U.S. DEPARTMENT OF ENERGY
OFFICE OF INSPECTOR GENERAL

AUDIT OF SELECTED ASPECTS OF THE UNCLASSIFIED COMPUTER SECURITY PROGRAM AT A DOE HEADQUARTERS COMPUTING FACILITY

The Office of Inspector General wants to make the distribution of its reports as customer friendly and cost effective as possible. Therefore, this report will be available electronically through the Internet five to seven days after publication at the alternative addresses:

Department of Energy Headquarters Gopher
gopher.hr.doe.gov

Department of Energy Headquarters Anonymous FTP
vm1.hqadmin.doe.gov

U.S. Department of Energy Human Resources and Administration
Home Page
http://www.hr.doe.gov/refshelf.html

Your comments would be appreciated and can be provided on the Customer Response Form attached to the Report.

Report Number: AP-B-95D02
Date of Issue: July 31, 1995

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

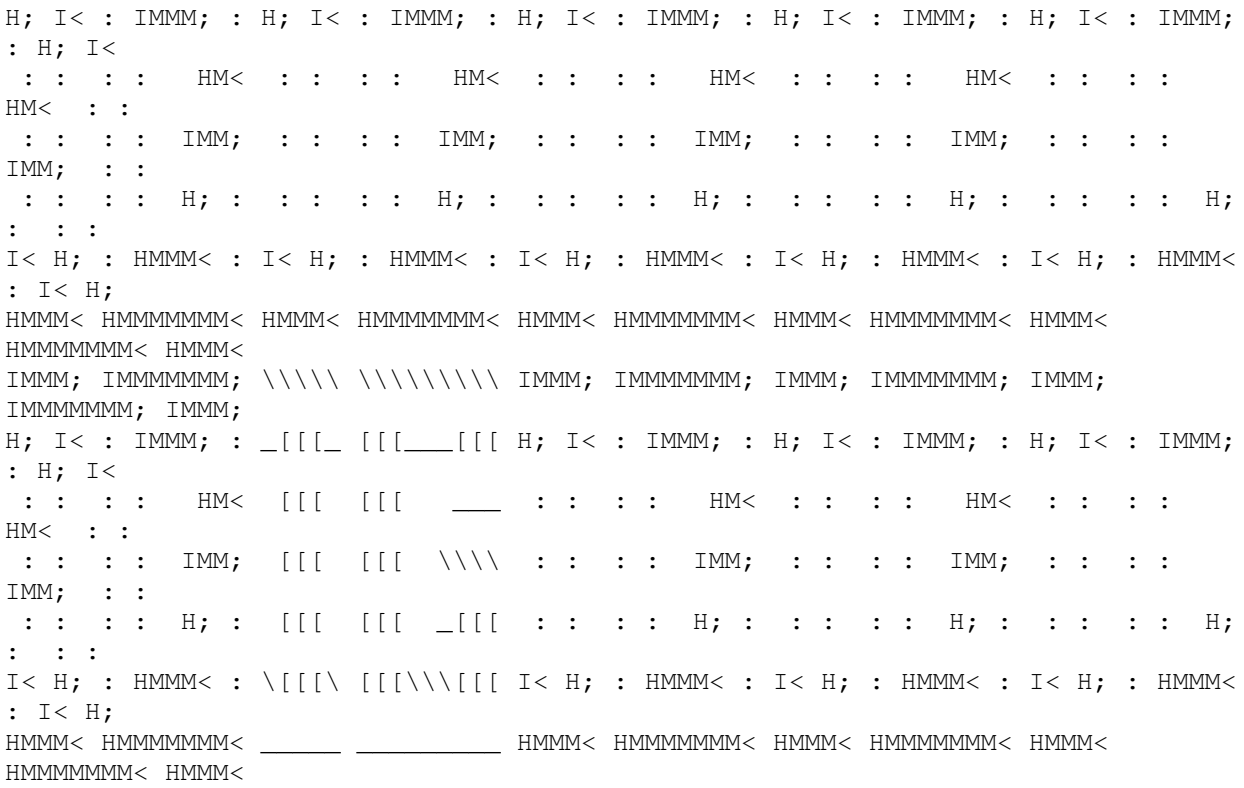
DDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD
D
REPORT NO.   U.S. DEPARTMENT OF ENERGY   RELEASE
DATE
                         OFFICE OF INSPECTOR GENERAL

AP-B-95-02   July 31,
1995

AUDIT OF SELECTED ASPECTS OF THE UNCLASSIFIED COMPUTER

SECURITY PROGRAM AT A DOE HEADQUARTERS COMPUTING FACILITY

ZDDD? ZDDDDDDD? ZDDD? ZDDDDDDD? ZDDD? ZDDDDDDD? ZDDD? ZDDDDDDD? ZDDD?
ZDDDDDDD? ZDDD?
@? ZY 3 ZDDD? 3 @? ZY 3 ZDDD? 3 @? ZY 3 ZDDD? 3 @? ZY 3 ZDDD? 3 @? ZY 3 ZDDD?
3 @? ZY
 3 3 3 3   @DY 3 3 3 3   @DY 3 3 3 3   @DY 3 3 3 3   @DY 3 3 3 3
@DY 3 3
 3 3 3 3 ZDD? 3 3 3 3 ZDD? 3 3 3 3 ZDD? 3 3 3 3 ZDD? 3 3 3 3
ZDD? 3 3
 3 3 3 3 @? 3 3 3 3 3 @? 3 3 3 3 3 @? 3 3 3 3 3 @? 3 3 3 3 3 @?
3 3 3
ZY @? 3 @DDDY 3 ZY @? 3 @DDDY 3 ZY @? 3 @DDDY 3 ZY @? 3 @DDDY 3 ZY @? 3 @DDDY
3 ZY @?
@DDDY @DDDDDDDY @DDDY @DDDDDDDY @DDDY @DDDDDDDY @DDDY @DDDDDDDY @DDDY
@DDDDDDDY @DDDY
IMMM; IMMMMMMM; IMMM; IMMMMMMM; IMMM; IMMMMMMM; IMMM; IMMMMMMM; IMMM;
IMMMMMMM; IMMM;



AUDIT OF SELECTED ASPECTS OF THE UNCLASSIFIED COMPUTER SECURITY PROGRAM AT A DOE HEADQUARTERS COMPUTING FACILITY

TABLE OF CONTENTS

			Page
		SUMMARY	1
PART I	-	APPROACH AND OVERVIEW	2
		Introduction	2
		Scope and Methodology	2
		Background	3
		Observations and Conclusions	4
PART II	-	FINDING AND RECOMMENDATIONS	6
		Unclassified Computer Security Program at a DOE Headquarters Computing Facility	6

PART III D MANAGEMENT AND AUDITOR COMMENTS 13

U.S. DEPARTMENT OF ENERGY
OFFICE OF INSPECTOR GENERAL
OFFICE OF AUDIT SERVICES

AUDIT OF SELECTED ASPECTS OF THE UNCLASSIFIED COMPUTER SECURITY PROGRAM AT A DOE HEADQUARTERS COMPUTING FACILITY

Audit Report Number: AP-B-95-02

SUMMARY

The purpose of this audit was to evaluate the effectiveness of the unclassified computer security program at the Germantown Headquarters Administrative Computer Center (Center). The Department of Energy (DOE) relies on the application systems at the Germantown Headquarters Administrative Computer Center to support its financial, payroll and personnel, security, and procurement functions. Our review was limited to an evaluation of the administrative, technical, and physical safeguards governing utilization of the unclassified computer system which hosts many of the Department's major application systems.

Our audit identified weaknesses in the Center's computer security program that increased the risk of unauthorized disclosure or loss of sensitive data. Specifically, we found that (1) access to sensitive data was not limited to individuals who had a need for the information, and (2) accurate and complete information was not maintained on the inventory of tapes at the Center. Furthermore, the risk of unauthorized disclosure and loss of sensitive data was increased because other controls, such as physical security, had not been adequately implemented at the Center.

Management generally agreed with our audit conclusions and recommendations, and initiated a number of actions to improve computer security at the Center.

PART I

APPROACH AND OVERVIEW

INTRODUCTION

The Department relies on the application systems at the Center to support its financial, payroll and personnel, security, and procurement functions. At the time of our audit fieldwork, the Center was managed and operated by The Office of Information Technology Services and Operations (ITSO). In November 1994, subsequent to the completion of our fieldwork, ITSO's computer

security functions were transferred to the Systems Engineering Group under the Deputy Assistant Secretary for Information Management.

The objective of our audit was to evaluate the effectiveness of the unclassified computer security program at the Center. Specific objectives included determining whether (1) computer security procedures and practices adequately protected sensitive data from unauthorized disclosure or loss, and (2) a contingency plan had been developed that provided reasonable assurance of the continuity of data processing support should events occur that prevent normal operations.

SCOPE AND METHODOLOGY

The audit was performed primarily at Departmental facilities in Germantown, Maryland, with most of our fieldwork conducted between February 1994 and October 1994. Our review was limited to an evaluation of the administrative, technical, and physical safeguards governing utilization of the unclassified IBM computer system which hosts many of the Department's major application systems. A separate report will be issued on controls for the classified system at the Center.

We examined (1) ITSO's plans and procedures for protecting unclassified sensitive data and operations, and (2) reports by the Office of Security Evaluations and the Office of Information Resource Management Policy, Plans, and Oversight. We interviewed program managers and staff in Departmental Headquarters to discuss the adequacy of computer security controls, monitoring, and training. We also inspected ITSO's contractor-operated backup media storage facility and interviewed contractor and ITSO personnel to discuss security and contingency issues.

The audit was performed according to generally accepted Government auditing standards for performance audits and included tests of internal controls and compliance with laws and regulations to the extent necessary to meet the objectives of the audit. We assessed the significant internal controls with respect to the unclassified security program at the Center. Our assessment consisted of reviewing the administrative, technical, and physical safeguards governing use of the unclassified IBM computer system. Because our review was limited, it would not necessarily have disclosed all internal control deficiencies that may have existed at the time of our audit.

An exit conference was held with management officials from the Office of Information Management on May 16, 1995.

BACKGROUND

The Office of Information Technology Services and Operations (ITSO), under the Deputy Assistant Secretary for Information Management, has responsibility for managing and operating the Headquarters classified and unclassified computer-based data processing facilities, including the Center. Its functions include (1) identifying mission-supportive information processing

opportunities for DOE Headquarters offices, (2) managing information technology resource planning for DOE Headquarters, and (3) developing and maintaining DOE-wide classified and unclassified information systems under the responsibility of Headquarters organizations. In November 1994, subsequent to the completion of our fieldwork, ITSO's computer security functions were transferred to the Systems Engineering Group under the Deputy Assistant Secretary for Information Management.

The Center is the Department's central administrative processing facility. According to ITSO's October 1994 records, the Center had computer processing equipment with an estimated cost of about $6.6 million. At the Center, ITSO operates three IBM computers that service the administrative computing needs of the Department's Headquarters and field users nation-wide. One computer is used for processing many of the Department's mission-essential application systems. Another is used to support a large number of users with file transfer, electronic mail, and scheduling functions. The third computer is used for processing classified data. The Center also has Hewlett-Packard computers which support the processing of accounting and financial data.

According to ITSO, about 3,600 users, of which 45 percent were contractors, were provided access to the IBM computer system dedicated to processing the Department's mission-essential applications. These users can access the applications on the unclassified system through dial-up or hardwired terminals. In addition to providing computer processing time, ITSO offers other end-user computing services, including computer training and microcomputer repair.

The following major Department application systems were processed on the unclassified system at the Center.

- The Financial Information System (FIS), which is the official source of consolidated financial information for the Department;
- The DOE Integrated Payroll/Personnel System (PAY/PERS), which supports both personnel and payroll activities throughout the Department;
- The DOE Integrated Security System (DISS), which provides tracking capabilities for security clearances, visitor information for DOE facilities, and security badge accountability;
- The Energy Manpower Personnel Resource Information System, which supports the Department's human resource management and manpower resource planning, budgeting, and accounting activities; and
- The Procurement and Assistance Data System, which provides the Assistant Secretary for Human Resources and Administration with the ability to track and report on procurement and assistance actions throughout the Department.

ITSO had employed various tools and techniques to manage the Center. As part of its computer security program, security software was installed on the IBM computer processing the Department's major application systems. Through use of the security software, ITSO had implemented two measures--user identifications (userid) and passwords--intended to protect these applications from unauthorized access, fraud, and abuse. In addition, a tape management system was installed to manage and report on magnetic media (i.e., tape reels and cartridges). In May 1992, ITSO conducted a risk analysis of the Center. In November 1992, ITSO developed a disaster recovery plan intended to identify the mission essential applications that should be maintained if the Center's operations were unexpectedly interrupted.

OBSERVATIONS AND CONCLUSIONS

Weaknesses existed in the computer security program at the Center that increased the risk of unauthorized disclosure or loss of sensitive data. Specifically, we found that (1) access to sensitive data was not limited to individuals who had a need for the information, and (2) accurate and complete information was not maintained on the inventory of tapes at the Center. Furthermore, the risk of unauthorized disclosure and loss of sensitive data was increased because other controls, such as physical security, had not been adequately implemented at the Center. For example, a disaster recovery plan had not been fully implemented to mitigate the consequences caused by an unexpected loss of computer systems and data that support critical Department operations.

These weaknesses existed because ITSO had not fully performed an assessment of risk at the Center and the controls in place to mitigate these risks, and computer security officers did not adequately monitor activities on the unclassified computer system in accordance with computer security requirements. The weaknesses in general controls over computer security of the Center's unclassified system increased the risk of unauthorized disclosure and/or loss of sensitive data, and diminished the reliability of the Department's financial management information that resides at the Center.

During our audit, positive steps were taken to improve the unclassified computer security program at the Center. Management took action to (1) reduce the number of user accounts with broad access privileges and (2) validate access to tape data sets through implementation of the security software feature. Controls were instituted to ensure that the tape management system accurately reflected the disposition of magnetic media. In addition, management took action to reduce the number of persons who had unrestricted physical access to the Center, including the tape library housing sensitive data.

Individually, the computer security weaknesses identified in this report may not represent material deficiencies in the Center's computer security program. However, when considered together, they represent internal control weaknesses that should

be considered by management when preparing its yearend assurance memorandum on internal controls.

PART II

FINDING AND RECOMMENDATIONS

Unclassified Computer Security Program at a DOE Headquarters Computing Facility

FINDING

An effective computer security program requires the development and implementation of adequate controls to ensure that sensitive data processed on computer systems is protected from unauthorized disclosure and/or loss and that potential risks relating to this data are identified and mitigated to the extent practical. Weaknesses existed in the Center's unclassified computer security program that increased the risk of unauthorized disclosure or loss of sensitive data. These weaknesses occurred because (1) ITSO had not fully performed an assessment of risks on the unclassified computer system and the controls in place to mitigate those risks, and (2) computer security officers did not adequately monitor activities on the unclassified computer system in accordance with computer security requirements. Weaknesses in general controls over the computer security of the Department's unclassified system increased the risk of unauthorized disclosure and/or loss of sensitive data, and diminished the reliability of the Department's financial information.

RECOMMENDATIONS

We recommend that the Deputy Assistant Secretary for Information Management:

1. Conduct a comprehensive risk analysis of the Center to assess the unclassified system's unique risks, as well as the adequacy of the administrative, technical, and physical controls to mitigate those risks and to protect sensitive data.

2. Ensure that security officers monitor activities on the unclassified system and in the program, and take appropriate actions to bring the program into compliance with sound data processing practices, especially to

    a. limit access authorization for the unclassified computer system to only those computer programs and data that individuals need to perform their duties and periodically review these authorizations to ensure that they remain appropriate;

    b. reflect the accurate location and disposition of magnetic media in the tape management system;

    c. document changes to operating system software;

    d. provide adequate physical security safeguards to

limit access to computing resources and protect against fire; and

e. fully implement an up-to-date disaster recovery plan for the Center to mitigate the consequences caused by an unexpected loss of use of computer systems and data.

MANAGEMENT REACTION

Management agreed, in principle, with our audit finding and recommendations, and identified actions planned or implemented to improve computer security at the Center. See Part III of this report for further discussion of management's comments.

DETAILS OF FINDING

GUIDANCE FOR COMPUTER SECURITY

An effective computer security program requires the development and implementation of adequate controls to ensure that sensitive data processed on computer systems is protected from unauthorized disclosure and/or loss, and that potential risks relating to this data are identified and mitigated to the extent practical. Guidance on the controls to be implemented by Federal and Departmental organizations are set forth in various documents issued by the Congress, the National Institute of Standards and Technology (NIST), the Office of Management and Budget (OMB), and the Department.

The Computer Security Act of 1987 (Public Law 100-235) was passed by the Congress to improve security over sensitive Federal computer systems. The Act assigns responsibility to NIST for developing standards and guidelines needed to ensure the cost-effective security and privacy of sensitive information in Federal computer systems. NIST has issued Federal Information Processing Standards (FIPS Pubs) as guidance to Federal agencies in the management and security of Federal automated information systems. FIPS Pubs containing guidance for computer security issues include FIPS Pub 31, "Guidelines for Automatic Data Processing Physical Security and Risk Management," issued June 1974; FIPS Pub 65, "Guidelines for Automatic Data Processing Risk Analysis," issued August 1, 1979; FIPS Pub 73, "Guidelines for Security of Computer Applications," issued June 30, 1980; FIPS Pub 87, "Guidelines for ADP Contingency Planning," issued March 27, 1981; and FIPS Pub 112, "Password Usage," issued May 30, 1985.

OMB Circular A-130, Appendix III, "Security of Federal Automated Information Systems," establishes a minimum set of controls to be included in Federal automated information systems security programs. This Circular states that agencies shall assure an adequate level of security for all agency information systems, whether maintained in-house or commercially, and shall implement and maintain a computer security program, including the preparation of policies, standards, and procedures. OMB Bulletin 90-08, "Guidance for Preparation of Security Plans for Federal

Computer Systems That Contain Sensitive Information," also provides guidance to Federal agencies on computer security planning activities required by the Computer Security Act of 1987.

Departmental policies and procedures governing unclassified computer security are addressed in DOE Order 1360.2B, "Unclassified Computer Security Program." This Order establishes requirements, policies, responsibilities, and procedures for developing, implementing, and sustaining an unclassified computer security program. For example, the Order states that DOE managers are required to designate an individual to be the Computer Protection Program Manager (CPPM). The CPPM may designate assistant CPPMs to accomplish specific security responsibilities. The Order further states that the CPPM shall implement and administer a management control process to ensure that appropriate administrative, technical, physical, and personnel protection measures are incorporated into all new and operational unclassified computer systems. The Order also states that the CPPM shall develop and implement procedures establishing controls designed to prevent misuse and abuse of unclassified computer resources.

WEAKNESSES IN THE COMPUTER SECURITY PROGRAM AT THE CENTER

Weaknesses existed in the Center's unclassified computer security program that increased the risk of unauthorized disclosure or loss of sensitive data. Specifically, we found that (1) access to sensitive data was not limited to individuals who had a need for the information, and (2) accurate and complete information was not maintained on the inventory of tapes at the Center. Other controls, such as physical security, had not been adequately implemented to protect sensitive data and computing resources.

System Access

ITSO's computer security program did not ensure that access to sensitive data was limited to individuals who had a need for the information. Specifically, we found that:

- Computer support personnel had broad system access privileges which allowed them access to operating and application system files, as well as sensitive data sets. Such broad access privileges exceeded that which the individuals typically needed to perform their job functions, and increased the risk that an individual could copy, modify, or destroy any data set in the system, or create or change access rules and execute restricted programs.

- Non-unique identifiers were established that allowed unlimited access to the unclassified system. Such broad access through non-unique identifiers increased the risk that an individual could copy, modify, or destroy any data set in the system, or access restricted programs without being detected and having their access privilege

revoked.

- Terminated contractor employees maintained access privileges.

- Access privileges were maintained for inactive user accounts that had not been accessed in over 6 months.

- Individuals were using other people's passwords for convenience.

We found that technical safeguards were not in place that would lessen the risk of unauthorized disclosure of sensitive data. Access to data sets on tape was not validated by the security software. Batch jobs did not have to be validated by the security software to ensure that the user was authorized to carry out this function. Users were also allowed to enter the system through batch processing without providing a password.

Tape Management

ITSO did not maintain accurate and complete information on the inventory of tapes at the Center. As of March 7, 1995, the Center's tape management system showed there were about 14,500 reels of tape. However, we observed on March 8, 1995, that the Center had only approximately 1,900 reels of tape in its inventory. According to Center personnel, (1) the tape management system was not being modified to reflect the degaussing and destruction of tapes; (2) documentation was not being maintained on destroyed tapes; and (3) there was no formal inventory performed of tapes.

Other Controls

Other controls had not been adequately implemented at the Center. These conditions increased the risk of unauthorized disclosure and/or loss of sensitive data. Specifically, we found that:

- Weaknesses existed in the management and use of the computer operating system. An ITSO official acknowledged that they did not fully document the changes made to system software. In the operating system, we identified 19 commands and 5 programs that were unrecognized on the listing of authorized operating system entries. Authorization for operating system commands and programs is critical because entries can be used to bypass system validity checks and security.

- Physical security measures did not adequately limit access to computing resources or fully protect against fire. Contrary to Federal guidance, various persons who should not have had access to the tape library held card keys, including sixteen systems programmers. Although the room adjacent to the Center was used to store combustible materials such as paper and office supplies, it did not have a smoke detection system.

- Although ITSO had a disaster recovery plan, it had not been fully implemented to mitigate the damaging potential consequences caused by the unexpected loss of use of computer systems and data that support critical Departmental operations. Backup tapes for all data and programs necessary to continue operations were not maintained at an offsite storage facility. In its November 1992 disaster recovery plan, ITSO designated 14 application systems as "mission-essential." According to ITSO records, backup tapes were stored off-site for only 6 of these applications. Furthermore, a complete set of documentation for each mission critical application was not kept in an off-site storage facility in order to facilitate its retrieval in case of need. In September 1994, ITSO negotiated a formal agreement for disaster recovery services for its mainframe and minicomputers. According to management, a test of the plan will be conducted in September 1995 to ensure that appropriate steps have been taken to provide for contingency operations should the Center be unable to operate.

We also noted that computer operator intervention was not restricted during the operating system initialization process. The acting Center manager told us that computer operator intervention was needed to facilitate proper maintenance of the Center's computers. However, he agreed that the risk of inappropriate activity could be reduced by reviews of the access activities of these employees.

%PAGES
REASONS FOR WEAKNESSES IN THE COMPUTER SECURITY PROGRAM

The weaknesses in the computer security program at the Center occurred because (1) ITSO had not fully performed an
%PAGEE
assessment of risks on the unclassified computer system and the controls in place to mitigate those risks, and (2) computer security officers did not adequately monitor activities on the unclassified computer system in accordance with computer security requirements.

Security Planning

ITSO had not fully performed an assessment of the risk of unauthorized disclosure or loss of sensitive data and the controls in place to mitigate such risks on the unclassified system. DOE Order 1360.2B, "Unclassified Computer Security Program," requires that the applicable Computer Protection Program Manager formulate a computer protection plan. The plan must be kept current and include certain elements, such as (1) a summary of the management control process describing the administrative, technical, and personnel safeguards employed at the site; (2) reference to lists that identify unclassified computer applications that process sensitive information, the owners of such applications, and the unclassified computer systems which provide processing support; and (3) reference to schedules

indicating planned and completed risk assessments.

Although ITSO had developed a computer protection plan, it had not conducted a comprehensive risk assessment of the unclassified system in order to identify the unique risks that existed with the system. Furthermore, the plan did not adequately cover the technical and physical safeguards employed to mitigate these unique risks and protect the sensitive data at the Center.

Security Management

Officials assigned to carry out computer security functions were not adequately monitoring activities on the unclassified computer system at the Center. The Headquarters' Computer Protection Plan assigns responsibility to the CPPM for developing and managing the Headquarters computer protection program. Assistant CPPMs are assigned to assist the CPPM in implementing the program. The Plan required security officers to ensure the implementation of a continuous audit, monitoring and review process to identify waste, fraud, abuse and unauthorized activity in the access and use of computer resources.

While a review process was implemented, it was not sufficient for monitoring activities on the unclassified system. The formal report on system activities highlighted unsuccessful attempts to access the system. However, security officials told us that they did not routinely conduct formal monitoring or reporting of system activities, such as reviewing the actions of individuals granted broad system access privileges.

%PAGES
IMPACT OF WEAKNESSES

Weaknesses in general controls over the computer security of the Department's unclassified system increased the risk of %PAGEE unauthorized disclosure and/or loss of sensitive data and diminished the reliability of the Department's financial management information. In particular, the access allowed for terminated contract employees and the existence of non-unique identifiers on the unclassified system heightened the opportunity for unauthorized use, and diminished security officers' ability to identify who had gained access to what data. Additionally, the inaccurate accounting for tapes increased the opportunity for loss of data. Computer operations were also at risk because ITSO had not taken the steps to ensure that computer support for critical mission activities could be continued should disasters or major service disruptions occur.

Individually, the computer security weaknesses identified in this report may not represent material deficiencies in the Center's computer security program. However, the weaknesses identified, collectively, provide an environment in which individuals could exploit those weaknesses to obtain unauthorized access to sensitive data, including that for many of the Department's major financial management systems.

MANAGEMENT AND AUDITOR COMMENTS

Management agreed, in principle, with our audit finding and recommendations, and identified corrective actions planned or implemented to improve computer security at the Center.

Recommendation 1.

Management Comments. Management indicated that a risk assessment, as defined by DOE Order 1360.2B, was performed on the computer installation of which the unclassified processor is a part. Because of their co-location, management believed that the unclassified processors enjoyed a majority of the same administrative, technical, and physical controls afforded to the classified processor. However, a risk assessment will be performed of the unclassified system as part of the process of reaccreditation of the classified processor. This process will include a review of physical security controls, technical safeguards and administrative controls as these pertain to the unclassified operating system based environment, and should be completed by December 1995.

Auditor Comments. Management's comments are responsive to our recommendation.

Recommendation 2.a.

Management Comments. Management identified a number of actions planned or taken to improve system access controls. The number of user accounts with broad access privileges has been reduced, and access to tape data sets through implementation of the security software feature is now validated. Also, a process of removing generalized, non-privileged access to the unclassified processors, where an access ID has not been used for 15 consecutive months, will be initiated. This process will be fully operational by October 1995. Management further stated that a refined access monitoring and reporting is currently being engineered. This process will concentrate on monitoring and reporting the data access of the personnel with privileged access authorities. This refined monitoring and report process should be fully operational by November 1995. Management also noted that users of the unclassified processors will be reminded annually that the use of their access ID and password combination should be controlled and not shared with other users.

Auditor Comments. Management's comments are responsive to our recommendation.

%PAGES
Recommendation 2.b.

Management Comments. Management indicated that a number of actions have been planned or taken to improve the tape management
%PAGEE
system. In June 1995, the system was modified to clearly identify the disposition of destroyed tapes. An engineering

effort, scheduled for completion by August 1995, is being performed to affect the recording within the tape management system of the media stored offsite. Also, an inventory methodology, based upon exceptions, will be developed and fully operational by October 1995. This methodology will employ controls within both the "Tape Robotics and Tape Management Systems" to report discrepancies between the media stored offsite, the locations of all known media and any differences (i.e., missing media) between these two known entities.

Auditor Comments. Management's comments are responsive to our recommendation.

Recommendation 2.c.

Management Comments. In its comments, management stated that several locally authorized and developed commands as well as utility functions had been introduced into the operating system. These commands and utility functions will be fully identified and documented by December 1995. Management also stated that other specific anomalies within the operating system will be evaluated for their effect on computer security and corrected as necessary to reinforce computer security controls.

Auditor Comments. Management's comments on planned actions appear to be responsive to our recommendation.

Recommendation 2.d.

Management Comments. In its comments, management expressed the belief that the Center is adequately protected against fire and has limited physical access due to the safeguards and countermeasures employed for the classified processor. However, in April 1995, management took action to request a smoke detector for the room, which was used to store combustible materials, adjacent to the Center. In June 1995, management completed a review of the current card key system to ensure that individuals with physical access needed such access in order to carry out their duties and responsibilities. Subsequent action was taken to reduce the number of individuals with unrestricted access to the Center.

Auditor Comments. Management comments on actions taken are responsive to our recommendation.

%PAGES
Recommendation 2.e.

Management Comments. In its comments, management noted that the Center had a disaster recovery plan which addressed the
%PAGEE
issues raised in our report, and that the plan was continually in the process of being updated. They also pointed out that a contract was initiated in September 1994 to provide "hot site" disaster recovery services from a contractor. According to management, this plan will be tested in September 1995. Management stated that they are "partnering" with the owners of

the fourteen "mission essential" application systems to obtain their participation in disaster recovery preparedness. In addition, every attempt will be made to have backup files and documentation for all the "mission essential" application systems in effect by January 1, 1996.

Auditor Comments. Management's comments are responsive to our recommendation. We have also amended our report to reflect the awarding of a contract for a "hot-site".

IG Report No. AP-B-95-02

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) 586D0948, 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) 586D3223.

□