United States General Accounting Office

GAO

Report to the Secretary of Defense

August 1986

INFORMATION SECURITY

Need for DOD Inspections of Special Access Contracts

GAO/NSIAD-86-191

GAO

United States
General Accounting Office
Washington, D.C. 20548

National Security and
International Affairs Division
B-223830

August 7, 1986

The Honorable Caspar W. Weinberger
The Secretary of Defense

Dear Mr Secretary:

On July 24, 1986, we testified at a hearing held by the Subcommittee on Oversight and Investigations, House Committee on Energy and Commerce, on the Lockheed Corporation's control of classified documents for a special access program. Our testimony focused on (1) Lockheed's poor document-control system over classified special access documents, (2) the Department of Defense (DOD) program office's ineffective oversight over document control, and (3) the control and oversight provided Lockheed's regularly classified programs. A copy of our testimony is included as appendix I

The document-control problems at Lockheed and the findings and recommendations of the DOD Security Review Commission[1] reinforce our continuing concerns about security assurance in special access, carve-out contracts In a prior report, Further Improvements Needed in Department of Defense Oversight of Special Access (Carve-Out) Contracts (GAO/GGD-83-43, 43[A], Feb. 18, 1983), we recommended that the Defense Investigative Service be made responsible for periodically inspecting special access contracts and verifying the accountability of classified documents.

While DOD did not then agree with our recommendation, DOD's Information Security Program Regulation was subsequently revised to provide that each DOD component, with approved carve-out contracts, conduct security inspections semiannually as prescribed for regularly classified programs being inspected by the Defense Investigative Service

Although the DOD component responsible for the carve-out contract at Lockheed has a permanent on-site security representative at the Lockheed/Burbank plant, that individual was not overseeing the document-accountability system on a continuing basis, partly because of the magnitude of work related to other physical and personnel security matters, and partly because of inexperience in the field of information security We do not know whether the Lockheed case is atypical or symptomatic

[1] Keeping The Nation's Secrets A Report to the Secretary of Defense by the Commission to Review DOD Security Policies and Practices, Nov 19 1985

of the emphasis that DOD components place on document accountability. However, the deterioration of document accountability for the special access contract at Lockheed may not have occurred if the Defense Investigative Service had been permitted to conduct semiannual inspections of the contract, as it does with other contracts at Lockheed.

The situation at Lockheed and the findings of the DOD Security Review Commission illustrate the need for independent oversight of special access contracts. Therefore, we are reiterating our previous recommendation that you make the Defense Investigative Service responsible for periodically inspecting special access contracts and verifying the control of classified documents.

As you know, 31 U.S.C 720 requires the head of a federal agency to submit a written statement on actions taken on our recommendations to the House Committee on Government Operations and the Senate Committee on Governmental Affairs not later than 60 days after the receipt of the report and to the agency's first request for appropriations made more than 60 days after the date of the report.

We are sending copies of this report to the Chairmen, Subcommittee on Oversight and Investigations, House Committee on Energy and Commerce; House and Senate Committees on Appropriations and Armed Services; House Committee on Government Operations; and Senate Committee on Governmental Affairs; and the Director, Office of Management and Budget

Sincerely yours,

Frank C. Conahan
Director

GAO Testimony on Classified Document Control at Lockheed

The following testimony, "Control Over Classified Documents for a Special Access Program at Lockheed Corporation," was given by Martin M Ferber, Associate Director, National Security and International Affairs Division, on July 24, 1986, before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives.

Mr Chairman and Members of the Subcommittee·

We are pleased to be here today to discuss controls over classified documents for a special access program at one of the Lockheed Corporation's California facilities Our review confirmed the existence of serious problems in the procedures and practices used to account for classified documents for the special access program Lockheed management has acknowledged its problems and has instituted or proposed corrective actions. Before we discuss the results of our review, some background on special access programs and contracts might be helpful

Special Access Programs and Contracts

Before August 1965, each military service or DOD component was responsible for security administration over its own contracts with industry To preclude inconsistencies and duplication—especially for contractors doing business with more than one service or component—responsibility for security administration over practically all of DOD's contracts was centralized. Currently, that responsibility is with the Defense Investigative Service, which makes periodic on-site inspections of contractor facilities—in most cases semiannually—to check for compliance with security requirements In 1965, security administration responsibility for certain special access programs, because of their especially sensitive nature and small number, was retained by the military service or component

These "special access programs" can involve almost any facet of DOD's operations where security of the program is a primary consideration. According to DOD's Information Security Program Regulation, a special access program may be created or continued only on a specific showing that

"normal management and safeguarding procedures are not sufficient to limit 'need-to-know' or access, and the number of persons who will need access will be reasonably small and commensurate with the objective of providing extra protection for the information involved "

The existence of some special access programs is acknowledged by DOD Others are not and their very existence is classified. Many special access programs involve contractors and special access contracts

The number of special access contracts, or "carve-out contracts"—as they are sometimes called because they are carved out of the Defense Investigative Service's periodic inspection program—has grown substantially since 1965 In 1983, we estimated that there probably were several thousand such contracts. Although exact information is not available, we believe that the number of special access contracts has continued to increase at a rapid pace

Lockheed Accountability Over Classified Documents

Mr Chairman, your June 11, 1986, letter to the Secretary of Defense identified serious problems with Lockheed's accountability over classified documents associated with a major special access program. Your July 7, 1986, letter to the Comptroller General asked that we (1) verify an internal inventory of accountable classified documents and other data related to the special access program, (2) identify weaknesses in Lockheed's document-control procedures, and (3) assess the nature of the information that may have been contained in documents already reported missing.

In order to respond to your request in the limited time available, we (1) reviewed the control records at Lockheed's Master Document Control Station for the special access program and at 17 of 53 document-control substations, (2) tested the document-control records at 6 substations, and (3) reviewed the company's investigative records and the records of the DOD resident plant-security representative We discussed our findings with company officials, the DOD plant-security representative, and other DOD officials who are responsible for security policy and administration [1] Lockheed and DOD representatives agree with our findings

Verification of Inventory of Accountable Classified Documents

The DOD security guide for the special access program at Lockheed requires a complete inventory of all top secret material at least annually and a random inventory every 60 days of at least 10 percent of all classified material. Lockheed's records show that the company previously

[1] As part of DOD's granting us access to the special access program to respond your request, we agreed not to identify the nature of the program or the specific DOD component or military service involved

had not been doing the required inventories for most of its control substations.

In February 1986, the DOD plant-security representative requested copies of Lockheed inventory reports for the prior 18-month period. The company was unable to provide the reports, and said that it planned to do a 100-percent inventory of all of its classified material within 12 months. That time frame was not acceptable to the DOD representative, and he requested prompt completion of the inventory. Initially, Lockheed was slow in reacting to the request, and assigned fewer than 3 full-time staff to the inventory. At about the same time, your Subcommittee received information from some Lockheed employees concerned about the company's document security, and your Subcommittee became involved in the issue. Subsequently, Lockheed management temporarily assigned about 25 to 30 employees to oversee and complete the inventory and investigate discrepancies.

A physical inventory of classified documents involves at least two stages. The first stage includes visually verifying that the document is where it is supposed to be. The second stage includes investigating and reconciling any discrepancies. An example of a discrepancy is a missing document. That is, control records may show a document charged to a substation, but the document is not there when the physical inventory is taken.

The current inventory of all 53 document control substations has just been completed, and we have not yet had the opportunity to test the inventory accuracy Lockheed has reported 1,460 discrepancies. The large number of discrepancies is not surprising, considering the weaknesses in the system and the fact that the inventory consists of about 40,000 secret and top secret items.

As of July 19, 1986, Lockheed was still investigating 1,225 of the 1,460 discrepancies, and had completed investigation on 235 of them. Lockheed's reported results—which we have not yet had the opportunity to verify—are that 224 documents were later accounted for, and 11 were unresolved "Unresolved" is defined as "all logical leads have been exhausted and the documents remain out of accountability and referred to DOD for resolution " Lockheed says that 7 of the 11 unresolved documents were inadvertently destroyed, and it could not locate the other 4 For the 224 resolved cases, Lockheed lists the following dispositions:

- 111 documents that were later located at document control substations;

- 50 documents that had been removed from accountability by DOD;
- 46 documents that had been destroyed, with destruction receipts reportedly on file; and
- 17 documents that been transferred out of the company

The inventory also identified classified documents that had been received or generated by the company, but had never been made a part of the document-control system.

Weaknesses in Document-Control Procedures

In response to your request that we identify weaknesses in the company's document-control procedures, we evaluated policies, procedures, and practices governing the special access programs and compared them to Lockheed's document controls for classified information in its regular programs that are not special access

There were some major differences in the way document-control systems for the two types of programs were working, although they were basically designed to work the same. The system for the regular programs appeared to be well-managed and working smoothly. Because of time constraints, we made only limited tests of various aspects of the system and found that the various controls appeared to be working and that classified documents were being properly accounted for The Defense Investigative Service has made semiannual security inspections of regular classified document security, and Lockheed security personnel told us that they take extra precautions to make sure that the Service does not have reason to issue a bad report on them.

Unfortunately, the control system for special access program documents—as evidenced by the results of Lockheed's complete inventory and our testing of the system—was not operating as it should The DOD security guide for the special access program requires (1) the company to establish and maintain a document-control system, (2) the company to conduct a random inventory every 60 days of 10 percent of all classified material; and (3) the company to do a complete inventory of all classified material whenever there is a change in the document custodian However, we found that, before the current investigation, Lockheed did not

- have controls to ensure that each substation was inventorying 10 percent of its documents every 60 days,
- make complete inventories of all documents at a document-control station when the document-control officer at the station changed,

- transfer accountability for classified documents when employees transferred to other areas or retired,
- update accountability records when moving classified documents from one controlled area to another, or
- always prepare the documentation needed to establish proper accountability for classified documents received or generated by the company (Some documents were not made a part of the document-control system until discovered during the recently initiated inventory. This provides the opportunity for documents to be missing without any indication that they ever existed)

The DOD security guide also requires that two individuals be involved in the destruction of classified information, and that the destruction be properly documented and recorded in the document-control records. However, Lockheed employees acknowledge destroying classified documents without preparing destruction-request forms, or sometimes with no evidence of a witness to the destruction. We also found that, earlier this year, when employees could not actually recall destroying documents or thought that the documents had been inadvertently destroyed, destruction forms were prepared certifying that material had been destroyed, sometimes 1 or 2 years earlier. Also, we observed several instances where material to be destroyed already had destruction forms filled out. In other words, employees had signed destruction forms, including certifying to witnessing the destruction, even though the classified material had not yet been destroyed.

The DOD security guide further requires the company to investigate discrepancies promptly, report unresolved discrepancies to the DOD program security office, and maintain records of document inspections for review by the DOD program security representative However, we found that Lockheed did not do the following.

- Initiate investigations promptly when classified documents could not be located For example, we noted cases where substations were unable to locate items but did not even report the items as missing.
- Support conclusions in some investigation reports For example, one report concluded that the item was destroyed on a certain day, when the person involved only suggested the possibility that he had put the item in a burn box along with other materials
- Maintain investigative files so that they could be readily located and examined The company did not file investigative reports centrally, and distribution system weaknesses prevented some reports from reaching the DOD program representative

- Take disciplinary action where warranted Investigative reports often recommended that the case be closed, without indicating whether disciplinary action was warranted Also, the reports were not directed to the persons who would need to act

We believe that weaknesses in Lockheed's document-control system for the special access program occurred because of a variety of factors, stemming from the fact that Lockheed was not required to maintain a document-control system on these programs before 1980. It was not until after the requirement came into effect that the company formalized its control system We believe that major factors affecting document control include the following.

- Company emphasis on document controls appeared low For example, Lockheed reduced the resources assigned to document control even though the program activity increased.
- Lockheed did not provide its employees adequate training and indoctrination in document-control procedures or in use of control forms
- DOD did not make periodic inspections and tests of the system to ensure its integrity, and to identify weaknesses. DOD officials told us that, with limited resources, the attention has been on major problems

Sensitivity of Information in Missing Documents

Mr. Chairman, the final part of your request was that we assess the nature or sensitivity of the classified information that has been lost or otherwise not properly accounted for. Except for one top secret document, all the materials the company could not account for were classified secret. A long-standing definition for the use of the secret designation, has been established by executive orders dating back at least to 1972. The definition indicates that the secret classification is to be used if the unauthorized disclosure of the information reasonably could be expected to cause serious damage to the national security.

Based on our review of the description of the contents of unaccounted-for documents and other secret documents that were properly accounted for, it is our opinion that the information was generally of the type that, if compromised, could cause damage to national security. However, it is DOD's and Lockheed's position that, to their knowledge, none of the unaccounted-for documents have been compromised

Lockheed's Corrective Actions

Lockheed officials acknowledge that they have not maintained proper control over classified documents and told us that they have begun corrective measures to improve controls over classified information in their special access programs. The company has set up a blue ribbon committee of security specialists not previously affiliated with Lockheed to review the existing system and recommend improvements. The company also has established a preliminary plan of improvements, based on its own review

The proposed improvements include changes in the organization, the document-control system, and training. To improve organizational controls, Lockheed proposes to

- elevate the Director of Security position so that the Director reports to the second level of management,
- appoint an ombudsman for all security areas, and
- establish a separate audit/investigative group within the security organization.

To improve the document-control system, Lockheed proposes to

- do a complete inventory of all classified material, including working papers that are not required to be accounted for, and to review with DOD what is to be included in accountable material;
- replace the manual control system with an automated one;
- make a complete study of the destruction process; and
- maintain audit records and report results to Lockheed management and DOD.

To improve training, Lockheed proposes to establish a

- comprehensive training program for all employees who handle classified information, and
- document-control station-operator training program

Additional Actions Needed

There is little doubt that Lockheed was deficient in fulfilling its contractual responsibility to properly control and protect classified information in its special access program However, we believe that DOD also shares some of this responsibility because of its insufficient oversight The DOD program office did not make periodic inspections of the system used to protect classified information or require periodic reports from the company on the results of its self-inspections and investigations

In contrast, Lockheed's controls over classified information outside the special access program appeared better As we will discuss further in a moment, semiannual inspections by the Defense Investigative Service may be one reason for this condition. Document-control personnel outside the special access program told us that they routinely did a semiannual inventory of all their classified information, before each inspection by the Service

Previous GAO Review of DOD Special Access Contracts

In 1982, we visited 40 contractors and 20 DOD offices and installations in 5 states to review the physical, personnel, and information security measures used to protect classified information associated with special access contracts. In February 1983, we issued a report—Further Improvements Needed in Department of Defense Oversight of Special Access (Carve-Out) Contracts (GAO/GGD-83-43)—in which we recommended that the Secretary of Defense make the Defense Investigative Service responsible for periodically inspecting special access contracts and verifying the accountability of classified documents.

DOD did not agree with our recommendation and cited six reasons. Prominent among its reasons were (1) the Defense Investigative Service was not staffed to assume the added responsibilities; (2) the program security officer, with program familiarity, was better equipped to make inspections than a Service inspector; and (3) access by Service inspectors would proliferate access beyond the minimum number of persons necessary to meet the objective of providing extra security protection

The situation at Lockheed demonstrates that the problems we described in our prior report still exist Further, our work showed significant differences between controls under Lockheed's special access program and controls outside the program. It is still our conclusion that Defense Investigative Service inspections can help ensure better controls over documents under all classified contracts—whether under special access programs or not. We will recommend again that the Secretary of Defense make the Defense Investigative Service responsible for periodically inspecting special access contracts and verifying the control of classified documents

In summary, it appears inconsistent to us to establish a special access program because of security considerations and then afford it less document protection than normal classified programs

Mr. Chairman, that concludes my prepared testimony. We will be happy to answer questions that you may have.

Requests for copies of GAO reports should be sent to.

U.S General Accounting Office
Post Office Box 6015
Gaithersburg, Maryland 20877

Telephone 202-275-6241

The first five copies of each report are free. Additional copies are $2 00 each.

There is a 25% discount on orders for 100 or more copies mailed to a single address.

Orders must be prepaid by cash or by check or money order made out to the Superintendent of Documents.