 violations, DSS did not notify the customer for more than 30 days after the contractor reported that information was lost, compromised, or suspected of being compromised. In one case, 5 months passed before an industrial security representative was able to notify a government customer that its information was suspected of being compromised. This delay was a result of the facility's inability to readily determine which government customer was affected by the compromise.

Figure 2: Amount of Time DSS Took to Notify Government Customers of Compromise Determinations in 16 Cases



Source: DSS's facility file folders (data); GAO (analysis).

When a loss, compromise, or suspected compromise has been determined, the industrial security representative generally relies on the facility to identify the affected government customer. However, when the facility is operating as a subcontractor, it may not be aware of the government customer's identity. In such instances, the subcontractor may have to work with the prime contractor to identify the government customer to provide the industrial security representative with this information. In one case we reviewed, a subcontractor made repeated attempts over a 5-

month period to obtain the affected government customer's identity from the prime contractor. In another case, an official with a subcontractor facility informed us that it was extremely difficult and time-consuming for him to identify the affected government customer, which took approximately 2 months. Such delays limit the government customer's opportunity to assess the extent of potential damage to national security.

Representatives Often Do Not Notify Facilities of Their Determinations Even Though It May Be Useful to Do So

While the Industrial Security Operating Manual requires industrial security representatives to notify government customers of loss or compromise determinations, there is no requirement for representatives to inform facilities of their final determinations. However, senior DSS officials told us that they expect representatives to provide facilities with their final determinations. They explained that this helps facility officials understand what constitutes loss, compromise, or suspected compromise. Contractor security officials at one facility confirmed this by telling us that receiving determinations enables them to better understand which violations must be reported to DSS. Yet, industrial security representatives provided facilities with determinations for only 34 of the 93 reported violations we reviewed, and 18 of the 34 were inappropriate determinations. As a result of both inappropriate determinations and determinations not being provided by DSS, facility officials may misunderstand what constitutes a violation that must be reported to DSS and whether they have taken appropriate actions to contain any possible compromise and prevent future incidents.

Conclusions

By granting contractors access to classified information, the government has entrusted them with protecting national security. Ensuring that contractors safeguard classified information is DSS's mission, yet DSS cannot provide adequate assurances that it is fulfilling this mission. Through its oversight, DSS cannot prevent every incident of information compromise, but unless DSS knows whether its oversight minimizes the risk of information compromise, it does not have an informed basis for managing its oversight. By not evaluating the information it maintains on how well contractors protect classified information, DSS may not realize where the risks and systemic vulnerabilities exist. Further, DSS has no basis for adjusting its resources to address emerging security weaknesses, such as the electronic transmission of classified information. Although DSS's inability to assess its performance as well as evaluate and make changes to its oversight does not necessarily mean that contractors are not fulfilling their responsibilities under the NISP, the effectiveness of DSS's oversight is diminished and the assurances it provides to government

customers regarding the protection of their information cannot be relied on.

Likewise, by not making appropriate determinations regarding compromise or loss, DSS does not always notify government customers that their information has been lost or compromised, thereby, limiting corrective actions and possibly increasing the damage to national security. Inappropriate determinations may also confuse contractors' understanding of the reporting requirements and result in contractors not reporting incidents that should be reported.

Recommendations for Executive Action

To enable DSS to evaluate whether its oversight reduces the risk of information compromise, we recommend that the Secretary of Defense direct the Director, Defense Security Service, to take the following three actions:

- establish results-oriented performance goals and measures that would enable DSS to assess the extent to which it is achieving its industrial security mission,
- identify the information that needs to be analyzed to detect systemic vulnerabilities and identify trends regarding how contractor facilities protect classified information, and
- regularly analyze that 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.

In carrying out these actions, DSS will need to evaluate alternatives for creating a new system or further developing an existing system to record and analyze standard information on how well contractors protect classified information.

We also recommend that the Secretary of Defense direct the Director of DSS to take the following four actions to ensure that appropriate determinations are made regarding possible information compromises and that government customers are notified of such situations in a timely manner:

- evaluate industrial security representatives and field office chiefs' understanding of the criteria for making determinations regarding the compromise of classified information and revise training and guidance for representatives and chiefs based on the results of that evaluation,

- revise Industrial Security Operating Manual requirements to emphasize the need to apply the established determinations regarding the compromise or loss of classified information,
- explore the effects of establishing specific time-based criteria in the Industrial Security Operating Manual for representatives to make determinations and notify government customers, and
- 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. This could be accomplished by requiring representatives to maintain such information in their file folders or ensuring that contractors, particularly when they are subcontractors, know the identity of their government customers before an incident resulting in compromise or loss occurs.

Additionally, to improve contractors' understanding of which security violations must be reported to DSS, we recommend that the Secretary of Defense direct the Director of DSS to 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.

Agency Comments and Our Evaluation

In written comments on a draft of this report, DOD concurred with our recommendations. However, DOD stated that the report's conclusion—that DSS cannot provide adequate assurances that its oversight ensures the protection of classified information by contractors—is not supported because we did not evaluate how well contractors protect classified information. While agreeing that its performance measures are not results-oriented, DOD stated that DSS is able to provide assurances regarding the protection of classified information through its security reviews. For 99 percent of security reviews, according to DOD, contractors were found to be satisfactorily protecting classified information. Additionally, DOD indicated that the problems we identified with security violations and possible information compromises were purely administrative. DOD stated it assumes that DSS's current processes for handling security violations and possible information compromises did not leave classified information at risk.

While contractors are ultimately responsible for protecting the classified information entrusted to them, DSS is charged with ensuring that contractors fulfill this obligation. Our review focused on how effectively DSS's oversight ensures that contractors protect classified information. As

explained in our report, DSS does not assess the effectiveness of its oversight based on how well contractors are protecting information from compromise nor does it analyze data to identify systemic vulnerabilities in contractors' protection of classified information. Therefore, DSS cannot provide adequate assurances that its oversight ensures the protection of classified information. DSS is also hindered in its ability to identify and implement corrective changes to reduce the risk of information compromises resulting from security violations. In its comments, DOD stated that DSS does not have the ability to identify and analyze trends regarding how contractors protect classified information because it lacks the information technology infrastructure to conduct such analyses.

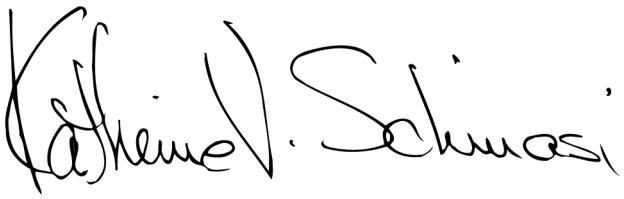
We are uncertain of the basis for DOD's statement that 99 percent of the facilities received satisfactory security review ratings because DSS officials told us during the course of our review that they do not track the facilities' ratings. Also, by focusing only on security review ratings, DOD is overlooking other indicators—such as security review findings and incidents of possible compromise—that could enable DSS to improve its oversight. Further, the rating may not be an adequate measure of effectiveness. First, an industrial security representative can rate a facility's security program as satisfactory even if the facility does not fully comply with the NISPOM and its failure to do so could logically lead to information compromise. Second, because DSS does not track information on security review ratings and violations, it cannot establish whether there is a correlation between a facility's rating and the frequency and seriousness of that facility's violations and information compromises. Finally, as we noted in our report, DSS's security review quality metric is based not on the quality of reviews, but rather on the completeness of industrial security representatives' reports. Also, the manner in which field office chiefs select reports for the quality review is not statistically valid and, therefore, DSS cannot draw conclusions about the quality of security review reports nationwide based on that quality review.

The problems we identified with DSS's response to security violations and possible information compromises go beyond administrative processing. Our findings focus on whether DSS has fulfilled its oversight responsibilities. As DOD noted in its comments, DSS is responsible for determining whether a violation has resulted in compromise, ensuring that the contractor took corrective action, and notifying the government customer. Yet, as discussed in our report, industrial security representatives failed, in 39 of the 93 security violations we reviewed, to determine whether the violations resulted in the loss, compromise, or suspected compromise of classified information. For an additional 30

violations, representatives made inappropriate determinations, which created variability in their decisions on whether to notify the government customer of a violation. Absent a determination consistent with the Industrial Security Operating Manual, one cannot draw conclusions on whether the contractor conducted an adequate inquiry into the violation and took corrective action to prevent its recurrence. Therefore, we cannot agree with DOD's assumption that weaknesses in DSS's handling of security violations did not leave classified material at risk. DOD's comments are reprinted in appendix II, along with our evaluation of them.

We are also sending copies of this report to interested congressional committees; the Secretary of Defense; the Director, Defense Security Service; the Assistant to the President for National Security Affairs; and the Director, Office of Management and Budget. We will make copies available to others upon request. In addition, this report will be available at no charge on the GAO Web site at http://www.gao.gov.

If you or your staff have any questions regarding this report, please contact me at (202) 512-4841. Key contributors to this report are listed in appendix III.



Katherine V. Schinasi
Managing Director
Acquisition and Sourcing Management

Appendix I: Scope and Methodology

To assess the Defense Security Service's (DSS) oversight of contractors' implementation of the National Industrial Security Program (NISP), we reviewed Department of Defense (DOD) regulations and guidance on industrial security, including the National Industrial Security Program Operating Manual, as well as DSS policies, procedures, and guidance for overseeing contractor facilities. We also assessed DSS's performance goals and measures contained in its strategic plan and annual report against our reports related to the Government Performance and Results Act[1] and internal controls.[2] We discussed the development of DSS goals, objectives, and performance metrics with DSS officials. To become more familiar with the roles and responsibilities of DSS staff, particularly as they relate to maintaining information on facility security programs, we reviewed DSS's training materials, the Industrial Security Operating Manual, and selected facility file folders. We also discussed with DSS officials at headquarters and field locations how they use the information in the facility file folders to manage the industrial security program and oversee contractor facilities.

To assess adherence to required procedures by DSS after a security violation and possible compromise of classified information, we used a case study approach. Using DSS's Facilities Database, we selected cases from all facilities participating in the NISP as of March 2003. We reviewed the data and identified facilities that reported to DSS security violations since January 1, 2001, and selected 13 cleared facilities that varied according to size, clearance level, and geographic location. For those 13 facilities, we reviewed DSS's official facility file folders and identified 93 reported violations. For those violations, we examined DSS's actions to determine whether industrial security representatives and field office chiefs handled these reports in accordance with the Industrial Security Operating Manual. We also spoke with representatives and chiefs regarding the actions they take after receiving violation reports. We analyzed the information in DSS's files on the 13 facilities and their violations to identify the determinations made by industrial security representatives, how frequently government customers were contacted, and the timeliness of government customer notification. In addition, we visited the facilities selected for our case study and interviewed those

[1]See U.S. General Accounting Office, *The Results Act: An Evaluator's Guide to Assessing Agency Annual Performance Plans*, GAO/GGD-10.1.20 (Washington, D.C.: Apr. 1, 1998).

[2]See U.S. General Accounting Office, *Standards for Internal Control in the Federal Government*, GAO/AIMD-00-21.3.1 (Washington, D.C.: Nov. 1, 1999).

facilities' security officials to obtain clarification and additional information about the reported security violations and actions taken by DSS. Because we did not take a statistical sample of facilities, the results from our analyses cannot be generalized. We also did not assess the reliability of the Facilities Database as a whole. However, we confirmed that the data used to select the 13 cases, specifically the facility size and clearance level, were consistent with the information in the facility files we reviewed.

We performed our review from March 2003 through January 2004 in accordance with generally accepted government auditing standards.

Appendix II: Comments from the Department of Defense

Note: GAO's comments supplementing those in the report's text appear at the end of this appendix.

INTELLIGENCE

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

FEB 1 2 2004

Ms. Katherine V. Schinasi, Director
Acquisition and Sourcing Management
U. S. General Accounting Office
441 G. Street, N. W.,
Washington, DC 20548

Dear Ms. Schinasi:

This is the Department of Defense (DoD) response to the GAO draft report, "INDUSTRIAL SECURITY: DOD Cannot Provide Adequate Assurances That Its Oversight Ensures the Protection of Classified Information," dated January 15, 2004, (GAO Code 120212/GAO-04-332)."

The National Defense Authorization Act for fiscal year 2004 directed GAO to review the National Industrial Security Program (NISP) and DoD's oversight of contractors' programs to protect sensitive information and technology. According to the report, the GAO review team assessed (1) DSS oversight of contractor facilities implementation of the NISP and (2) DSS adherence to required procedures after a security violation and possible compromise of classified information.

See comment 1.

Thank you for reaffirming in your recommendations the direction DSS is taking with respect to the protection of classified information. However, while I have concurred with all specific recommendations in the draft report, it appears that your team does not understand DSS' oversight role or how they perform their oversight mission. Contractors, not DSS, are responsible for the protection of classified information in industry. The draft report ignores the work performed by the approximately 11,500 industry Facility Security Officers who work to protect national security information on a daily basis.

In conducting this assessment, the GAO team concluded that DSS measured the success of its oversight role solely by the metrics in its performance contract with the Office of the Secretary of Defense. We acknowledge that those are not results-oriented measures. DSS has already begun the process of developing a strategic plan and balanced scorecard to replace them.

It is the security review process that is used to evaluate the protection of classified information. Assurance is conveyed to the government contracting activity (GCA) through verification of the contractor's facility clearance and safeguarding capability.

See comment 2.

Also, DSS conducts recurring security reviews encompassing all aspects of the contractor's classified industrial security operations (i.e., personnel, physical, information assurance, etc.). DSS consistently meets its current performance metric of conducting 98% of security reviews within required timeframes and exceeds its quality standards. Nothing in the draft report questioned the methodology used by DSS in conducting these security reviews or in evaluating the quality of the reviews. In fact, 99% of the cleared contractors were awarded satisfactory ratings. Any contractor assigned less than a satisfactory rating receives compliance security inspections until all issues have been resolved. Further, when a contractor is assigned an unsatisfactory rating, the GCA is notified of the rating and the circumstances on which that rating was based.

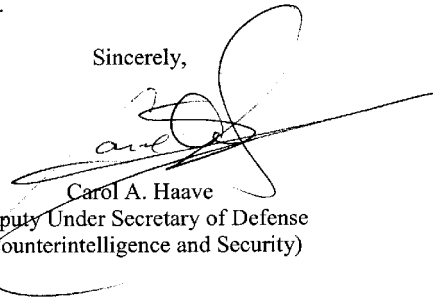
See comment 3.

The report and recommendations indicate that the GAO team placed significant emphasis on administrative processing of ***contractor- reported*** security violations at selected field locations. They reviewed the administrative handling of those reports based on the DSS internal operating manual. It is important to note that by the time a security violation has been reported to DSS, the contractor has already accomplished an inquiry and corrective action has been taken. DSS' responsibility is to ensure that an adequate inquiry was conducted; corrective action was taken to preclude a recurrence, determine whether there has been a compromise and notify the GCA. As the GAO team did not note any concerns with corrective action and the recommendations focus on the administrative process used by DSS to handle security violations, it is our assumption that the process currently used by DSS did not leave classified material at risk. It is noted that the draft report expresses a concern that the sampling of data used in the GAO review of facility file folders was not statistically valid and, therefore, the analysis of data could not be generalized. However, many of GAO's conclusions in the draft report were based on this same data.

See comment 4.

As the title and primary conclusion of the draft report are not supported by the conduct of the review, the draft report is a disservice to personnel in industry and government who oversee the protection of classified information and is misleading to Congress. When your review began I had high hopes that you would provide value to our ongoing transformation efforts at DSS and also acknowledge the many positive initiatives currently underway.

Sincerely,



Carol A. Haave
Deputy Under Secretary of Defense
(Counterintelligence and Security)

GAO DRAFT REPORT – DATED JANUARY 15, 2004
GAO CODE 12012/GAO-04-332

"INDUSTRIAL SECURITY: DOD CANNOT PROVIDE ADEQUATE ASSURANCES THAT ITS OVERSIGHT ENSURES THE PROTECTION OF CLASSIFIED INFORMATION"

DEPARTMENT OF DEFENSE COMMENTS TO THE RECOMMENDATIONS

RECOMMENDATION 1: The GAO recommended that the Secretary of Defense direct the Director, Defense Security Service (DSS) to establish results-oriented performance goals and measures that would enable DSS to assess the extent to which it is achieving its industrial security mission.

DOD RESPONSE:

See comment 5.

Concur that the performance metrics currently contained in the DSS Defense Review Board Performance Contract are not results-oriented measures. Fortunately, DSS does not rely solely on those measures to determine success in accomplishing its mission. In order to improve upon its efforts to measure performance, DSS has initiatives underway to develop a strategic plan and balanced scorecard to measure results achieved through the goals contained in the strategic plan. This effort is expected to be completed by the end of 2004.

RECOMMENDATION 2: The GAO recommended that the Secretary of Defense direct the Director, DSS to identify the information that needs to be analyzed to detect systemic vulnerabilities and identify trends regarding how contractor facilities protect classified information.

DOD RESPONSE:

Concur. DSS currently lacks the information technology infrastructure to conduct this type of analysis. DSS is in the process of developing requirements for a new automated information management system to support the Industrial Security Program that will facilitate the ability to identify and analyze trends regarding how contractors protect classified information. The requirements phase is expected to be completed within the next 6 months.

RECOMMENDATION 3: The GAO recommended that the Secretary of Defense direct the Director, DSS to regularly analyze the systemic vulnerability and trend 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.

DOD RESPONSE:

Concur. The recommended trend analysis will be facilitated by the information management system described in Recommendation 2, above.

RECOMMENDATION 4: The GAO recommended that the Secretary of Defense direct the Director, DSS to evaluate the industrial security representatives and field office chiefs' understanding of the criteria for making determinations regarding the compromise of classified information and revise training and guidance for representatives and chiefs based on the results of that evaluation.

DOD RESPONSE:

Concur. DSS will make the review of the process used by field personnel to review and process security violations an area of interest during management assistance visits as they occur. These visits to the various field elements allow DSS management the opportunity to discuss areas of concern with the field staff, ensure that consistent processes and procedures are in place, and conduct informal training sessions as needed.

RECOMMENDATION 5: The GAO recommended that the Secretary of Defense direct the Director, DSS to revise Industrial Security Operating Manual requirements to emphasize the need to apply the established determinations regarding the compromise or loss of classified information.

DOD RESPONSE:

Concur. DSS will review the guidance currently contained in the ISOM and will make changes or clarifications as appropriate. Necessary updates and changes to the ISOM will be completed by the end of 2004.

RECOMMENDATION 6: The GAO recommended that the Secretary of Defense direct the Director, DSS to explore the effects of establishing specific time-based criteria in the Industrial Security Operating Manual for representatives to make determination and notify government customers.

DOD RESPONSE:

Concur. As the ISOM is reviewed for updates and changes, in accordance with the response to Recommendation 5 above, such time-based criteria will be considered.

RECOMMENDATION 7: The GAO recommended that the Secretary of Defense direct the Director, DSS to establish mechanisms that create accountability for knowing the identify of government customers so that industrial security representatives can readily notify those customers of any loss or compromise.

DOD RESPONSE:

See comment 6.

Concur. Although the DD Form 254 already requires that the prime contract number be entered for each contract, it appears that in at least 1 instance that did not occur. As part of the new automated information management system, the prime contract number will be a mandatory data element for all tiers of contracts.

RECOMMENDATION 8: The GAO recommended that the Secretary of Defense direct the Director, DSS to revise the Industrial Security Operating Manual to require industrial security representatives to inform facilities of the official determination regarding the loss or compromise of classified information.

DOD RESPONSE:

Concur. As the ISOM is reviewed for updates and changes, in accordance with the response to Recommendation 5 above, a requirement for industrial security representatives to inform facilities of the official determination regarding the loss or compromise of classified information will be incorporated.

The following are GAO's comments on the Department of Defense's letter dated February 12, 2004.

GAO's Comments

1. Our report recognizes that contractors are responsible for protecting classified information entrusted to them. However, the focus of the report is how well DSS is fulfilling its mission to ensure that contractors are protecting classified information. We clearly state that DSS's inability to assess whether it is fulfilling its mission does not necessarily mean that contractors are not protecting the classified information entrusted to them.

2. We are uncertain of how DOD determined that 99 percent of cleared contractors were awarded satisfactory ratings nor do we know what time period this percentage covers and whether it has varied over time. However, for DSS to effectively manage its oversight, it needs to regularly analyze data and examine trends regarding the protection of classified information over time instead of producing the data to fulfill a one-time information request.

3. The results of our case studies can and do indicate serious weaknesses in how DSS oversees contractor facilities even though they cannot be generalized because, as discussed in appendix I, we did not take a statistical sample.

4. Our report identifies shortcomings in DSS's ability to evaluate whether it is fulfilling its mission, make informed management decisions, and ensure that industrial security representatives properly resolve security violations and possible information compromises. Our report offers specific recommendations for improvement, all of which DOD agreed to implement.

5. It is unclear from DOD's comments what other measures DSS relies on to determine success in accomplishing its mission. Our review assessed the goals and measures established by DSS and found that they do not provide a basis for determining whether DSS is fulfilling its mission.

6. Maintaining the prime contract numbers for all tiers of contracts in a new information management system may not be sufficient to ensure that government customers are readily notified of a loss or compromise. In at least two cases we reviewed, industrial security representatives informed subcontractor facility officials that, in addition to the prime contract number, the name and complete address of the government customer and

a point of contact needed to be provided before DSS could process the violation. In one case, an official at a subcontractor facility informed the representative that such information was not readily available on the DD Form 254, which is designed to provide a contractor with the security requirements and classification guidance needed for the performance of a classified contract.

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

Thomas J. Denomme, 202-512-4841

Acknowledgments

In addition to the individual named above, Johana R. Ayers; Ronald T. Bell, Jr.; Lily J. Chin; Brendan S. Culley; Ian A. Ferguson; Kenneth E. Patton; and Eric E. Petersen made key contributions to this report.

GAO's Mission

The General Accounting 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 the Internet. GAO's Web site (www.gao.gov) contains abstracts and full-text files of current reports and testimony and an expanding archive of older products. The Web site features a search engine to help you locate documents using key words and phrases. You can print these documents in their entirety, including charts and other graphics.

Each day, GAO issues a list of newly released reports, testimony, and correspondence. GAO posts this list, known as "Today's Reports," on its Web site daily. The list contains links to the full-text document files. To have GAO e-mail this list to you every afternoon, go to www.gao.gov and select "Subscribe to e-mail alerts" under the "Order GAO Products" heading.

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. General Accounting Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone:
Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Public Affairs

Jeff Nelligan, Managing Director, NelliganJ@gao.gov (202) 512-4800
U.S. General Accounting Office, 441 G Street NW, Room 7149
Washington, D.C. 20548