REPORT NO. AP-B-95-01

U.S. DEPARTMENT OF ENERGY
OFFICE OF INSPECTOR GENERAL

RELEASE DATE November 1, 1994

AUDIT OF MANAGEMENT AND CONTROL OF INFORMATION RESOURCES AT SANDIA NATIONAL LABORATORIES

U.S. DEPARTMENT OF ENERGY
OFFICE OF INSPECTOR GENERAL

AUDIT OF MANAGEMENT AND CONTROL OF INFORMATION RESOURCES AT SANDIA NATIONAL LABORATORIES

Report Number: AP-B-95-01
Date of Issue: November 1, 1994

ADP and Technical Support Div.
Washington, D.C. 20585

AUDIT OF MANAGEMENT AND CONTROL OF INFORMATION RESOURCES AT SANDIA NATIONAL LABORATORIES

TABLE OF CONTENTS

U.S. DEPARTMENT OF ENERGY
OFFICE OF INSPECTOR GENERAL
OFFICE OF AUDITS

AUDIT OF MANAGEMENT AND CONTROL OF INFORMATION RESOURCES AT SANDIA NATIONAL LABORATORIES

Audit Report Number: AP-B-95-01

SUMMARY

The Sandia National Laboratories makes extensive use of information resources and systems to support its research and development activities and to carry out its defense related activities. During fiscal year 1993, Sandia's expenditures for these types of resources and activities amounted to about $120 million. The objective of this audit was to determine whether information resources at Sandia were managed in a cost-effective and controlled manner. Our work addressed information resource management activities at Sandia operated facilities in Albuquerque, New Mexico, and Livermore, California.

Our audit identified specific areas in which Sandia could improve its policies and procedures for acquiring, managing, using, and controlling information resources. For example, Sandia could achieve substantial cost avoidance or savings in future years by (1) ensuring the efficient use of nearly 24,000 personal computers and workstations in its inventory before acquiring new equipment, and (2) recovering the full cost of operating its mainframe and supercomputers. In addition, better controls are needed to ensure that computer resources will be protected and that data will be available when needed to meet mission requirements.

Officials at Sandia and the Albuquerque Operations Office partially agreed with our conclusions and recommendations. During the course of our audit, they initiated a number of corrective actions to resolve internal control weaknesses in the management of information resources.

Office of Inspector General

PART I

APPROACH AND OVERVIEW

INTRODUCTION

The Sandia National Laboratories has extensive information resources to support its research and development activities. It also relies heavily upon these resources to support our national defense policies. These resources are primarily located in Albuquerque, New Mexico, with a small laboratory in Livermore, California.

The objective of our audit was to determine if Sandia acquired and used its information resources in a cost-effective and controlled manner. Specifically, we wanted to determine whether Sandia had effective procedures and practices for acquiring, managing, protecting, and recovering costs for information resource management (IRM) services provided to users, in accordance with Federal and Departmental regulations, standards and guidance.

SCOPE AND METHODOLOGY

The audit was performed primarily at the Albuquerque Operations Office (ALO) and contractor operated facilities in Albuquerque, New Mexico, and Livermore, California. The audit was conducted by the Office of Inspector General, with participation by Irving Burton and Associates, Inc., and focused on certain IRM functions carried out by Sandia, such as hardware acquisition, cost recovery, and computer security. Most of our on-site audit work was conducted between May and August 1993, although a limited amount of follow-up work was conducted in May 1994.

We interviewed employees and officials involved in IRM activities at Sandia, ALO, and the Oakland Operations Office (formerly the San Francisco Operations Office), and reviewed records and documents describing IRM and computer security plans, policies, and procedures. We also met with representatives from the Department's Office of IRM Policy, Plans, and Oversight, and the Office of Security Evaluations (OSE) to discuss planned, ongoing and completed evaluations and inspections in the IRM area.

We (1) reviewed Federal laws and regulations and Departmental orders and regulations regarding IRM; (2) judgmentally selected eight subcontracts valued at about $23 million and reviewed key contract documents, such as implementation plans, clearance documents, and delivery orders; (3) statistically selected Sandia employees and confirmed the location of property items in their possession in the property records in order to assess the accuracy of these records; and (4) assessed the effectiveness of the technical, administrative, and physical safeguards employed on nine of Sandia's classified and unclassified computer systems (see Appendix B for a listing of systems reviewed).

We also obtained and reviewed reports from prior audits and evaluations by various organizations to determine whether prompt and appropriate corrective actions had been taken on IRM related issues. However, our audit did not address personnel security issues since our office issued a report on "Review of DOE's Personnel Security Clearance Program" in March 1993.

The audit was performed in accordance with generally accepted Government auditing standards for performance audits. This included tests of internal controls and compliance with laws and regulations to the extent necessary to meet the objectives of the audit. Because our review was limited, it would not necessarily have disclosed all internal control deficiencies that may exist.

An exit conference was held with Albuquerque Operations and Sandia officials on September 15, 1994.

BACKGROUND

Sandia is a Departmental facility with a mission dedicated to ensuring that the nuclear stockpile meets the highest standards of safety, security, control, and military performance. Its responsibilities include (1) maintaining a nuclear stockpile that has deterrent value; (2) ensuring the safety, reliability, and quality of the nuclear stockpile; (3) developing technologies to protect nuclear materials throughout their life cycle; and (4) promoting science and mathematics education to ensure that scientific expertise needed in the future is developed. Sandia also performed work, commonly referred to as "Work for Others," for other Federal agencies and private entities when approved by DOE.

Computers, telecommunications, and related information resources play an important role in Sandia's overall mission. For example, Sandia's continued maintenance and enhancement of its Central Computing Facilities is critical to the research and development of new technologies directly impacting Department of Energy (DOE) missions. At the time of our audit, Sandia had over 300 mainframe and supercomputers, acquired at a cost of over $44.5 million. It also had nearly 24,000 personal computers and workstations, plus related equipment, acquired at a cost of over $117 million. During fiscal year 1993, Sandia spent about $120 million on information technical systems, including operation and maintenance.

The organizational structure established to manage these resources consists of a central office and six other individual components. Sandia's central computers are managed and controlled by the Office of Scientific Computing Directorate, whose areas of responsibility include software, computing resources, and telecommunications.

Sandia was operated by Sandia Corporation, an AT&T Technologies, Inc. entity, for the United States Government on a no-fee, no-profit, no-loss contract. In September 1993, the Department awarded a new contract for the management and operation of the facility to Sandia Corporation, a now separate autonomous business entity of Martin Marietta, Inc.

A number of reviews by OSE and the General Accounting Office (GAO) have disclosed significant deficiencies in Sandia's IRM program and the administration of the contract by the Department's Albuquerque and Oakland Operations Offices. The operations offices, and Sandia's internal auditors, have also identified and documented shortcomings in Sandia's IRM program. Examples of problems identified by these various organizations include (1) subcontracts awarded on a sole-source and non-competitive basis without adequate justification; (2) cost and price analyses not performed to determine the reasonableness of vendors' proposals; (3) a property management system not properly maintained in order to account for valuable property, such as computer equipment; (4) passwords on classified systems not properly administered; (5) a computer protection plan not developed and maintained; and (6) security reviews not adequately performed by the Department.

OBSERVATIONS AND CONCLUSIONS

In recent years, Sandia has taken steps, as well as set goals, to improve its management and use of information resources. For example, Sandia has (1) plans to establish central telecommunications networks based on single, homogenous, secure and restricted computing environments; (2) plans to consolidate its supercomputing facilities at the Albuquerque site in New Mexico; (3) developed multi-layers of protection measures designed to restrict access to data and computer facilities; and (4) enhanced its property management system in order to improve accountability.

While these efforts were positive, selected improvements are needed in Sandia's acquisition, management, and use of information resources in order to ensure full compliance with applicable policies and regulations and to fully protect the classified and sensitive data that resides on Sandia's information systems. Also, savings can be obtained by ensuring efficient use of existing information resources and recovering the full cost of operating mainframe and supercomputers from users. In addition, improved contract administration procedures by the Albuquerque and Oakland Operations Offices are needed to correct identified problems and ensure the efficient management and use of Department-owned information resources.

The finding contained in Part II involved material internal control weaknesses that Management should consider when preparing its yearend assurance memorandum on internal controls.

PART II

FINDING AND RECOMMENDATIONS

Management and Control of Information Resources

FINDING

Federal and Departmental guidance requires governmental agencies to ensure that information resources be acquired and used in an efficient and economical manner, and that computer-processed data be adequately protected. Information resource management (IRM) activities account for a significant portion of Sandia's annual expenditures; however, inefficiencies and weaknesses existed in Sandia's acquisition, use and control of computer resources, and in the protection of computer-processed information. These conditions occurred because (1) Sandia had not fully developed and implemented IRM policies and procedures consistent with Federal and Departmental regulations or sufficient to ensure the efficient use of information resources; and (2) responsibilities and procedures for the review and oversight of Sandia's IRM program were not clearly assigned and carried out. Without specific improvements in its IRM procedures, Sandia cannot ensure that information resources are acquired and used in an efficient and cost-effective manner, or that classified and sensitive computer-processed data is adequately protected.

RECOMMENDATIONS

We recommend that the Manager, Albuquerque Operations Office:

1. Direct the Sandia National Laboratories to:

   a. Reexamine planned computer equipment acquisitions and related acquisition policies and procedures to ensure conformance with Federal and Departmental regulations, orders and standards, particularly with respect to key factors—e.g., mission and program requirements, utilization of existing resources, consideration of sharing existing Department resources, audit verification, and cost or price analyses;

   b. Revise cost recovery/chargeback policies and procedures so they are consistent with relevant Federal and Department regulations;

   c. Recompute and collect undercharges for computing services provided to Work for Others program users; and

d. Revise computer security policies and programs to ensure full and consistent implementation of Federal and Departmental regulations and standards for the protection of classified and sensitive information stored on computer systems.

2. Strengthen Departmental review and oversight of Sandia's IRM program by:

   a. Clarifying and/or revising operations office responsibilities for review and oversight of Sandia's IRM activities contained in the existing management agreement and local order; and

   b. Ensuring that procedures are in place that provide for full review of IRM activities and the timely correction of identified deficiencies.

MANAGEMENT REACTION

Management partially agreed with our conclusions and recommendations. Management partially concurred with recommendation 1a, concurred with recommendations 1b, 1c and 2a, but nonconcurred with recommendations 1d and 2b. See Part III for further discussion.

DETAILS OF FINDING

GUIDANCE ON INFORMATION RESOURCES MANAGEMENT

Federal guidance requires governmental agencies to ensure information resources are acquired and used in an efficient and economical manner. With respect to management and operating (M&O) contractors, guidance relating to the acquisition and use of information resources is contained in Federal regulations, DOE regulations and orders, and the M&O contract. Departmental regulations and orders require that M&O contractors develop and maintain efficient computer security programs to protect the confidentiality of classified and sensitive unclassified data.

The Department of Energy Acquisition Regulation (DEAR) requires M&O contractors to develop and maintain systems of management and control to ensure that subcontractors comply with contract terms and promote efficient and effective operations. DEAR Part 970 requires M&O contractors to comply with the procedures contained in applicable Departmental orders when acquiring information resources. Part 970 states that contractors' purchasing systems follow business practices appropriate for the requirement and dollar amount of the purchase involved. Purchases must be made in the most advantageous manner in meeting the Department's overall mission considering price, quality, and timely and efficient contract performance.

Other IRM guidance for M&O contractors is contained in various Departmental orders and the Federal Information Processing Standards (FIPS) publications:

- DOE Order 1360.1B, dated January 7, 1993, establishes specific policies and procedures for the acquisition and management of computer resources. The Order states that Departmental elements must prepare an implementation plan for major acquisitions. The implementation plan must include several elements, including validation of current workload and workload forecast.

- DOE Order 2100.8A, dated January 27, 1993, establishes policies and procedures for the distribution and recovery of the costs of operating information technology facilities. The Order requires actual billing and recovery of all automated data processing (ADP) costs, including depreciation, for services provided to other organizations.

- DOE Order 5639.6, dated September 15, 1992, establishes uniform requirements, policies, and procedures for developing a security program to ensure the protection of classified information stored within ADP systems. The Order requires that contingency plans be developed, documented, and maintained for each classified ADP system.

- DOE Order 1360.2B, dated May 18, 1992, provides similar guidance for computer systems with unclassified information. The Order requires that a computer protection plan be developed and maintained that describes the administrative, technical, physical, and personnel safeguards used to protect unclassified systems located at a site.

- FIPS 112 identifies fundamental elements that must be considered and controlled when operating a password system for accessing data stored within a computer system.

- FIPS 73 specifies software features or technical safeguards to be implemented to help control access, limit user privilege, and maintain the confidentiality of classified or proprietary information.

The former AT&T contract also required Sandia to carry out its IRM activities in an efficient and economical manner. For example, the contract required Sandia to select subcontractors on a competitive basis to the maximum extent practical, to use a system of accounting and property control conforming to sound accounting principles, and to safeguard all Departmental property in its custody.

INFORMATION RESOURCES MANAGEMENT AT SANDIA

To support its missions during fiscal year 1993, Sandia spent about $120 million, or 12 percent of its approximately $1 billion annual budget, in total expenditures on information technology systems. About $63 million of the expenditures on information technology, or 53 percent, was for the purchase of commercial services. These services included the operation and maintenance of computer systems and voice and data communications. The next largest portion of these expenditures was $42 million, or about 35 percent, for capital investments.

Although Sandia had taken some positive steps to develop an effective IRM program, it had not made sufficient efforts to ensure that information resources were acquired and used in an efficient manner or that information on its computer systems was adequately protected. Problems were noted in both the acquisition and use of (1) mainframe and supercomputing resources, and (2) personal computing resources. Also, problems previously identified at Sandia concerning the acquisition, management, and control of information resources still exist.

Acquisition and Use of Mainframe and Supercomputing Resources

In acquiring and using information resources, Sandia did not take the actions needed to ensure that information resources were obtained in the least costly manner, efficiently used, and adequately protected. In awarding acquisition contracts for major information resources, Sandia did not take necessary actions to ensure that such resources were obtained at reasonable prices. Also, Sandia did not equitably distribute and recover all costs for operating its computer equipment and facilities, nor did it ensure the adequate protection, integrity and confidentiality of classified and sensitive information stored on this equipment.

Mainframe and Supercomputing Acquisitions

Contracts to acquire information resources were not awarded, and other necessary actions were not taken, by Sandia to ensure that goods and services were obtained at reasonable prices, and procurements were made in the government's best interest. A review of eight subcontracts awarded from 1987 to 1992, relating to the acquisition of about $23 million in mainframe and supercomputing resources, disclosed that Sandia did not provide adequate justification for sole-source procurement or perform other actions, such as audit verifications and performance and capability validations, necessary to support the acquisition of information resources. Further information concerning the results of our review of Sandia's acquisition of information resources is provided in Appendix A.

Prior audit reports have addressed Sandia's methods for acquiring information resources. For example, a December 1982

report by the General Accounting Office (GAO) identified major problems in Sandia's acquisition process and pointed out that sole-source, noncompetitive contracting for computer resources was a relatively common practice. In an August 1987 report, GAO again pointed out limitations in Sandia's efforts to obtain goods and services at the most reasonable prices. GAO noted that Sandia had waived requirements for publishing procurement notices, and market searches were either not completed, limited or inadequately documented. Also, advertising through published notice was rarely performed to determine potential qualified vendors capable of satisfying the Laboratories' requirements, to include computing resources.

In addition to the GAO reports, an October 1991 report by ALO pointed out that only 29 percent of Sandia's procurements were competitive. This report also discussed a number of weaknesses relating to sole-source procurements and Sandia's overall acquisition planning. Our audit results indicated the conditions found by GAO and ALO concerning the acquisition of information resources still largely existed at Sandia.

Control and Use of Mainframe Computers and Supercomputers

Sandia, in using its mainframe and supercomputing information resources, did not ensure efficient use of direct access storage devices; equitably distribute and recover the cost of operating its computer equipment and facilities; or adequately provide for the protection, integrity and confidentiality of classified and sensitive information.

We found that Sandia was not making efficient use of its disk space. Our analysis of two systems, acquired at a cost of over $840,000, showed that 44 percent of the total disk space had not been allocated for use by Sandia. Of the total disk space, 15 percent had been allocated, but not used within the past three months, and 13 percent had been allocated, but never used by Sandia. Thus, only 28 percent of the total disk space on the two systems had been allocated and used within the past 90 days. Overall, this condition represents an inefficient use of a costly storage medium.

The costs of operating mainframe and supercomputer equipment were not appropriately identified and charged out to users. For example, Sandia's inventory records contained over $44 million in mainframe and supercomputing equipment, as of May 1993. However, the cost for this equipment was not fully recovered from or distributed through charges to equipment users. In addition, other costs incurred in the operation of ADP facilities—such as space occupancy and disk drive utilization—were not appropriately identified and charged out to equipment users.

Since DOE Order 2100.8A requires the recovery of all costs, including depreciation, for services provided to other

organizations, procedures that do not provide for full recovery of cost can result in the Department subsidizing computing services that are provided to outside users. For example, at Sandia, Work for Others program users provided about seven percent of the fiscal year 1993 subscriptions for the Scientific Computing organization, which controlled and operated almost $28 million worth of mainframe or supercomputing equipment. Since Sandia did not appropriately provide for full cost recovery in charges to users, Other Federal Agency Work for Others program users were not billed for their share of annual depreciation cost for this equipment. However, it should be noted that we did not attempt to perform a comprehensive audit of all elements of costs charged or billed to equipment users.

We also noted Sandia's computer security programs were not sufficient to ensure protection, integrity and confidentiality of classified and sensitive information stored on the Laboratories' computer systems. For example, Sandia employees were granted access to computer systems that stored and processed classified and sensitive data in excess of what was necessary for them to perform their job functions. Furthermore, only limited efforts were made by Sandia to remove inactive users from the computer systems. Overall, deficiencies existed in the areas of (1) access controls and technical safeguards, (2) operating system controls, (3) password administration, (4) organizational controls and audit trails, and (5) computer security and contingency planning. Further information on computer security weaknesses at Sandia is provided in Appendix B.

Acquisition and Use of Personal Computers

In acquiring and using personal computing resources, including related peripherals, Sandia neither ensured the efficient use of equipment already on-hand before purchasing additional equipment, nor adequately accounted for, controlled, or reported on computer equipment in its property management system.

Personal Computing Acquisitions

Sandia acquired personal computing equipment without sufficient regard to resources already on-hand and available for use. Decisions for purchasing new personal computing equipment were not based on key factors like the availability of excess property on-hand and the utilization and distribution of existing equipment among personnel. Sandia organizational units were allowed to acquire personal computing equipment, independently with little justification, through the use of indefinite quantity contracts with five vendors.

During the last three fiscal years, Sandia expended $67 million, including $25 million in fiscal year 1993 alone, for personal computing equipment, excluding related peripherals. In addition to 1,649 computers provided to subcontract employees and

466 computers in reclamation, inventory records showed Sandia had 21,845 personal computers assigned to 6,496 employees, representing an average of nearly 3.4 computers per employee. Over 200 of these employees had two or more computers designated for home use. Overall, 1,806 of these personal computers, with an acquisition value of $6,218,000, were listed as being located at Sandia employee private residences. Despite the amount of personal computing equipment already on-hand and in use, the long range IRM plan indicated that Sandia planned to expend an additional $10 million on personal computers in fiscal year 1994. However, a Sandia official stated that (1) a new policy, which applies to employee home use of personal computers, was issued on September 7, 1994, that suggested acquisition of portable-type computers for dual home and office use; and (2) the number of personal computers listed in inventory records as located at employee private residences had been reduced to 1,202 as of September 1, 1994.

Use of and Accountability for Personal Computers

Sandia had not efficiently used or adequately accounted for its personal computing resources. A statistical sample of Sandia employees was selected to evaluate the use of personal computing equipment at Sandia and the accuracy and completeness of ADP inventory records maintained on Sandia's property management system. These employees possessed 470 pieces of equipment (e.g., printers, central processing units, etc.) with an acquisition value of about $2.4 million. From this sample, we learned that:

- Utilization of Sandia's personal computers was limited. The employees interviewed told us that 48 items with an acquisition value of $158,000, or about 10 percent of total items in possession of the employees sampled, were not needed to carry out assigned duties and responsibilities. The employees indicated that over thirty percent of their equipment had a utilization rate of less than 10 percent. They also indicated that some of the equipment (e.g., computers, printers, plotters) would not be needed if this equipment was available through a "computer lab" or if other sharing arrangements were made.

- ADP inventory records maintained in Sandia's property management system were substantially in error regarding location or possessor of equipment. For example, over 20 percent of total items in possession of the employees sampled had an incorrect location. We also could not locate about 6 percent of total items in possession of the employees sampled. Employees interviewed had in their possession 51 items of personal computing equipment not assigned to them in the property management system.

A recent Office of Inspector General (OIG) report, issued March 1994, disclosed problems at Sandia in the management and control of property. For example, $388,669 in excess property,

including personal computing equipment, was missing. Also, excess property was classified as surplus, when in good condition, and inventory control identification tags were missing. Further, personal property, including computers and peripheral equipment, was stored outdoors exposed to weather conditions. This personal property had been categorized as "excess."

REASONS FOR SHORTCOMINGS IN IRM PROGRAM

A primary reason for inefficiencies and weaknesses in Sandia's IRM program was that Sandia had not fully developed or implemented IRM policies and procedures consistent with Federal and Departmental IRM regulations or sufficient to ensure the efficient use of information resources. Although a number of the deficiencies identified during our audit had been previously identified in other reviews and reports, Departmental organizations with oversight responsibility for Sandia did not have adequate procedures in place to ensure that these deficiencies were corrected in a timely manner.

Sandia's Policies and Procedures

Although Sandia had developed and implemented policies and procedures for its IRM program, they were sometimes inconsistent with Federal and Departmental regulations and standards, or not sufficient to ensure cost effective acquisition, efficient use and adequate protection of information resources. Specific weaknesses were noted in Sandia's policies and procedures for (1) procurement of computing resources, (2) cost recovery of mainframe and supercomputing resources, and (3) computer security and protection.

Acquisition Policies and Procedures

Policies and procedures governing Sandia's procurement of computing resources did not sufficiently ensure that funds allocated to acquire information resources were cost effectively and economically used. DOE Order 1360.1B requires that computer resources not be acquired until it is determined that requirements cannot be efficiently and economically met by sharing existing resources. Although Sandia Procedure 6900 required that property acquisitions be limited to only those essential for program performance, and excess or underutilized property be used as a first source of supply, specific procedures were generally lacking to ensure conformance with provisions of this Order. For example, Sandia Laboratory Instruction 6620-1, a procedure governing the acquisition of general purpose equipment, like personal computers, by non-Sandia personnel, required only an approval from the requesting organization for equipment acquisitions without requiring a search of excess property available from internal sources by the requesting organization or the organization controlling excess property. In November 1993, guidance was issued by Sandia to provide employees with instruction on obtaining or turning in excess property. Also, according to

Sandia officials, a computer based on-line listing is now employee accessible that not only provides an up-to-date catalog of available excess property, but also lists similar equipment in use within Sandia operating organizations.

Cost Recovery/Chargeback Procedures

Policies and procedures for cost recovery were not consistent with Federal and Departmental regulations and did not result in the equitable distribution and recovery of the full cost of operating the Laboratories' mainframe and supercomputing equipment and facilities. For example, in 1991, Sandia established a "service center concept" for operation of its computer facilities. Under this concept, Sandia customers were provided specialized products or services, such as software development and maintenance. However, this "service center concept" did not provide for full and equitable recovery of costs incurred by the computer facilities, such as depreciation, space occupancy, and disk drive utilization, in accordance with Departmental regulations. At the start of fiscal year 1994, Sandia management switched the allocation method for space, occupancy and utility costs in charge rates in order to ensure a more equitable allocation of these costs to computer system users.

Computer Security and Protection

Sandia's policies and procedures for its computer security programs were not sufficient to ensure the protection of computing information resources. These policies and procedures did not contain specific guidance that was consistent with Federal and Departmental regulations and standards for providing adequate protection for classified and sensitive information stored on the Laboratories' computer systems. For example, there were no requirements related to the frequency of analysis of access privileges and activity to determine the propriety and continued need for user accounts. As a result, security officers at Sandia were not giving adequate attention to monitoring aspects of computer security in their organizations to be sufficiently informed on the adequacy and effectiveness of security measures. Also, computer system access controls, technical safeguards, and operating systems controls were not adequately employed, activated and monitored. Contingency and security plans were not being developed and modified based on system changes.

Departmental Oversight of Sandia's IRM Activities

Existing responsibilities and procedures for review and oversight of Sandia's IRM program were not clearly assigned and carried out. Policies and procedures (1) did not clearly define responsibility for oversight of Sandia's IRM program activities, and (2) did not sufficiently provide for comprehensive review and assessment of Sandia's IRM program activities.

Other reports also pointed out deficiencies in Departmental organization management policies and procedures. For example:

- GAO reported on Albuquerque's inability to (1) eliminate overlap and duplication in existing systems, or (2) implement an effective program for evaluating existing systems at contractor facilities under its jurisdiction.

- The recent OIG report on Sandia's property management system noted that Albuquerque was required to perform appraisals of functional segments of the system at least every two years. However, due to shortages in personnel, Albuquerque had appraised only 3 of 14 functional areas.

- An OSE review pointed out that the operations offices (i.e., ALO and Oakland) were not identifying some major problems in the appraisals of the computer security programs at the two Sandia locations. Furthermore, OSE noted that where appraisals identified problems, the M&O contractor had not corrected them.

Responsibility for Oversight of Sandia

Responsibility for oversight and review of Sandia's IRM activities was contained in ALO Order 1360.1A, Revision 1, and in a management agreement for Sandia-Livermore. However, these policies did not clearly define responsibility for oversight and review of Sandia's IRM program activities. For example, the management agreement between ALO and Oakland delegated some responsibilities for oversight at Sandia-Livermore to Oakland. These oversight responsibilities included performing appraisals and surveillance of the operational effectiveness of the M&O contractor's activities and the computer security program. However, an Oakland official reported that a lack of communication existed in that Sandia would consult ALO about changes or events relating to the Sandia-Livermore computer security program, but Oakland would not be informed about the matter.

Also, ALO Order 1360.1A did not clearly define responsibility for review of Sandia's IRM program activities in a manner consistent with Departmental and Federal regulations. For example, the Order did not require the contracting officer to take an active role in carrying out oversight of the M&O contractor's acquisition activities, as required in the DEAR. For the eight mainframe and supercomputer contracts that we reviewed, the ALO contracting officer did not review the cost, price, or documentation aspects of Sandia's information resource acquisition functions. Instead, we found that other ALO personnel approved the implementation plans for the eight sole-source contracts without ensuring that (1) adequate justification existed for the sole-source contracts, (2) price reasonableness and fairness had been sufficiently evaluated through such measures as audit review and verification, and (3) performance and capability validations

were performed to assess how a vendor's system would process the workload—e.g., processing speed and resource consumption—when compared to the performance of other systems.

Review, Appraisal and Surveillance Procedures

Existing operations office procedures did not sufficiently provide for comprehensive assessment and review of Sandia's IRM program activities. Reports prepared for the operations office appraisal and review programs of Sandia's information resource activities generally focused on compliance with Departmental orders and regulations, but did not normally address the impact of deficiencies found or determine compliance with applicable Federal regulations and standards. Also, the procedures did not include methods for ensuring timely and effective correction of prior found deficiencies.

For example, procedures utilized during the 1991 and 1992 reviews of Sandia's purchasing system enabled ALO review teams to identify 8 and 49 recommendations, respectively, to findings, including excessive reliance on sole-source contracting. However, the work performed did not include steps for determining or measuring the impact that the findings relating to Sandia's purchasing methods had on the Department and for ensuring the effectiveness of corrective actions for prior findings. The reviews culminated in recommendations being given to the ALO contracting officer for continuing approval of the Sandia purchasing system despite the number and recurrence of findings and recommendations. As a result, problems persisted in the information resource acquisition portion of the IRM program without effective corrective actions being taken by Sandia.

Also, procedures utilized in computer security program surveillance were not structured to adequately assess Sandia's compliance with Federal standards. At the time of our audit, the existing Sandia contract required Sandia to conform to all security regulations and requirements of the Department, which would include compliance with applicable Federal computer security standards. However, an ALO Security Official explained that their reviews and appraisals were only performed to determine compliance with applicable Departmental orders, which only directly addressed one Federal standard.

In addition, operations office procedures were not established for the review of other aspects of Sandia's IRM program activities to ensure compliance with contract functions and Departmental and Federal regulations. The operations office personnel were not sufficiently evaluating other IRM practices at Sandia, such as property management or cost recovery systems, to ensure that these systems provided the information necessary to evaluate the M&O contractor's mission performance and compliance with applicable Departmental and Federal regulations.

IMPACT OF IRM DEFICIENCIES

Without specific improvements in its IRM procedures, Sandia cannot ensure that information resources are acquired and used in an efficient and cost-effective manner, or that classified and sensitive computer-processed data is adequately protected.

Benefits Available From Improving Acquisition Practices

By improving its acquisition practices, Sandia can better ensure that fair and reasonable prices are paid for information resources. For the eight subcontracts we reviewed, Sandia awarded the subcontracts without (1) providing adequate justification for sole-source procurement, or (2) conducting negotiations based on adequate cost and price analyses that included the performance of advisory audits and technical reviews. As a result, the Department may have paid excessive prices in the acquisition of computing resources since other vendors may have been available to perform required tasks more efficiently, effectively, or reasonably than the vendors selected. Also, contracting officials lacked the bases necessary for determining and attaining a fair and reasonable contract price during negotiations. We were unable to determine potential savings available in the cases cited in this report, because Sandia did not perform sufficient market analyses at the time of the subcontract award to identify potential vendors and their bid prices and did not obtain necessary cost or pricing data from vendors.

Also, by implementing procedures for evaluating the most effective solutions for meeting computing needs, Sandia can ensure that information resources are not acquired in excess of that necessary to support the Laboratories' mission. For five of the eight contracts reviewed, Sandia did not conduct performance and capability validations—e.g., benchmark testing to assess how a vendor's system would process the workload, processing speed, and resource consumption. As a result, Sandia did not have meaningful information to determine the most effective solution for meeting its computer needs.

Sandia planned to spend almost $10 million in fiscal year 1994 for personal computers and work stations. Based upon our survey of users, we believe that Sandia could reduce its investment in personal computers and workstations if Sandia's organizational units adequately identified and reported excess equipment to inventory control points for possible redistribution to other users, or if they addressed other alternatives for satisfying employee equipment needs.

Sandia planned to spend almost $53 million in fiscal year 1994 for other types of computers (e.g., mainframes, minis, etc.) despite having over 300 computers in inventory. Yet, the contractor excessed a supercomputer system after less than two years due to limited utilization. Although we did not have an

effective means to readily assess the utilization of Sandia's systems, monies could be saved if Sandia implements procedures for monitoring utilization and includes the results as part of its basis for determining future acquisitions of computing resources.

Benefits from Improving Controls Over Information Resources

By improving its controls over information resources, Sandia will be better able to ensure that computing resources are efficiently used and available for supporting the Laboratories' mission. Sandia needs to ensure that it has adequate procedures to account for and safeguard valuable equipment. During our audit, we could not readily locate all equipment assigned to Sandia employees based on the information in the property management system. Also, as noted in the prior OIG report, excess property was not adequately protected. As a result, Sandia was missing $388,669 worth of excess property.

Through improvements in cost recovery procedures, Sandia can better ensure that (1) appropriate consideration is given to all information resource costs in determining how to satisfy each user's computing needs, and (2) users are equitably charged for information resource consumption. If users are not charged for, or made aware of, costs of using information resources, it is difficult to hold them accountable for using those resources in an efficient and cost-effective manner. Because of inconsistencies in Sandia's cost recovery procedures, when compared to DOE Order 2100.8A, Other Federal Agency Work for Others program users at Sandia were undercharged for mainframe computing services.

By improving its computer security programs, Sandia can better ensure that computer-processed information, both classified and sensitive, is accessible only to authorized personnel and is available when needed to support the Laboratories' mission. Based on our audit results, weaknesses in computer security controls increased the potential for loss or disclosure of classified or sensitive data. In addition, Sandia could be vulnerable to prolonged disruptions—such as those caused by earthquakes, fire, or sabotage—because it did not have adequate requirements for maintaining a contingency plan to continue critical data processing operations.

PART III

MANAGEMENT AND AUDITOR COMMENTS

Albuquerque Operations Office (ALO) management partially agreed with our conclusions and recommendations in its response to our official draft report. ALO partially concurred with recommendation 1a, concurred with recommendations 1b, 1c and 2a, but nonconcurred with recommendations 1d and 2b of the finding. In addition, management noted that corrective actions for some deficiencies cited in our finding were completed or in process. We revised Part II and Appendix B of the report to reflect these actions. Management's comments to our recommendations and our response are summarized below.

Recommendation 1.a.

Management Comments. Management acknowledged that Sandia National Laboratories (SNL) failed, in some cases, to provide adequate justification for sole source computing resource acquisitions and to give adequate consideration to the sharing of Departmental resources located at other DOE facilities. Management stated that procedures would be modified to assure that these two deficiencies are corrected.

Auditor Comments. Management's comments are partially responsive to our recommendation. In light of improvements to be made in acquisition procedures and efficiencies in computing resource use, Sandia also needs to reexamine computing equipment acquisition plans to ensure that these procurements will still prove prudent and cost effective.

Recommendation 1.b.

Management Comments. Management pointed out that the new SNL contract with Martin Marietta does include DOE Order 2100.8A in the baseline list of financial documents. Therefore, Management stated that SNL would develop the accounting and reporting required to disclose non-fund depreciation expense associated with computer usage.

Auditor Comments. Management's comments do not fully address our recommendation. ALO should ensure that revisions to Sandia policies and procedures for cost recovery and charge back comply with Federal and Departmental regulations for not only selective costs like depreciation, but also for all other costs of providing computing services to users. DOE Order 2100.8A requires both the charging of fund costs, for internal purposes, and the billing of non-fund costs, like depreciation, on a memorandum basis to Department users. Furthermore, the Order requires actual billing and/or recovery of full costs, fund and non-fund, for operating information technology facilities from other users, including other Federal agencies.

Recommendation 1.c.

Management Comments. Management stated that it did not believe that the depreciation expense associated with Other Federal Agencies program users would result in a significant difference for the period of October 1, 1993 through April 30, 1994. However, Management did indicate that future billings to Work for Others users would include cost distribution for depreciation. Because of the new Sandia contract, Management also expressed the need for a timeframe to recompute and collect undercharges from prior years.

Auditor Comments. Given the requirements of DOE Order 2100.8A, ALO has a clear responsibility, as Sandia contract manager, to ensure that funds due to the Department are collected by Sandia for providing computing services to users. However, we believe that ALO's concern is valid regarding a timeframe for undercharges from prior years. Since the Department awarded the new contract for the management of Sandia in September 1993, we feel that it is reasonable, at minimum, for ALO to direct Sandia to recompute and collect computing service undercharges for Work for Others program users arising since the start date of this new contract.

Recommendation 1.d.

Management Comments. Management stated that SNL computer security policy has been, and is, in full compliance with applicable Federal and Departmental regulations, and was in no need of revision at the time of the audit. Management also stated that most SNL requirements are derived directly from applicable DOE orders, such as DOE Order 1360.2B "Unclassified Computer Security Program", and executive orders, such as OMB Circular A-130. Management remarked that the audit conclusions were not valid since only nine of the thousands of systems at Sandia were addressed therein. Management explained that, since the time of the audit, a Departmental and regulatory change was implemented that requires the changing of the passwords on classified computers every six months instead of once a year. Management noted that SNL has made the change to comply with the new requirement. Also, Management pointed out other SNL improvements: (1) access to operating system datasets has been further restricted, (2) all accesses are logged on three of the systems reviewed, thereby providing an audit trail, and (3) users are notified of their login attempts on two of the systems reviewed.

Auditor Comments. We do not consider Management's comments to be fully responsive to our recommendation. Our report noted areas where Sandia was not in full compliance with applicable guidance. For example, Sandia had not established sufficient organizational controls and audit trails to fully comply with Departmental regulations like DOE Orders 1360.2B and 1000.3B. The latter Order, cited by reference in DOE Order 1360.2B and

relating to internal control systems, specifically identifies "general control environmental factors" such as proper segregation of duties and the adequacy of audit trails. Therefore, there is still a need for Management to direct Sandia to take additional steps to revise policies and programs for the protection of classified and sensitive information stored on computer systems. Sandia policies like the "Computer Security Desk Reference" could receive additional revision to establish Sandia management requirements for regular review and monitoring of computer system user access need and inactive user accounts. Revisions of this nature, in conjunction with other Management noted actions, would address computer system access control weaknesses cited in the report. Also, the computer security portion of our finding has significance since the nine systems reviewed included the only unclassified system considered by Management to be mission-essential at Sandia.

Recommendation 2.a.

Management Comments. Management noted that security oversight responsibility had been established for many years; they also stated that action has been taken to bring all computer security oversight activities for SNL-Livermore under ALO.

Auditor Comments. Management's comments are not viewed as being fully responsive to our recommendation since computer security is only one aspect of Sandia's IRM activities. Our recommendation addresses more than ALO responsibility for review and oversight of computer security. There still remains a need for Management to clarify and/or revise ALO Order 1360.1A to be consistent with Departmental regulations and to establish a more active ALO contracting officer role in Sandia information resource procurement actions, rather than providing assistance on an "as needed" basis as the Order now provides.

Recommendation 2.b.

Management Comments. Management stated that Federal policy and procedure, pertaining to review, surveillance and appraisal, is followed to detect, track, correct and eliminate the recurrence of identified deficiencies in SNL activities. Management pointed out that the possible failure of SNL to meet the requirements of DOE and ALO orders would not be criteria for revising Federal policy or procedures.

Auditor Comments. Management's comments did not address the need for ALO to revise its procedures for review and oversight of Sandia's IRM program. We were not recommending that ALO revise "Federal policy and procedures." Rather, ALO has a responsibility to institute site specific guidelines and procedures to effectively implement applicable Federal and Departmental regulations and standards at its cognizant sites, and to ensure that identified deficiencies are corrected in a timely manner.

MAJOR COMPUTER ACQUISITIONS

This appendix contains detailed information concerning the results of our review of Sandia's acquisition of major information resources.

APPLICABLE CRITERIA

DOE and Federal regulations contain provisions relating to the acquisition of goods and services, like information resources, that if followed, will reasonably assure acquisitions are executed in an economical manner and in the government's best interest.

DOE Order 1360.1B requires that implementation plans and/or clearance documents for major items of automated data processing equipment be adequately reviewed at appropriate levels within DOE. ALO Order 1360.1A, that implements the directive, establishes review and approval authority levels. ALO has approval authority for acquisitions from $200,000 up to $1 million. Approval authority for acquisitions of $1 million or more rests with DOE Headquarters unless delegated to ALO.

DEAR 970 requirements are intended to encourage M&O contractors to enter into contracts on behalf of the Department on a competitive basis to the maximum extent possible, and to discourage the use of sole-source procurements, solicitation, and negotiation directed to only one source. DEAR 970.7103 requires M&O contractors to perform price and cost analyses of vendors' proposals consistent with principles of FAR subpart 15.8 and DEAR subpart 915.8 prior to negotiating contracts on behalf of the Department. DEAR 970.7104-11 and FAR 15.8 require negotiations with vendors be based on proposals supported by current certified cost or pricing data obtained from vendors for awards expected to exceed $100,000, unless certain exemptions are granted, such as a waiver for vendors offering proposed items at catalog or market prices. DEAR 915.805-70 addresses the performance of pre-award audits to determine fairness and reasonableness of vendors' proposals that exceed $500,000, if fixed price, and $1,000,000, if cost reimbursable. FAR 15.804-3 encourages verification, including audit, of data pertaining to catalog or market prices that supports a vendor's proposal prior to issuance of an exemption from submission of certified cost or pricing data.

RESULTS OF REVIEW

Sandia did not award subcontracts and perform necessary actions to ensure that major information resources were obtained at reasonable prices and in the government's best interest. Sandia's inventory and contract records showed that, from June 1985 through May 1993, it had completed 36 mainframe and supercomputing acquisitions, over $200,000 each, with an initial

value of over $40 million. Included were 6 acquisitions, in excess of $1 million each, with a total value of about $23 million. We reviewed the eight subcontracts which comprised these 6 acquisitions. We found that these subcontracts, awarded from 1987 to 1992, generally contained the appropriate level of Department approval. However, the subcontract files did not contain sufficient evidence of the performance of actions, such as audit verifications and performance and capability validations, necessary to support the reasonableness of the acquisitions. Also, the files did not contain sufficient justification for sole-source procurement.

Three of the files reviewed pertained to the award in August and September 1992 of three contracts (LA-3927, LA-4643, and LA-7081) totaling nearly $1.5 million for two Convex network storage systems, including related software and peripherals. System specifications appeared to restrict competition as Sandia required offerors to provide UNIX based systems and demonstrate the ability to run UNITREE software. Contrary to Departmental regulations, the files did not contain evidence to show that Sandia had conducted market research before awarding the sole-source contracts or that they used publications like the Commerce Business Daily to publicize notice of prospective awards. A Sandia official pointed out that market surveys of potential vendors, as in this procurement, were usually informal and not documented.

Also, other factors may have greatly influenced Sandia's sole-source procurement decision, to the detriment of other prospective vendors, such as the previous purchase of a similar system from the contract awardee and the contract awardee making a system available to Sandia for use in evaluating configuration requirements. No audit reviews or verifications were performed to determine qualification for the exemption that was granted from submission of the certified cost or pricing data. Such data would be needed to determine the fairness and reasonableness of the awardee's proposal.

The results of our review for the remaining five contract files were as follows:

- In November 1992, Sandia awarded a $15.9 million sole-source contract (AD-1874) for a supercomputer based on its previous sole-source acquisitions of massively parallel processing supercomputers. This award was made to the selected vendor despite existence of five other vendors with machines of similar capability. In its proposal, the vendor stated it could not qualify for an exemption from submission of certified cost or pricing data needed to perform an adequate evaluation of cost and price reasonableness; yet Sandia granted an exemption and awarded them the contract. Sandia also relied on generalizations about scientific research to

justify award of the sole-source contract. Although Sandia justified the acquisition by stating its primary objective was to meet scientists' needs, the contract files contained no evidence that any effort was made to identify those needs. In addition, Sandia had five other machines which it used to conduct similar research; yet trends in their data processing work loads were not identified to show when their existing system capabilities would be saturated, if at all.

- In January 1991, Sandia awarded a $995,000 sole-source contract (12-4175Y) to upgrade to an existing supercomputer system initially acquired in September 1988 (contract 75-4148). The Laboratories used the critical nature of its scientists' work to justify the system. Its justification indicated that a high performance system was required to perform its scientific applications and numerical algorithms. In January 1993, the system was surplused due to limited utilization. Sandia also did not (1) require the selected vendor to provide certified cost and pricing data; (2) obtain advisory audit reviews/verifications and technical evaluations; and (3) use the results of these advisory reviews, verifications and technical evaluations to develop and document negotiation objectives.

- In October 1989, Sandia awarded a $2 million sole-source contract (54-72197) to upgrade a computer system previously acquired in February 1987 (contract 02-6651). In its justification, Sandia maintained the system upgrade was needed because the existing system did not meet its demands and the level of service provided by the system was continuously degrading. Specifically, they maintained the existing system had severe limitations in terms of processor speed and memory. However, Sandia did not have adequate support for their assertions about capacity and response time problems. Little data on utilization and response times was available on the existing system. Also, the vendor, in its proposal, indicated that it could not provide support for exemption from submission of certified cost or pricing data; yet, Sandia granted an exemption and awarded the contract to the vendor.

- In September 1988, Sandia awarded a $600,000 sole-source contract (75-4148) for a supercomputer system to a vendor despite the existence of other vendors who could have provided a similar system. In its justification, Sandia pointed out that the "Connection Machine (CM-2) is the only commercially available general purpose system designed to support the variety of problems that will be investigated in the research." No audit review or verification was performed to ensure that the vendor qualified for exemption from submitting the cost or pricing data needed to evaluate price reasonableness and fairness. Moreover, the implementation

plan did not address important topics, such as (1) the acquisition's role in support of Sandia's research mission; (2) how the acquisition should be configured to most effectively complement other Sandia systems in meeting Sandia's diverse computing needs; and (3) capacity management activities including the present and projected work loads.

- In February 1987, Sandia awarded a $980,000 sole-source contract (02-6651) for a supercomputer system without advisory audit review or verification prior to negotiations. Audit verification would have shown that the vendor did not qualify for an exemption that was granted from submission of the certified cost or pricing data necessary to determine fairness and reasonableness of the vendor's proposed price. Sandia also pronounced as part of its sole source justification:

  > "We are funding a small research effort at Cal Tech which is investigating algorithm implementation on hypercubes. They have recently purchased an NCUBE machine, which they are using to develop some of their algorithms. They have agreed to share all of their software developed for the NCUBE with us."

  This represented insufficient basis to: (1) support the need for procurement and (2) preclude giving ample consideration to two other potential vendors.

Overall, the contract files did not contain sufficient evidence to support and document the performance of adequate analyses by Sandia to determine the reasonableness of vendor's proposals and the justification for sole-source procurement. Certified cost and pricing data was not obtained from vendors when necessary; advisory audit reviews and verifications were not sought from Government or internal sources; and sufficient weight was not given to the importance of advisory audits and technical reviews or verification in developing and documenting negotiation objectives. This increased the likelihood that more funds than necessary were paid by Sandia for mainframe computing resources.

COMPUTER SECURITY PROGRAM

Because of control weaknesses, Sandia's computer security programs did not adequately ensure the protection, integrity and confidentiality of classified and sensitive information stored on its computer systems. Our conclusions were based on a review of the security controls for nine computer systems at the Sandia Albuquerque and Livermore locations. Five of these systems were used for processing classified data and four were used for processing unclassified data. One of these systems was deemed mission essential to Sandia. We found that specific deficiencies existed in the areas of (1) access controls and technical safeguards, (2) operating system controls, (3) password administration, (4) organizational controls and audit trails, and (5) computer security and contingency planning. The specific computer security control weaknesses for these nine systems are described below for each of the major areas we reviewed (see page B-5 for a summary of weaknesses by system).

Access Controls and Technical Safeguards

Sandia employees were granted access, to computer systems that stored and processed classified and sensitive data, in excess of what was necessary for them to perform their job functions. An analysis of user accounts on the nine sampled computer systems revealed that nearly 35 percent of these accounts had not been accessed in over a six month period:

INACTIVE ACCOUNTS

System Number	Total Number of Accounts	Inactive for At Least 6 Months	Percent Inactive
1	289	127	43.9
2	446	221	49.6
3	249	120	48.2
4	299	169	56.5
5	236	90	38.1
6	203	77	37.9
7	193	23	11.9
8	43	9	20.9
9	3,178	957	30.1
Total	5,136	1,793	34.9

The analysis also revealed that almost 50 percent of the 1,793 inactive accounts had never been accessed by the users.

Interviews of a sample of 56 employees with inactive user accounts disclosed that 31, or 55 percent, no longer needed access privileges due to changes in job responsibilities. Six of these employees stated they never needed the access that was granted to

Sandia computer systems. During the audit, Sandia had taken steps to better monitor computer system access. One of these steps was notification to users that account status required updating to maintain login privileges and account activation.

Elevated levels of access privilege (i.e., the ability to perform all computer-related functions, such as read, write, delete, etc.), were granted to an excessive number of user accounts on the computer systems, thereby diminishing control over access to classified and sensitive data. For example, on one classified system, 36 user accounts were granted the highest levels of access privilege. Of the 36 accounts, three had not been used within the past three months, nine had not been used in six months, and one account had never accessed the system. On an unclassified system, 28 user accounts were granted elevated levels of access privilege. Of these 28 accounts, three had not been used in three months, eight had not been used in six months, and three had never accessed the system.

We also noted that some of the systems lacked technical safeguards to control access to classified and unclassified information. Users of three unclassified systems were not terminated after 60 minutes of inactivity, and users of a classified system were not terminated after 30 minutes of inactivity. The lack of this control feature could increase the opportunity for an unauthorized individual to gain access to classified or sensitive data on an unattended terminal.

Operating System Controls

Controls were not adequate to prevent unauthorized changes to features in Sandia's computer operating systems. Operating system programs, when programmed to do so, could circumvent security mechanisms, obliterate audit trails, or perform other debilitating actions. Restricting access to these sensitive areas of the operating system, which controls operations of the computer itself, is essential to maintaining systems integrity. However, Sandia did not restrict access to these operating system programs and features on three of the nine computer systems we reviewed, thus, increasing the possibility that unauthorized changes could be made to the operating system and sensitive programs. Although only two system programmers were responsible for maintaining the operating systems, and associated sensitive program libraries, for one unclassified and two classified computer systems, the number of users with "read" and "write" capabilities ranged from 10 to 3495. The "read" capability to sensitive program libraries allows users to scan existing programs and perhaps find programs that would allow them to circumvent normal security procedures and controls.

On two of the aforementioned systems (one classified and one unclassified), the operating system parameters allowed programs to be exempted from security process monitoring features when run

from sensitive program libraries. Hence, Sandia neither accounted for access to these libraries nor possessed the capability to detect the insertion of unauthorized program code.

Use of unrestricted supervisor calls was allowed on three of the aforementioned systems reviewed, thus, creating a potential integrity exposure to the computer operating systems. These operating system features could allow an individual an opportunity to access authorized program library members without detection. Sandia allowed 60 users unrestricted access to 62 supervisor calls on the three systems.

Password Administration

Although Sandia employed passwords to control system access, password systems were not properly administered to provide for continuing protection against unauthorized system access. On three systems, more than one person had identical passwords for access to classified and sensitive data. Also, passwords were not changed frequently enough to provide for continuing protection of system programs and data. On five systems processing classified data passwords were not changed within six months, as recommended by DOE Order 5639.6.

Organizational Controls and Audit Trails

Better separation of duties and responsibilities and better audit trails are needed in order to ensure adequate protection of classified and sensitive data. The previously described weaknesses in operating system controls and password administration, combined with inadequate separation of duties, lessened the effectiveness of existing system security measures and prevented the creation of reliable audit trails. This condition increased the opportunity for unauthorized access to modify or destroy data, and prevented individual accountability for system use.

At one site, computer system operators had the ability to override and modify established controls. Also, employees assigned responsibility for monitoring classified systems at both sites had other conflicting duties and responsibilities. These employees served as both security officers and systems administrators. Thus, these employees had the capability to add, modify, or delete classified security files without review by other person(s).

Without reliable audit trails, Sandia security administration personnel cannot effectively monitor computer data use and security features regulating system integrity. Also, two classified computer systems neither notified users of their last successful nor any unsuccessful attempts to gain access to their user accounts. Users of two other systems, one being classified, were not notified of unsuccessful login attempts to their accounts. Thus, users of these systems would have no means of

knowing if someone was using or attempting to guess their user ID and password.

Computer Security and Contingency Planning

In some cases, Sandia's computer security plans were outdated and not reflective of modifications or adjustments to hardware and software configurations and locations. For example, a Cray supercomputer was transferred to Albuquerque from Livermore without a modified security plan to reflect this change. Also, two IBM mainframe computers comprising the Common File System were replaced with Convex computers without this modification being reflected in the security plan. In addition, OSE inspection reports noted that Sandia did not have adequate security plans. However, an ALO security official stated that updated computer security plans for the aforementioned Cray Computer and Common File System were approved in May 1994.

At Sandia's Livermore facility, contingency plans were not adequately developed or maintained to provide reasonable continuity of data processing support should events, such as an earthquake, occur to prevent normal operations. Plans did not sufficiently identify critical applications to be processed and essential functions to be performed in the event of a disaster. Also, contingency plans had not been tested at Livermore to ensure workability. According to an Oakland official, a new contingency and disaster recovery plan was approved by ALO for the Central Computing Facility at Sandia-Livermore in January 1994.

SECURITY WEAKNESSES	COMPUTER SYSTEMS 1	2	3	4	5	6	7	8	9
Access Controls and Technical Safeguards									
Inactive User Accounts	X	X	X	X	X	X	X	X	X
Excessive or Elevated Access Privileges	X	X							
Untimely or No Automatic Logoff From Inactivity	X			X	X	X			
Operating System Controls									
Unrestricted Access to Operating System and Program Libraries							X	X	X
Operating System Parameters with Security Bypass Attributes							X		X
Use of Supervisor Calls Not Restricted							X	X	X
Password Administration									
Password Confidentiality Not Maintained				X	X	X			
Recommended Password Life Exceeded		X	X			X	X	X	
Organizational Controls and Audit Trails									
Inadequate Separation of Duties	X	X			X	X	X	X	X
Users Not Notified of Last Logon Attempt					X	X	X	X	

IG Report No. AP-B-95-01

CUSTOMER RESPONSE FORM

The Office of Inspector General has a continuing interest in improving the usefulness of its products. We wish to make our reports as responsive as possible to our customers' requirements, and therefore ask that you consider sharing your thoughts with us. On the back of this form, you may suggest improvements to enhance the effectiveness of future reports. Please include answers to the following questions if they are applicable to you:

1. What additional background information about the selection, scheduling, scope, or procedures of the audit or inspection would have been helpful to the reader in understanding this report?

2. What additional information related to findings and recommendations could have been included in this report to assist management in implementing corrective actions?

3. What format, stylistic, or organizational changes might have made this report's overall message more clear to the reader?

4. What additional actions could the Office of Inspector General have taken on the issues discussed in this report which would have been helpful?

Please include your name and telephone number so that we may contact you should we have any questions about your comments.

Name_____ Date_____

Telephone_____ Organization_____

When you have completed this form, you may telefax it to the Office of Inspector General at (202) 586-0948, or you may mail it to:

Office of Inspector General (IG-1)
Department of Energy
Washington, D.C. 20585
ATTN: Customer Relations

If you wish to discuss this report or your comments with a staff member of the Office of Inspector General, please contact Rob Jacques at (202) 586-3223.