FOR RELEASE ON DELIVERY
EXPECTED AT 10:00 A.M.
Thursday, July 24, 1986

UNITED STATES GENERAL ACCOUNTING OFFICE
Washington, D. C.

STATEMENT OF
MARTIN M FERBER, ASSOCIATE DIRECTOR
NATIONAL SECURITY AND INTERNATIONAL AFFAIRS DIVISION

BEFORE THE
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS
HOUSE COMMITTEE ON ENERGY AND COMMERCE

ON

CONTROLS OVER CLASSIFIED DOCUMENTS FOR A SPECIAL ACCESS PROGRAM AT LOCKHEED CORPORATION

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 discussing 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 Department of Defense (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--the Defense Investigative Service was given responsibility for security administration over practically all of DOD's contracts. The Service makes periodic on-site inspections of contractor facilities--in most cases semi-annually--to check for compliance with security requirements. In 1965, DOD decided that special access programs, because of their especially sensitive nature and small number, would be excluded from supervision by the Defense Investigative Service.

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

1As part of DOD 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.

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 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 less 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 been completed, and 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 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 were later located at document control substations.

--50 documents had been removed from accountability by DOD.

--46 documents had been destroyed, with destruction receipts reportedly on file.

--17 documents had 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 semi-annual 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, prior to 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.

--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 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 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:

--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.

--Did not 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 back to 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 has not provided 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 its 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 programs. However, we also believe that DOD also shares some of this responsibility because of its insufficient oversight. DOD 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, semi-annual 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 semi-annual inventory of all their classified information, prior to 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.