Audit Report

OFFICE OF THE INSPECTOR GENERAL

GENERAL CONTROLS FOR COMPUTER SYSTEMS AT THE INFORMATION PROCESSING CENTERS OF THE DEFENSE INFORMATION SERVICES ORGANIZATION

Report No. 94-060 March 18, 1994

Department of Defense

Additional Copies

To obtain additional copies of this report, contact the Secondary Reports Distribution Unit, Audit Planning and Technical Support Directorate, at (703) 614-6303 (DSN 224-6303) or FAX (703) 614-8542.

Suggestions for Future Audits

To suggest ideas for or to request future audits, contact the Planning and Coordination Branch, Audit Planning and Technical Support Directorate, at (703) 614-1868 (DSN 224-1868) or FAX (703) 614-8542. Ideas and requests can also be mailed to:

Inspector General, Department of Defense
OAIG-AUD (ATTN: APTS Audit Suggestions)
400 Army Navy Drive (Room 801)
Arlington, Virginia 22202-2884

DoD Hotline

To report fraud, waste, or abuse, call the DoD Hotline at (800) 424-9098 (DSN 223-5080) or write to the DoD Hotline, The Pentagon, Washington, D.C. 20301-1900. The identity of writers and callers is fully protected.

Acronyms

ABENDS	Abnormal Endings
ADP	Automatic Data Processing
AFAFC	Air Force Accounting and Finance Center
AIS	Automated Information Systems
CMCS	Case Management Control System
DBMS	Defense Business Management System
DFAS	Defense Finance and Accounting Service
DDMS	Defense Debt Management System
DISA	Defense Information Systems Agency
DISO	Defense Information Services Organization
DLA	Defense Logistics Agency
FMFIA	Federal Managers' Financial Integrity Act
IBM	International Business Machines
IG	Inspector General
JSS	Joint Service Software
JSS-AC	Joint Service Software for Active Components
JSS-RC	Joint Service Software for Reserve Components
MOCAS	Mechanization of Contract Administration Services
OMB	Office of Management and Budget

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-2884

March 18, 1994

MEMORANDUM FOR DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY
DIRECTOR, DEFENSE FINANCE AND ACCOUNTING SERVICE

SUBJECT: Audit Report on General Controls for Computer Systems at the Information Processing Centers of the Defense Information Services Organization (Report No. 94-060)

We are providing this final report for your review and comments. It discusses matters concerning general controls at selected Defense Information Services Organization information processing centers that support the Defense Finance and Accounting Service and the Financial Systems Activity Directorate of the Defense Finance and Accounting Service, Denver Center. The Defense Information Systems Agency provided comments on the recommendations addressed to the Defense Information Services Organization. We also received comments from the Defense Finance and Accounting Service, Financial Systems Activity, Denver, Colorado. We considered the comments in preparing this final report.

DoD Directive 7650.3 requires that all recommendations be resolved promptly. Therefore, we request that the Defense Information Services Organization provide final comments by May 16, 1994. See the "Response Requirements for Each Recommendation" chart at the end of Findings A and C for the recommendations you must comment on and the specific requirements for your comments. If you concur, describe the corrective actions taken or planned, and give the completion dates for actions already taken and the estimated completion dates of planned actions. If you nonconcur, please state your specific reasons for each nonconcurrence. If appropriate, you may propose alternative methods for accomplishing desired improvements.

The courtesies extended to the audit staff are appreciated. If you have any questions about this audit, please contact Mr. David C. Funk, Program Director, at (303) 676-7445 (DSN 926-7445), or Mr. W. Andy Cooley, Project Manager, at (303) 676-7393 (DSN 926-7393). Appendix F lists the distribution of this report. The audit team members are listed inside the back cover.

David K. Steensma

David K. Steensma
Deputy Assistant Inspector General
for Auditing

Enclosure

Office of the Inspector General, Department of Defense

Report No. 94-060 March 18, 1994
(Project No. 2FD-2002)

AUDIT REPORT ON GENERAL CONTROLS FOR COMPUTER SYSTEMS AT THE INFORMATION PROCESSING CENTERS OF THE DEFENSE INFORMATION SERVICES ORGANIZATION

EXECUTIVE SUMMARY

Introduction. The Defense Information Services Organization (DISO)* provides information processing support to help the Defense Finance and Accounting Service (DFAS) prepare the financial statements required by the Chief Financial Officers Act of 1990. Our audits of the FY 1992 financial statements included an evaluation of the general controls at the information processing centers because weaknesses in those controls affect all computer applications. During FY 1992, the DISO information processing centers included in this audit processed over $133.6 billion in financial transactions.

Objectives. Our audit objective was to determine the adequacy of the general controls over the operations and protection of the DISO information processing centers at Columbus, Ohio (DISO-Columbus Center); Denver, Colorado (DISO-Denver Center); and Indianapolis, Indiana (DISO-Indianapolis Center). We also evaluated the internal controls applicable to the automatic data processing (ADP) environment at each DISO Center. In addition, at the DISO-Denver Center, we determined the adequacy of the general controls over the organization and management of the information processing center and over system design, development, and change controls.

Audit Results. At all three DISO Centers, the general controls over operations and protection of the information processing centers were generally adequate. However, opportunities existed for improving the general controls and related internal controls. At the DISO-Denver Center, we noted one deficiency in the general controls over organization and management of the information processing center. These conditions are summarized below.

o None of the DISO Centers effectively analyzed and followed up on abnormal endings to computer operations or provided adequate oversight for the maintenance of ADP equipment. As a result, computer operations were not efficiently managed, and the Government made excessive or inadequately supported payments for contract maintenance services. We could not determine the amount of excessive payments because of a lack of documentation (Finding A).

o At one or more DISO Centers, requirements were not met for evaluating computer security risks, performing and reporting on analyses of internal controls and related weaknesses, or centralizing control over information systems security. Consequently, material internal control weaknesses disclosed in prior audits were not reported in the Annual Statements of Assurance to DoD management and Congress, and inadequate oversight existed over the security of computer operations (Finding B).

---

* The Defense Information Technology Services Organization and its local information processing activities were reorganized effective September 7, 1993. They are referred to in this report by their new names, the Defense Information Services Organization and its information processing centers.

o Weaknesses existed at all three DISO Centers in the controls over access to computer assets (including application programs), thus increasing the risk of unauthorized access to those assets (Finding C).

o At two DISO Centers, known weaknesses existed in safeguards against fire and other environmental risks to computer assets. Thus, costly computer assets supporting vital operational and business computer applications were unnecessarily exposed to accidental or deliberate destruction (Finding D).

o Application program changes at the DISO-Denver Center were not always properly authorized and approved. Therefore, application programs used to process over $22.0 billion in FY 1992 business transactions were exposed to higher risk of fraud, waste, or abuse (Finding E).

Internal Controls. Inadequate controls existed over passwords to key computer applications at the DISO-Columbus Center and over changes made to certain application programs at the DISO-Denver Center. We consider these inadequate controls to be material internal control weaknesses as defined by Office of Management and Budget Circular No. A-123 and DoD Directive 5010.38. We did not evaluate the effectiveness of the implementation of the DoD Internal Management Control Program for the audit objectives. See Part I, "Internal Controls," and Part II, Findings C and E, for more details on the internal controls examined and our audit results.

Potential Benefits of Audit. We could not quantify the potential monetary benefits from implementing the corrective actions for specific internal control weaknesses. See Appendix D for a summary of the benefits resulting from this audit.

Summary of Recommendations. We recommended that DISO establish better control over abnormal endings to computer operations and maintenance of ADP equipment. We recommended improvements at individual DISO Centers in management oversight and reporting, computer security, and environmental protection. We recommended that the DFAS-Denver Center improve change control procedures and practices.

Management Comments. DISO agreed to improve the oversight of maintenance of ADP equipment and ADP security oversight, but did not agree that controls over abnormal endings to computer operations needed strengthening. The DISO-Columbus Center concurred with documenting the tests made of the physical security plan, but proposed an alternative to manual control of user passwords. The DISO-Denver Center did not agree that additional access controls were needed for individuals who have unescorted access to the computer room. The DISO-Denver Center and the DISO-Columbus Center agreed to improve the environmental protection at their location, but stated that certain improvements were not feasible or necessary. DFAS-Denver Center concurred with improving procedures and practices for software change controls.

Audit Response. Additional comments on this final report are required from DISO by May 16, 1994. A discussion of the responsiveness of management comments is in Part II of the report, and the complete text of the comments is in Part IV.

Table of Contents

Executive Summary i

Part I - Introduction 1

Background 2
Objectives 3
Scope and Methodology 4
Internal Controls 4
Prior Audits and Other Reviews 5

Part II - Findings and Recommendations 7

Finding A. Operational Improvements 8
Finding B. ADP Security Oversight 13
Finding C. Controls Over Access 17
Finding D. Environmental Protection 21
Finding E. Change Controls at the DISO-Denver Center 23

Part III - Additional Information 27

Appendix A. Major Automated Data Processing Systems of the Defense Information Services Organization 28
Appendix B. Physical Protection Improvements Needed at the DISO-Indianapolis Center 30
Appendix C. Statistical Sampling Plan and Results 31
Appendix D. Summary of Potential Benefits Resulting from Audit 35
Appendix E. Organizations Visited or Contacted 37
Appendix F. Report Distribution 38

Part IV - Management Comments 41

Defense Finance and Accounting Service 42
Defense Information Systems Agency 45

This report was prepared by the Financial Management Directorate, Office of the Assistant Inspector General for Auditing, DoD.

Part I - Introduction

Background

This audit was made in response to the Chief Financial Officers Act of 1990. The Act required that agency Inspectors General, or independent external auditors, audit Government financial statements. The statements should provide accurate, complete, and timely information to DoD, the Office of Management and Budget, and Congress. The Defense Information Services Organization (DISO)[1] is responsible for collecting, processing, accounting for, and storing financial data for the Defense Finance and Accounting Service (DFAS). Until DISO was established in May 1992, DFAS managed the DISO information processing centers at Cleveland and Columbus, Ohio; Denver, Colorado; Indianapolis, Indiana; and Kansas City, Missouri.

Major Financial Systems. Financial statements for FY 1992 were required for several DoD reporting entities, such as the Department of the Air Force, the Foreign Military Sales Trust Fund, and the Defense Business Operations Fund. Supplementing the audits of those statements, we examined the general controls for the information processing centers that processed the financial data used to prepare the statements. Major financial systems included in this audit are the Joint Service Software for Active Components (JSS-AC), Joint Service Software for Reserve Components (JSS-RC), and the Defense Debt Management System (DDMS).[2] As detailed in Appendix A, those major automated systems processed over $133.6 billion in military payrolls, contract payments, and other transactions during FY 1992.

Definition of General Controls. Unless other tests and procedures are applied, financial statement audits include an evaluation of the general and application controls at the information processing centers that provide data processing support for preparing financial statements. Such evaluations are made to determine the reliability of computer-processed data. General controls represent the structure, methods, and procedures of the overall computer operations in an organization. General controls are independent of the controls built into individual computer applications. General controls include the center's controls over its organization and management; system design, development, and maintenance; operations; protection (including backup and disaster recovery); hardware; and software. The effectiveness of those general controls must be considered when evaluating computer-based systems because weaknesses in general controls affect all applications processed. General control weaknesses at the DISO information processing centers could materially affect the accuracy, completeness, or timeliness of the financial statements prepared by DFAS.

---

[1] The Defense Information Technology Services Organization and its local information processing activities were reorganized effective September 7, 1993. They are referred to in this report by their new names, the Defense Information Services Organization and its information processing centers.

[2] The JSS-AC was formerly known as the Joint Uniform Military Pay System, and the JSS-RC was known as the Joint Uniform Military Pay System for Reserve Pay.

Objectives

Controls Over Operations and Protection. Our audit objective was to determine the adequacy of the general controls over the operations and protection of the DISO information processing centers at Columbus, Ohio (DISO-Columbus Center); Denver, Colorado (DISO-Denver Center); and Indianapolis, Indiana (DISO-Indianapolis Center). Specifically, at each DISO Center, we determined:

o the adequacy of the general operational controls intended to promote efficiency and effectiveness; limit operator access to computers to authorized purposes; and control and schedule computer inputs, error corrections, and outputs; and

o the adequacy of the general controls intended to protect each DISO Center from physical destruction (excluding backup and disaster recovery plans) or unauthorized physical or electronic access.

We also evaluated the internal controls applicable to the automatic data processing (ADP) environment at each DISO Center.

Controls Over Organization, Management, and Systems. In addition, at the DISO-Denver Center, we determined the adequacy of the general controls over the organization and management of the information processing center and over system design, development, and change controls. Specifically, we determined:

o the adequacy of the general controls intended to clearly define and communicate organizational structure, policies, and procedures; separate duties and responsibilities among employees; properly supervise employee activities; and verify the competence and integrity of employees; and

o the adequacy of the general controls intended to verify the integrity of system design and development efforts, control application program changes, sufficiently test new and modified systems, and properly document new and modified systems.

Revision of Audit Objectives. During our audit, we revised our announced audit objectives. To better focus our limited audit resources, we did not evaluate the general controls over computer hardware, software, or backup and disaster recovery at any DISO Center. At the DISO-Columbus and DISO-Indianapolis Centers, we did not evaluate the general controls over the organization and management of the information processing centers or those over system design, development, and change controls.

Scope and Methodology

Methodology, Locations, and Time Period. In performing our audit, we used the "Information System Review - Audit Guide" (December 1983), published by the Information Management and Technology Division of the General Accounting Office. Specifically, we completed the applicable audit tests and procedures in Section III, "General Controls," of that guide. We performed field work at all three DISO Centers and discussed the control objectives and techniques with personnel at each Center. The systems reviewed included JSS-AC, JSS-RC, and DDMS. We used judgmental and simple random sampling methods to verify whether specific control techniques were in place and effective at each location. We examined documents at each location covering the period April 1980 to February 1993. This program audit was performed from May 1992 through May 1993.

Auditing Standards Used. Except for testing the reliability of certain computer-based data, the audit was made in accordance with auditing standards issued by the Comptroller General of the United States as implemented by the Inspector General (IG), Department of Defense, and accordingly included such tests of internal controls as were considered necessary. We did not determine the reliability of the computer-processed data used to quantify the number of abnormal endings to computer operations or remedial maintenance calls, as discussed in Finding A, or the number of outdated passwords, as discussed in Finding C. Our tests of internal controls at each DISO Center did not include evaluating the implementation of DoD Directive 5010.38, "DoD Internal Management Control Program." Evaluating the internal management control program was not required to meet our audit objectives. Appendix E lists the organizations we visited or contacted.

Internal Controls

Material Weaknesses. We identified material internal control weaknesses as defined by Office of Management and Budget Circular No. A-123 and DoD Directive 5010.38. Two computer applications at the DISO-Columbus Center were exposed to unauthorized access because of inadequate controls over passwords (Finding C); those applications processed over $54.0 billion in FY 1992 transactions. Inadequate change control procedures at the DISO-Denver Center also exposed three applications to higher risk of fraud, waste, or abuse (Finding E); those applications processed over $22.0 billion in FY 1992 transactions. These material internal control weaknesses will be eliminated by implementing Recommendations C.1.a. and C.1.b., related to password controls, and Recommendations E.1. through E.3., related to program change controls.

General Controls. We also evaluated the general controls over the information processing centers' operations and protection. In addition, at the DISO-Denver Center, we evaluated the general controls over the organization and

management of the information processing center and over system design, development, and change controls. Because of limited resources, we did not evaluate the effectiveness of the implementation of the DoD Internal Management Control Program.

Prior Audits and Other Reviews

Prior audits had covered general controls over certain aspects of ADP equipment maintenance, software security, and backup and disaster recovery plans. Although we did not follow up on those prior audits (described below), our audit disclosed problems similar to those previously reported at the DISO-Columbus Center. Six previous audits had covered general controls over certain aspects of software security and backup and disaster recovery plans.

Four IG, DoD, Reports. In Report No. 88-103, "Final Report on the Audit of Maintenance Support of General Purpose Computers at the Defense Logistics Agency," issued by the IG, DoD, on March 15, 1988, we reported that maintenance support for general-purpose computers at Columbus, Ohio, and other DLA locations was not cost-effective, adequately planned and performed, or effectively monitored and controlled. As discussed in Finding A, we identified similar problems in our audit. In Report No. 89-058, "Management of Access Controls to Computers at the Defense Logistics Agency," issued by the IG, DoD, on March 14, 1989, we reported that automated access controls to mainframe computers at Columbus, Ohio, and other DLA locations had not been effectively implemented and managed. Similar problems concerning ADP recertification reviews and password control at the DISO-Columbus Center are discussed in Findings B and C.

In Report No. 93-002, "Controls Over Operating System and Security Software Supporting the Defense Finance and Accounting Service," issued by the IG, DoD, on October 2, 1992, we reported deficiencies in operating system and security software at the DISO-Cleveland and DISO-Indianapolis Centers. In Report No. 93-133, "Controls Over Operating System and Security Software Supporting the Defense Finance and Accounting Service," issued by the IG, DoD, on June 30, 1993, we reported similar deficiencies at DLA's Systems Automation Center in Columbus, Ohio, and at the DISO-Columbus and DISO-Dayton Centers.

Two Air Force Audit Agency Reports. On August 5, 1991, the Air Force Audit Agency issued Report No. 0195410, "Data Center Processing Center Operations and Security at the Air Force Accounting and Finance Center (AFAFC)." The report identified weaknesses in the operating system and security software, and in controls over data security and integrity at AFAFC (now the DISO-Denver Center).

Backup and disaster recovery controls were addressed in the Air Force Audit Agency's Report No. 1265611, "Review of the Contingency Plan for Continued Operations of DFAS-DE Centralized Pay and Accounting Systems," September 5, 1991. That report concluded that contingency planning for JSS-AC needed improvement in production of backup tapes and site testing.

Part II - Findings and Recommendations

Finding A. Operational Improvements

At all three DISO Centers, personnel did not effectively analyze and follow up on abnormal endings to computer operations or oversee the preventive and remedial maintenance provided under automatic data processing equipment (ADP) contracts. Those conditions existed because management had not developed and implemented a quality assurance program over abnormal endings and equipment maintenance. As a result, computer operations were not efficiently managed, and payments to vendors for maintaining ADP equipment were excessive or were made without adequate documentation that the services were provided.

Operational Downtime

The Federal Managers' Financial Integrity Act requires each executive agency to establish internal accounting and administrative controls, as prescribed in the standards issued by the Comptroller General of the United States, to provide reasonable assurance that " . . . funds, property, and other assets are safeguarded against waste, loss, unauthorized use, or misappropriation . . . ." As discussed below, when computer processing is unexpectedly halted by abnormal endings or equipment malfunctions, DISO's costs increase because less operating capacity is available for other uses, and response time increases because of downtime spent in correcting problems.

Abnormal Endings (ABENDS) to Computer Operations. At the three DISO Centers visited, the number of ABENDS that stopped operations varied. During FY 1992, the DISO-Columbus Center reported 9,242 ABENDS, and the DISO-Indianapolis Center reported 4,067. During the last 3 quarters of FY 1992, the DISO-Denver Center reported 2,464 ABENDS. None of the DISO Centers had a quality assurance program in place to track and correct ABENDS. Each of those ABENDS, however, resulted in system downtime that required personnel to restart an operation or postpone it. The DISO-Columbus and DISO-Indianapolis Centers did not maintain the records required to estimate the costs of downtime resulting from ABENDS. At the DISO-Denver Center, however, ABENDS due to programming errors and other non-equipment-related stoppages resulted in about 579 hours of downtime during the last 3 quarters of FY 1992. Based on the DISO-Denver Center's processing rate of $163 per hour, the total downtime was valued at about $94,000. Nearly 30 percent (164) of the 579 downtime hours had repetitive causes. The downtime costs at the DISO-Denver Center do not reflect the additional costs incurred because of increased system response time and missed production schedules. In addition to downtime costs, analyzing ABENDS caused by programming errors could expose weaknesses in programmer supervision and system testing and design.

ADP Equipment Maintenance. ADP equipment contracts at the DISO Centers included preventive and remedial maintenance by the vendor. As discussed below, our current and prior audits disclosed that improvements were needed at all three DISO Centers in administering ADP equipment contracts to verify that preventive and remedial maintenance were provided in accordance with contract terms.

Preventive Maintenance. Before providing preventive maintenance services, vendors should propose and the Government should review and accept the proposed (or modified) preventive maintenance schedules. DISO Center personnel should maintain records of preventive maintenance services provided by vendors to verify billings from the vendors. In turn, Government officials authorized to certify the receipt of preventive maintenance services should do so based on documentary evidence of those services maintained by the DISO Center. As detailed below, all three DISO Centers needed to improve their quality assurance programs over preventive maintenance.

DISO-Columbus Center. Contracting officials for the DISO-Columbus Center could not document their receipt, review, or approval of preventive maintenance schedules. Also, the form used to document the receipt of maintenance services was designed for recording only remedial maintenance, not preventive maintenance. Despite the lack of evidence that preventive maintenance was actually scheduled or provided, vendors were paid for such services. The contracting officer stated that he certified the receipt of preventive maintenance services for payment based on the presumption that he would have received complaints if those services had not been provided. Similar findings at the DISO-Columbus Center were previously reported in our Report No. 88-103, "Final Report on the Audit of Maintenance Support of General Purpose Computers at the Defense Logistics Agency," March 15, 1988.

DISO-Denver Center. As with the DISO-Columbus Center, contracting officials at the DISO-Denver Center could not document the receipt, review, or approval of preventive maintenance schedules for five of the six vendors who furnished maintenance. Likewise, vendor payments for preventive maintenance services were made without documentary evidence that such services had actually been received.

DISO-Indianapolis Center. Contracting officials at the DISO-Indianapolis Center could not provide any evidence of their approval of the preventive maintenance services proposed by vendors. However, personnel at the DISO-Indianapolis Center adequately documented the preventive maintenance services provided by the vendors.

Remedial Maintenance. For remedial repairs, vendors may provide on-call service during the standard business day and week, or full 24-hour, 7-day capability. Once a service call is placed, vendors may also have to meet a specific time-to-arrival or time-to-repair requirement. For example, a vendor may be required to arrive on-site within 2 hours of a service call to repair the equipment, or to repair the equipment within 4 hours from the time of the call. Terms may also specify that equipment operate at a given effectiveness level, e.g., 98-percent effectiveness monthly. To encourage vendors to respond

promptly to maintenance calls (and thus minimize computer downtime), the Government is due credits against the vendors' monthly maintenance fees if vendors do not meet the time-to-arrival, time-to-repair, and similar contract terms. The credits are taken at the time the Government certifies that the services were received. As discussed below, improvements were needed in equipment maintenance at all three DISO Centers.

DISO-Columbus Center. Based on a simple random sample, we projected that the vendors exceeded the time-to-arrival requirements for remedial maintenance calls on 3,361 (74 percent) of the projected 4,561 hardware-related ABENDS experienced during FY 1992 (see Appendix C). Vendors met the time-to-repair requirements in their contracts with the DISO-Columbus Center. Aside from the additional downtime costs resulting from the vendor's tardiness, contracting officials stated that the Government also did not receive appropriate billing credits in instances where the vendor did not meet the time-to-arrival or other contractual performance measurements. Thus, the vendors were overpaid to the extent of any credit due the Government. The contract administrator did not take action to collect credits because no quality assurance function was in place to notify him that such credits were due.

DISO-Denver Center. Based on a simple random sample, we projected that vendors did not meet the time-to-repair requirements on 149 (18 percent) of the 854 remedial maintenance calls made between October 1991 and May 1992 (see Appendix C). Vendor performance against time-to-arrival requirements was considered reasonable. We did not determine whether the Government received appropriate billing credits for the vendors' tardiness.

DISO-Indianapolis Center. We did not test vendor performance on remedial maintenance contracts at this location. However, as with the DISO-Columbus Center, contracting officials stated that the Government did not receive appropriate billing credits in those instances where the vendors did not arrive or make repairs within the benchmarks established in the contracts. This resulted in overpayments to the vendors, and contracting officials could not explain why billing credits were not received.

Summary

Information processing centers can achieve greater efficiency by monitoring events that lead to hardware or software failures. If abnormal endings to computer operations are not periodically analyzed, computer downtime is more likely to result because corrective actions will not have been taken to avoid repetitive problems. Some computer downtime can also be avoided by performing regular preventive maintenance on computer hardware. When hardware problems cause computer operations to cease, vendors must arrive promptly and make the necessary repairs in a reasonable amount of

time. The Government incurs unnecessary costs because of computer downtime when vendor maintenance services and abnormal endings to computer operations are not adequately or effectively monitored.

Recommendations, Management Comments, and Audit Response

We recommend that the Director, Defense Information Services Organization:

1. Establish an in-house quality assurance program to track and analyze the causes of abnormal endings to computer operations and take corrective action to prevent abnormal endings due to repetitive causes.

Management Comments. DISO partially concurred with our recommendation, stating that ABENDS have been tracked and analyzed daily for several years, and corrective actions are discussed with management and implemented as required. DISO noted that a restart/rerun program will be installed to automate ABENDS recovery, reducing manual intervention.

Audit Response. Management's comments were not fully responsive to our recommendation because no corrective action was proposed. Two of the three DISO Centers visited did not track and analyze ABENDS because required documentation or resources were not available. Computer operators at the DISO-Columbus Center normally did not complete the recovery trouble report and operator recovery log at the time an ABEND occurred. Without that data, no analyses of ABENDS could be made. At the DISO-Indianapolis Center, trend analyses were not made because the limited staff resources were used for higher priority work.

Information on ABENDS was available at the DISO-Denver Center and showed that a significant number of the ABENDS were caused by repetitive programming errors. However, written procedures did not require computer operators to report these ABENDS to programmers for analyses and correction. Eliminating the causes of repetitive ABENDS through such analyses would have increased operational economy and efficiency.

Management's plan to automate the ABENDS recovery process should reduce overall system downtime caused by ABENDS. However, installing such software will not eliminate the repetitive causes of those ABENDS. Additional comments are requested from DISO on the planned corrective actions by May 16, 1994. See Part IV for the full text of management's comments, and the "Response Requirements for Each Recommendation" chart below for the specific requirements for additional comments.

2. Establish an in-house quality assurance program over the maintenance performed under automatic data processing equipment contracts at the Defense Information Services Organization Centers to verify that:

a. Contracting personnel schedule and approve preventive maintenance services in advance.

b. Computer operators at the Defense Information Services Organization Centers maintain adequate documentation on actual preventive and remedial maintenance services.

c. Contracting personnel verify, before authorizing payments to vendors, that vendor billings (including appropriate credits) for preventive and remedial maintenance services are prepared in accordance with contract terms.

d. Defense Information Services Organization managers certify receipt of preventive or remedial maintenance services based on evidence that such services were actually received.

Management Comments. DISO fully concurred with our recommendation and plans to implement the recommended internal controls by March 31, 1994. See Part IV for the full text of management's comments.

Response Requirements for Each Recommendation

Responses to the final report are required from the addressee shown for the items indicated with "X" in the chart below.

		Response Should Cover:		
Number	Addressee	Concur/ Nonconcur	Proposed Action	Completion Date
1.	DISO		X	X

Finding B. ADP Security Oversight

At one or more DISO Centers, requirements were not met for conducting periodic reviews of ADP security, analyzing internal controls over ADP operations and reporting on related weaknesses, or providing centralized authority over all ADP security policies and safeguards. Periodic security reviews were not performed because local operating personnel knew that security accreditation requirements would not be met; therefore, they chose not to perform the required reviews. Internal control analyses and reports were not properly made because responsible personnel were not aware of reported material internal control weaknesses or were not adequately trained in their duties. Responsibility for ADP security was not centralized in one individual because no one individual was trained in using all operating systems. As a result, material internal control weaknesses disclosed in prior audits were not reported in the Annual Statements of Assurance, and oversight of ADP physical security and access controls was impaired.

Oversight and Reporting Requirements

The Federal Managers' Financial Integrity Act (the FMFIA) requires executive agencies to establish internal controls that will provide reasonable safeguards against the waste, loss, unauthorized use, or misappropriation of funds, property, and other assets. The FMFIA further requires executive agencies to comply with standards issued by the Comptroller General of the United States, which include the "Standards for Internal Controls in the Federal Government," issued in 1983. To safeguard assets, the standards require that access to resources and records be limited to authorized individuals, and that accountability for the custody and use of resources be assigned and maintained. The standards recognize that restricting access to resources should be based on periodic assessments of their vulnerability and the risk of loss. In an ADP environment, those internal control requirements are partially met when management assigns responsibility for physical security and access controls to competent personnel at appropriate levels within an organization.

Overall, the Office of the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) and the Defense Information Systems Agency (DISA) provide instructions and guidance on computer security to the DISO. DISO managers and security personnel are required to assess and report on physical security and computer access controls. As discussed below, certain DISO personnel did not adequately perform their responsibilities for conducting periodic risk analyses, preparing and releasing Annual Statements of Assurance, and providing centralized oversight and direction of ADP security policies and procedures.

Periodic Reviews and Recertifications. Office of Management and Budget (OMB) Circular No. No. A-130, "Management of Federal Information

Resources," December 1985, requires a periodic review and recertification of computer systems at least once every 3 years. DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AIS)," March 1988, requires the analysis and selection of appropriate, cost-effective security measures to achieve and maintain a minimum level of protection. At the DISO-Columbus Center, however, personnel had not conducted a recertification review since 1987. A similar finding was reported in our Report No. 89-058, "Management of Access Controls to Computers at the Defense Logistics Agency," March 14, 1989. For FY 1992, the DISO-Columbus Center, which was formerly a DLA activity, was directed by DISO headquarters to report the results of scheduled internal control reviews through DLA. The Deputy Commander, DLA, notified the DISO-Columbus Center in February 1991 that he would not provide security accreditation unless the requirement for a backup (disaster recovery) plan was met. The DISO-Columbus Center's security officer knew that the Center would not meet the Deputy Commander's requirement; therefore, he did not perform the recertification review required by OMB Circular No. A-130. Recertification reviews cover many security measures, such as facility protection and access, in addition to backup plans. As a result, the DISO-Columbus Center did not identify and report vulnerabilities resulting from the lack of a quality assurance program (Finding A) and inadequate password security, security training, and training plans (Finding C).

Statement of Assurance. DoD Directive 5010.38, "Internal Management Control Program," April 1987, requires an Annual Statement of Assurance on internal controls. Intended for Congress, the statement should explain how the evaluation was done and should disclose any material weaknesses, including those corrected in the reporting year or carried forward for correction to the following year.

At the DISO-Columbus and DISO-Indianapolis Centers, the Annual Statements of Assurance did not disclose material weaknesses that had been reported in our Reports No. 93-002 and No. 93-133, both entitled "Controls Over Operating System and Security Software Supporting the Defense Finance and Accounting Service," dated October 2, 1992, and June 30, 1993, respectively. Those two reports identified material weaknesses in the operating procedures and actual controls required to prevent unauthorized access to the computer systems at the two DISO Centers. At the DISO-Columbus Center, the material weakness was not reported because the preparer of the Annual Statement of Assurance had not read the audit report. At the DISO-Indianapolis Center, the material weakness was not reported because the preparer believed that corrective actions already taken had eliminated the reporting requirement. As a result, material internal control weaknesses disclosed in prior audits were not included in the Annual Statements of Assurance sent to Congress by the Secretary of Defense.

Information Systems Security Officer. The DISO-Denver Center did not meet the requirement in DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AIS)," March 1988, for a single information systems security officer. The employee assigned as information systems security officer did not enforce security policy and other safeguards affecting all

ADP systems and their operating environment. That employee was responsible for information security on all systems except for the Case Management Control System (CMCS). The Director, DISO-Denver Center, made a second individual responsible for controlling the security software that restricted computer access to CMCS. Another concern was that the second individual worked in the same division as employees who provided programming support to CMCS. Because the security responsibilities were divided, the information systems security officer could not require that CMCS comply with the security policies and safeguards established for all other ADP systems.

Management made a second individual responsible for security on CMCS because special knowledge was required to work in the Virtual Machine operating environment used by CMCS. A Multiple Virtual Storage operating environment was used with all other ADP systems, which were controlled by the information systems security officer. The different operating systems used at the DISO-Denver Center did not justify management's deviation from the requirements of DoD Directive 5200.28. Those requirements could have been met by placing the individual charged with security control and oversight over CMCS under the direct supervision of the information systems security officer.

In addition, inadequate segregation of duties existed between the CMCS security officer and the system's programmers because management assigned security oversight to an individual who reported to the same supervisor as CMCS programmers. CMCS is a major ADP system that processed about $12.0 billion in foreign military sales and over $5.0 billion in disbursements during FY 1992.

Summary

Adequate ADP security oversight requires periodic reviews and assessments of existing security over ADP systems, including any findings reported in external audits and reviews. Centralizing ADP security oversight in a single individual helps to ensure that all computer applications meet minimum security requirements. When ADP security oversight is inadequate, the physical security of computer assets is jeopardized, and the risk of unauthorized access to computer applications increases.

Recommendations, Management Comments, and Audit Response

1. We recommend that the Director, Defense Information Services Organization, Information Processing Center, Columbus, Ohio:

a. Perform the recertification review of the installation's computer systems required by the Office of Management and Budget Circular No. A-130 during FY 1994.

b. Review all audit reports covering the Defense Information Services Organization-Columbus Center, and include in the Annual Statement of Assurance all material internal control weaknesses reported (or provide written justification for their omission).

2. We recommend that the Director, Defense Information Services Organization, Information Processing Center, Indianapolis, Indiana, train personnel in preparing the Annual Statement of Assurance.

3. We recommend that the Director, Defense Information Services Organization, Information Processing Center, Denver, Colorado, assign responsibility for security control and oversight of the Case Management Control System to the information systems security officer.

Management Comments. Management concurred and stated that a recertification review will be conducted, open material weaknesses were reported in the FY 1993 Annual Statement of Assurance, personnel received training in the Internal Management Control Program, and the employee responsible for security of CMCS was transferred to the security office. Management made plans to complete the necessary corrective actions during FY 1994. See Part IV for the full text of management's comments.

Finding C. Controls Over Access

Weaknesses existed at the DISO-Columbus and Denver Centers in controls over access to computer rooms, equipment, sensitive documents and forms, and application programs. These weaknesses occurred because security oversight was inadequate or undocumented, and management did not emphasize password control over competing requirements. As a result, computer assets (including application programs) were exposed to unnecessary risk of unauthorized access.

Access Vulnerabilities

Executive agencies are required by the FMFIA to establish internal controls that will safeguard funds, property, and other assets against waste, loss, unauthorized use, or misappropriation. The FMFIA also requires executive agencies to comply with internal control standards issued by the Comptroller General of the United States, which require that access to resources and records be limited to authorized individuals. One means of meeting that requirement is to restrict access to computer rooms, equipment, and critical documents and forms to authorized personnel. Without electronic or physical safeguards to limit access to such assets, unauthorized access could result in fraud, waste, or abuse. We identified the following weaknesses in the safeguards against unauthorized access to ADP assets at two DISO centers.

Passwords. Passwords are used to limit access to computer applications and data bases to authorized individuals and for authorized purposes. If passwords are not periodically changed, there is a higher risk that unauthorized personnel can obtain access to computer applications. At the DISO-Denver and DISO-Indianapolis Centers, users were automatically prompted by the security software to change their passwords at fixed intervals. However, security software used by the DISO-Columbus Center did not offer similar capabilities for automatically prompting users to change their passwords. Problems with the DISO-Columbus Center's control over passwords were reported in our Report No. 89-058, "Management of Access Controls to Computers at the Defense Logistics Agency," March 14, 1989.

DLA Regulation 5200.17, "Security Requirements for Automated Information and Telecommunications System," October 9, 1991, required the DISO-Columbus Center users to change their passwords at least every 180 days. Computer security personnel were also required by the DLA regulation to monitor the age of passwords, notify users before passwords expire, and force a password change by denying access to users whose passwords exceeded the 180-day limit. Based on tests of the DISO-Columbus Center's two major financial systems (described below), we determined that the DISO-Columbus Center did not comply with the DLA regulations in effect at the time of our audit.

Defense Business Management System (DBMS).[3] Users of DBMS did not change their passwords every 180 days, as required by DLA guidelines. Of 32,227 users, about 1,886 (6 percent) had not changed their passwords within 180 days. Of those whose passwords had not been changed, 991 users (53 percent) had not changed their passwords in over 1 year. Users did not change their passwords because security personnel at the DISO-Columbus Center did not periodically review the age of passwords and deny access to users whose passwords had not been changed in 180 days. Because outdated passwords were used, the risk of unauthorized access to DBMS, which processed a civilian payroll of $2.7 billion in FY 1992, was unnecessarily increased.

Mechanization of Contract Administration Services (MOCAS) System. We could not determine how often passwords were changed by the 15,100 MOCAS users. At the time of our audit, security personnel could not provide us with reports needed to determine when passwords were last changed. Managers at the DISO-Columbus Center stated that the reports were not being prepared on a regular basis. This suggested that the standard reports were not periodically generated because other work was assigned a higher priority. Therefore, managers had no assurance that adequate control existed over the passwords used to gain access to MOCAS, which paid $52.0 billion in contract payments during FY 1992.

Physical Security Plans. Unlike the DISO-Denver and Indianapolis Centers, DISO-Columbus Center officials could not provide evidence that its physical security plan was tested periodically. Although the DISO-Columbus Center had a security plan that was in accordance with DLA Manual 5710.1, "Physical Security Plan," April 1980, security personnel could not tell us when the plan was last tested to verify that it was functional. The plan contained security measures that required periodic tests. These measures included key and lock control; access limitations, authority, and control; and security patrol requirements. Due to employee turnover, documentation of any tests of the physical security plan was not retained.

Contractor Clearances. At the DISO-Denver Center, two vendor maintenance personnel who did not have the National Agency Checks required by DoD Directive No. 5200.28 were allowed unescorted access to the information processing center. Adequate controls existed over similar contractor personnel at the other two DISO Centers. Improper access to the DISO-Denver Center occurred because responsible officials did not periodically reconfirm the status of the National Agency Checks made on vendors' maintenance employees. One official at the DISO-Denver Center stated that he was not notified that a vendor had withdrawn two employees' "clearance" pending a new National Agency Check. Allowing improper access to computer facilities that operate high-security computer systems, such as those at the DISO-Denver Center, could adversely impact national security.

[3] DBMS was formerly known as the Automated Payroll Cost and Personnel System.

Summary

Security for information processing centers relies on measures that prevent unauthorized access to financial systems by electronic and physical means. When passwords are not changed regularly and access is not adequately controlled or physically barred, unauthorized personnel may have access to the computer rooms, equipment, critical documents and forms, and application programs. Unauthorized access could result in the deliberate destruction of computer assets or in fraudulent financial transactions.

Recommendations, Management Comments, and Audit Response

1. We recommend that the Director, Defense Information Services Organization, Information Processing Center, Columbus, Ohio:

a. Obtain and implement an Automated Password Change Facility to automatically require users to change their passwords every 90 days.

b. Schedule and make periodic tests of the physical security plan, and retain evidence of such tests until new tests are completed.

Management Comments. DISO concurred with our finding on user passwords at the DISO-Columbus Center, but nonconcurred with our draft recommendation to have computer security personnel manually screen user passwords. As an alternative, by March 30, 1994, DISO plans to automate the oversight process by installing an Automated Password Change Facility that will force users to change their passwords every 90 days. DISO concurred with our recommendation on the physical security plan at the DISO-Columbus Center, and will obtain and retain documentation on periodic tests of the physical security plan at the DISO-Columbus Center. See Part IV for the full text of management's comments.

Audit Response. We modified our first recommendation to reflect the alternative corrective action proposed by DISO. The corrective actions planned by DISO related to the Center's physical security plan are fully responsive to our recommendation.

2. We recommend that the Director, Defense Information Services Organization, Information Processing Center, Denver, Colorado, require responsible managers to annually reconfirm that favorable National Agency Checks have been completed on vendors' maintenance employees who have unescorted access to the information processing center.

Management Comments. DISO did not concur with our draft recommendation to annually confirm the security clearances of vendors'

maintenance employees at the DISO-Denver Center. None of the vendors' maintenance employees had access to classified information. Therefore, security clearances were not needed. Furthermore, individuals who needed unescorted access had National Agency Checks. DoD Regulation 5200.2-R does not require the recommended annual confirmations.

Audit Response. DISO correctly stated that only favorable National Agency Checks, not security clearances, were required for the two employees who were given unescorted access to the computer room at the DISO-Denver Center, and that DoD regulations do not require annual confirmations. We changed our recommendation to refer to National Agency Checks. Regulations do not require periodic confirmations of National Agency Checks. However, if DISO had periodically confirmed the National Agency Checks made on individuals with unescorted access to the computer room, the condition identified would have been detected at an earlier date. DISO is requested to comment on our revised recommendation by May 16, 1994. See the chart below for specific requirements.

Response Requirements for Each Recommendation

Responses to the final report are required from the addressee shown for the items indicated with "X" in the chart below.

		Response Should Cover:		
Number	Addressee	Concur/ Nonconcur	Proposed Action	Completion Date
2.	DISO		X	X

Finding D. Environmental Protection

At the DISO-Denver and DISO-Indianapolis Centers, known weaknesses existed in the protection given to computer assets (including application programs and data files) against environmental risks. Management did not correct those weaknesses because they were willing to accept the risks assumed in not making the corrections. As a result, costly computer assets supporting military operations, payroll operations, and other vital computer operations were in danger of accidental or deliberate destruction through fire, water, or other hazards.

Physical Vulnerabilities

Under the FMFIA and internal control standards issued by the Comptroller General of the United States, executive agencies are responsible for safeguarding assets against waste, loss, unauthorized use, or misappropriation. That requirement is included in DoD Directive 5200.28 and in DISA Instruction 630-230-19, "Security Requirements for Automated Information Systems (AIS)," August 1991. The DoD directive requires that the physical controls in a computer room provide appropriate protection for the sensitivity of the data being processed. The DISA instruction explains the minimum security requirements for access controls, physical layout, fire protection, environmental controls, and building construction.

Periodically assessing the vulnerability of computer facilities and records to environmental risks is one means of ensuring that computer assets are adequately protected against accidental or deliberate destruction by fire, water, or other hazards. Adequate environmental protection controls were in place at the DISO-Columbus Center. However, as discussed below, known weaknesses existed in the protection of computer facilities and records at two DISO Centers.

DISO-Denver Center. In 1989, an independent contractor performed a risk analysis of the information processing center at the DISO-Denver Center. The contractor recommended that overhead shutoff valves and heat detection units be installed. DISA Instruction 630-230-19 also recommended shutoff valves to prevent water damage or flooding. The engineer at the DISO-Denver Center proposed that shutoff valves be installed, but the work order was not completed. The heat detection units were not installed because management believed that the fire protection system was adequate. However, the independent contractor noted that the existing system reacted only to smoke, which provided less protection than one that reacted to both smoke and heat. The system should be upgraded to react to smoke and heat.

DISO-Indianapolis Center. In June 1991, security personnel at the DISO-Indianapolis Center conducted a vulnerability analysis of the computer rooms and issued a special "Automation Security Task Force Findings Report" that identified numerous deficiencies in physical protection of the information

processing center's assets. At that time, the information processing center was an Army activity and was not required to follow DISO or DISA security guidance. Management did not correct all of the reported deficiencies because they believed that existing protection was adequate. Since then, however, the information processing center has been reorganized as the DISO-Indianapolis Center and is governed by DISA regulations. At the time of our audit, 33 reported deficiencies still remained uncollected. Based on our discussion with local managers, corrective action is required on 6 of the 33 deficiencies in order to comply with DISA or DISO regulations. For example, management did not install fire dampers in the information processing center's ductwork, as suggested in the special report from the DISO-Indianapolis Center's security personnel. Although it was not applicable to the DISO-Indianapolis Center at that time, DISA Instruction 630-230-19 requires fire dampers to be in place in the building ductwork. Appendix B lists the six deficiencies that still needed correction at the time of our audit.

Recommendations, Management Comments, and Audit Response

1. We recommend that the Director, Defense Information Services Organization, Information Processing Center, Denver, Colorado, install the overhead shutoff valves and heat detectors or provide other security measures approved by the Defense Information Systems Agency.

2. We recommend that the Director, Defense Information Services Organization, Information Processing Center, Indianapolis, Indiana, correct the physical protection deficiencies listed in Appendix B.

Management Comments. DISO concurred with both recommendations. DISO requested that DFAS-Denver Center install the necessary overhead shutoff values or control valves in the computer center. An environmental monitoring control system is also being evaluated, which may satisfy the requirements for a heat detection system. In response to our recommendation on physical protection deficiencies, DISO described the corrective actions planned or taken on the 19 deficiencies originally listed in Appendix B, or explained why corrective action was not feasible or necessary. See Part IV for the full text of management's comments.

Audit Response. The corrective actions planned by management are fully responsive to our recommendations. Management adequately explained why corrective action was not feasible or necessary on 13 of the original 19 deficiencies at the DISO-Indianapolis Center identified in our draft report. Based on management's comments, we revised our finding and Appendix B to state that only six physical protection deficiencies needed correction.

Finding E. Change Controls at the DISO-Denver Center

Application program changes at the DISO-Denver Center were not always properly authorized and approved by appropriate user and programming personnel. Specifically, application program changes were not properly authorized for two computer systems, and on another system, the same individual was authorized to make program changes and move the changed program into production. Programming changes were made without proper authorization and approval because local procedural requirements were not enforced or had not been established, and conflicting programming responsibilities were not adequately segregated. As a result, key application programs used to process over $22.0 billion in business transactions during FY 1992 (see Appendix A) were exposed to higher risk of fraud, waste, or abuse because of erroneous or fraudulent program changes.

Controls Over Application Program Changes

The FMFIA requires executive agencies to establish internal controls that will safeguard funds, property, and other assets against waste, loss, unauthorized use, or misappropriation. Internal control standards issued by the Comptroller General of the United States require that transactions and other significant events be authorized and executed only by persons acting within the scope of their authority. So that no individual controls all aspects of a transaction, agencies are also required to make separate employees responsible for authorizing, processing, recording, and reviewing transactions.

In the ADP environment, one means of meeting those requirements is to ensure that all application program changes are authorized by the appropriate users and information processing center personnel. To do so, different employees should be responsible for initiating, programming, and testing changes, and for moving changed programs into production. When combined with adequate supervision, such internal controls, incorporated into change control procedures, help maintain adequate system and program integrity.

Change Control Procedures and Practices

To evaluate change control procedures and practices, we selected three major ADP systems at the DISO-Denver Center for review. Those three systems were the Defense Debt Management System (DDMS), Joint Service Software for Active Components (JSS-AC), and Joint Service Software for Reserve Components (JSS-RC). Although not established for DDMS, change control

procedures for JSS-AC and JSS-RC were established in the Joint Service Software (JSS) Directorate Operating Instruction 205-3, "Computer Security, Program Module Certification," December 1, 1991. That local procedure implemented the change control and other procedural requirements of DoD Directive 5200.28. To establish accountability, the JSS instruction required that the signature of an authorized individual appear in all of the 10 coordination blocks on the certification sheets used to control program changes. In order to segregate conflicting programming duties, the JSS instruction also specified that no employee was authorized to sign more than one of seven coordination blocks on the certification sheet. The conflicting functions were identified as the programmer, certifier, and programming branch chief during the program development phase; the system tester and system test branch chief during the system test phase; and the customer and production move monitor during the final production phase.

Authorization or Approval of Program Changes

DISO-Denver Center personnel did not always comply with local requirements for authorizing and approving changes to application programs, including the need to maintain adequate segregation of duties in the change control process. Internal control weaknesses identified in three major applications at the DISO-Denver Center are discussed below.

JSS-AC. Overall, the DISO-Denver Center adequately controlled JSS-AC program changes; there were no instances where the same individual was involved in more than one of the key phases of making program changes, i.e., the program development, system test, and production phases. The segregation of duties among individuals involved in the key programming phases is a strong internal control. Although not a material internal control weakness, we projected that 171 (26 percent) of the 655 program changes to JSS-AC during FY 1992 were not authorized in accordance with JSS Directorate Operating Instruction 205-3. As detailed in Appendix C, the projection was based on a statistical sample of 65 program changes in which 17 changes were improperly authorized. Mandatory approvals for program changes were not obtained, and approvals were obtained from the same individual for conflicting coordination requirements. In our sample, programming branch chiefs did not sign to authorize eight changes during program development, and certifying personnel did not authorize four changes. Five changes in our sample were not properly authorized during the program development, system test, or production phase because an individual certified the change while acting in two different capacities. For example, the same individual frequently signed the certification sheet as both programmer and certifier. Allowing programmers to certify their own program changes is inadequate segregation of duties, is contrary to established procedures, and can result in erroneous or improper programming changes.

Improperly authorized program changes were made to JSS-AC (and JSS-RC, as discussed below) because the branch chiefs and other personnel involved in each of the three programming phases did not enforce or comply with local change control procedures.

JSS-RC. Overall, JSS-RC program changes were also adequately controlled. There was one instance where the same individual was both the system tester and the customer; however, we did not consider that deficiency significant, since the system tester's work was reviewed by two other individuals. Although not material, the internal controls over JSS-RC program changes were inadequate in certain respects. We projected that 44 (35 percent) of the 128 program changes made to JSS-RC during FY 1992 were not authorized in accordance with JSS Directorate Operating Instruction 205-3. As detailed in Appendix C, the projection was based on a statistical sample of 52 program changes in which 18 changes were improperly authorized. Customer authorization was not obtained during the final production phase for one change in our sample. Another 17 changes in our sample were not properly authorized during the program development, system test, or production phase because an individual certified the change while acting in 2 different capacities. For example, 15 program changes were tested by a system test branch chief who later certified the propriety of his own testing. This was inadequate segregation of duties, and could allow erroneous or improper programming changes to occur.

DDMS. Responsibility for making program changes and moving the changed program into production were not adequately segregated on DDMS. The DDMS lead programmer not only made program changes, but also moved the changed program into the production library for use. On other systems (JSS-AC and JSS-RC), those responsibilities were assigned to separate employees. Management agreed that giving the DDMS lead programmer such authority did not adequately separate the responsibilities. However, management stated that the DDMS staff was too small to make a single employee responsible for moving changed programs into the production library. We believe that the DISO-Denver Center has sufficient resources to assign these tasks to separate employees for DDMS and other small systems.

Summary

One of the primary general controls over ADP systems is maintaining adequate controls over application program changes. Such controls are obtained by establishing accountability for key review functions during each programming phase, and by segregating conflicting duties. Fraud, waste, and abuse can result if adequate change controls are not established and enforced.

Recommendations, Management Comments, and Audit Response

We recommend that the Director, Defense Finance and Accounting Service, Financial Systems Activity, Denver, Colorado:

1. Require that, at a minimum, all central design activities follow procedures similar to those established in Joint Service Software Directorate Operating Instruction 205-3.

2. Segregate the responsibilities for making program changes, performing system tests, and moving changed programs into production. This applies to the Defense Debt Management System and any other computer systems in which those responsibilities are currently performed by the same individual or group.

3. Enforce the coordination requirements established by Joint Service Software Directorate Operating Instruction 205-3 for making program changes to the Joint Service System for Active Components and the Joint Service System for Reserve Components.

Management Comments. DFAS concurred with all parts of our finding and recommendations, except for the discussion in our draft report on the use of the Superzap utility. Application software programmers are not authorized to access the Superzap utility. The Superzap changes identified in the draft report reflected changes made by Computer Associates, Inc., in its software maintenance releases, not changes to the application software. Since application modules include system software utilities during compilation, the compiled listings can show the changes made to the operating system software by the Superzap utility. See Part IV for the full text of management's comments.

Audit Response. Our draft report recommendations were addressed to the Director, Defense Information Services Organization, Information Processing Center, Denver, Colorado. Because of a reorganization, the Defense Information Services Agency forwarded the draft finding and recommendations to the Defense Finance and Accounting Service for comments. DFAS offered a valid explanation for the use of the Superzap utility; therefore, in the final report, we have deleted the reference to Superzap and the related recommendation. Regarding the other recommendations, we have directed them in the final report to the Defense Finance and Accounting Service, Financial Systems Activity, Denver, Colorado. DFAS's comments on the draft were adequate; therefore, no further comments are required.

Part III - Additional Information

Appendix A. Major Automated Data Processing Systems of the Defense Information Services Organization

Location	Automated Data Processing Systems	Financial Services Performed In FY 1992
DISO-Columbus	Defense Business Management System (DBMS)	Paid $2.7 billion in payroll to 110,300 civilians.
	Mechanization of Contract Administration Services (MOCAS)	Paid $52.0 billion on 334,645 contracts.
DISO-Denver	Joint Service Software for Active Components (JSS-AC)	Paid $19.6 billion in military pay and entitlements to 481,000 Air Force personnel.
	Joint Service Software for Reserve Components (JSS-RC)	Paid $1.7 billion in pay and entitlements to 205,000 Air Force Reserve and Air National Guard personnel.
	Defense Debt Management System (DDMS)	Maintained $80.3 million in year-end accounts receivable. Collected $7.0 million during FY 1992.
	Case Management Control System (CMCS)	Received $11.9 billion in foreign military sales. Disbursed $5.1 billion.

Location	Automated Data Processing Systems	Financial Services Performed In FY 1992
DISO-Indianapolis	Joint Service Software for Active Components (JSS-AC)	Paid $25.0 billion in pay and entitlements to 650,000 active duty personnel.
		Paid $2.1 billion in pay and entitlements to 270,773 Army Reserve personnel and $3.3 billion to 432,928 National Guard personnel.
	Army Retired Pay System	Paid $8.0 billion in retired pay benefits to 590,427 retirees.
	Transportation Pay System	Paid $2.1 billion in transportation costs.

Appendix B. Physical Protection Improvements Needed at the DISO-Indianapolis Center

The following six deficiencies, identified in the "Automation Security Task Force Findings Report" issued in June 1991 by the DISO-Indianapolis Center, had not been corrected at the time of our audit:

1. The smoke/fire detection system in the computer room does not shut down or reverse the air flow of the ventilation system.

2. There is no equipment in the computer room to exhaust smoke/combustion products directly to the outside atmosphere.

3. Alarms for air conditioning failure, airflow restriction, rising temperatures, and humidity fluctuations cannot be heard outside the computer room.

4. No automatic fire dampers are installed in the building ductwork.

5. No physical inventories are made to account for all computer storage devices.

6. Windows on the interior of the computer room do not have embedded wire support to prevent shattering.

Appendix C. Statistical Sampling Plan and Results

Sampling Plan. The universes, sample selection techniques, and sample sizes used in making the statistical projections discussed in Findings A and E, Part II, are detailed below.

Remedial Maintenance at the DISO-Columbus Center. As discussed in Finding A, we statistically projected the numbers and percentages of abnormal endings (ABENDS) to computer operations that were due to hardware problems caused when the vendor did not meet the contractual time-to-arrival requirements.

The audit universe consisted of the 9,242 ABENDS experienced during FY 1992 due to both hardware problems and non-hardware-related problems, e.g., programming errors.

We used simple random sampling for the statistical samples in this audit. We randomly selected 77 ABENDS from the DISO-Columbus Center universe.

Remedial Maintenance at the DISO-Denver Center. As discussed in Finding A, we statistically projected the numbers and percentages of remedial maintenance calls made at the DISO-Denver Center in which the vendor did not meet the contractual time-to-repair requirements.

The audit universe consisted of the 854 remedial maintenance calls made at the DISO-Denver Center between October 1991 and May 1992.

We used simple random sampling for the statistical samples in this audit. We randomly selected 40 remedial maintenance calls from the DISO-Denver Center universe.

Program Change Controls at the DISO-Denver. As discussed in Finding E, we statistically projected the numbers and percentages of program changes that were improperly authorized at the DISO-Denver Center. We made separate projections for the JSS-AC and the JSS-RC systems.

The two audit universes consisted of the 655 and 128 program changes made during FY 1992 to the JSS-AC and JSS-RC systems, respectively.

We used simple random sampling for the statistical samples in this audit. We randomly selected 65 program changes from the JSS-AC universe. The sample size for the JSS-RC universe was 52 program changes.

Sampling Results. Tables 1., 2., and 3. give statistical projections of the sample data on vendor performance at the DISO-Columbus and DISO-Denver Centers against time-to-arrival or time-to-repair requirements, as discussed in Finding A. Tables 4. and 5. give statistical projections of the sample data on

improperly authorized program changes at the DISO-Denver Center, as discussed in Finding E.

Table 1. Projected Number and Percentage of Hardware-Related Abnormal Endings to Computer Operations at the DISO-Columbus Center

	90-Percent Confidence Level			
	Lower Bound	Point Estimate	Upper Bound	Absolute Precision
Number	3,638	4,561	5,484	
Percentage	39.4	49.4	59.3	+/- 10.0

Using a 90-percent confidence level, from 3,638 (39.4 percent) to 5,484 (59.3 percent) of the 9,242 ABENDS in our audit universe resulted from hardware problems. The unbiased point estimate of 4,561 hardware-related ABENDS (49.4 percent) is the most likely number of ABENDS due to hardware problems.

Table 2. Projected Number and Percentage of Hardware-Related Abnormal Endings to Computer Operations Where Vendors Exceeded the Time-to-Arrival Requirements in Making Remedial Maintenance Calls at the DISO-Columbus Center

	90-Percent Confidence Level			
	Lower Bound	Point Estimate	Upper Bound	Absolute Precision
Number	2,760	3,361	3,962	
Percentage	60.5	73.7	86.9	+/- 13.2

Using a 90-percent confidence level, remedial maintenance calls made on from 2,760 (60.5 percent) to 3,962 (86.9 percent) of the projected 4,561 hardware-related ABENDS experienced during FY 1992 (see Table 1.) exceeded the time-to-arrival requirements specified in the ADP equipment contracts. The unbiased point estimate of 3,361 ABENDS (73.7 percent) is the most likely number of hardware-related ABENDS where the vendor was tardy in arriving at the work site.

Table 3. Projected Number and Percentage of Remedial Maintenance Calls Exceeding Time-to-Repair Requirements at the DISO-Denver Center

	90-Percent Confidence Level			
	Lower Bound	Point Estimate	Upper Bound	Absolute Precision
Number	56	149	243	
Percentage	6.6	17.5	28.4	+/- 10.9

Using a 90-percent confidence level, from 56 (6.6 percent) to 243 (28.4 percent) of the 854 remedial maintenance calls made between October 1991 and May 1992 exceeded the time-to-repair benchmarks specified in the ADP equipment contracts. The unbiased point estimate of 149 remedial maintenance calls (17.5 percent) is the most likely number of calls made in which the vendor was tardy in making equipment repairs.

Table 4. Projected Number and Percentage of Improperly Authorized Program Changes in JSS-AC

	90-Percent Confidence Level			
	Lower Bound	Point Estimate	Upper Bound	Absolute Precision
Number	110	171	232	
Percentage	16.9	26.2	35.4	+/- 9.3

Using a 90-percent confidence level, of the 655 program changes to JSS-AC, from 110 (16.9 percent) to 232 (35.4 percent) program changes were authorized improperly. The unbiased point estimate of 171 program changes (26.2 percent) is the most likely number of improperly authorized changes.

Table 5. Projected Number and Percentage of Improperly Authorized Program Changes in JSS-RC

	90-Percent Confidence Level			
	Lower Bound	Point Estimate	Upper Bound	Absolute Precision
Number	32	44	56	
Percentage	25.3	34.6	44.0	+/- 9.4

Using a 90-percent confidence level, from 32 (25.3 percent) to 56 (44.0 percent) of the 128 program changes were improperly authorized. The unbiased point estimate, 44 program changes (34.6 percent), is the most likely number of improperly authorized changes.

Appendix D. Summary of Potential Benefits Resulting from Audit

Recommendation Reference	Description of Benefit	Amount and/or Type of Benefit
A.1.	Economy and efficiency. Monitor ABENDS to reduce computer downtime at all DISO Centers.	Nonmonetary.
A.2.a., b., c., and d.	Compliance. Provide better planning and control at all DISO Centers over the maintenance of ADP equipment and payments made to vendors.	Nonmonetary.
B.1.a.	Compliance. Ensure the security of ADP operations by conducting periodic reviews at the DISO-Columbus Center.	Nonmonetary.
B.1.b.	Compliance. Ensure that the Annual Statement of Assurance issued by the DISO-Columbus Center provides complete disclosure.	Nonmonetary.
B.2.	Compliance. Ensure that the Annual Statement of Assurance issued by the DISO-Indianapolis Center provides complete disclosure.	Nonmonetary.
B.3.	Compliance. Establish a single point of contact for systems security at the DISO-Denver Center.	Nonmonetary.
C.1.a.	Compliance. Ensure that system passwords are periodically changed to prevent unauthorized access at the DISO-Columbus Center.	Nonmonetary.
C.1.b.	Compliance. Ensure that security plans are periodically tested and documented at the DISO-Columbus Center.	Nonmonetary.

Appendix D. Summary of Potential Benefits Resulting from Audit

Recommendation Reference	Description of Benefit	Amount and/or Type of Benefit
C.2.	Compliance. Verify that contract personnel possess the required National Agency Checks before they receive unescorted access to computer facilities at the DISO-Denver Center.	Nonmonetary.
D.1.	Compliance. Ensure that physical safeguards protect computer assets against fire, water, and other hazards at the DISO-Denver Center.	Nonmonetary.
D.2.	Compliance. Ensure that physical safeguards protect computer assets against fire, water, and other hazards at the DISO-Indianapolis Center.	
E.1. and E.2.	Compliance. Ensure that adequate controls exist over changes made to application programs at the DISO-Denver Center.	Nonmonetary.
E.3.	Compliance. Strengthen internal controls over application program changes at the DISO-Denver Center by enforcing existing procedures.	Nonmonetary.

Appendix E. Organizations Visited or Contacted

Office of the Secretary of Defense

Office of the Secretary of Defense (Command, Control, Communications and Intelligence), Washington, DC

Defense Agencies

Defense Information Systems Agency, Washington, DC
- Headquarters, Defense Information Services Organization, Denver, CO*
  - Defense Information Services Organization, Information Processing Center, Columbus, OH
  - Defense Information Services Organization, Information Processing Center, Denver, CO
  - Defense Information Services Organization, Information Processing Center, Indianapolis, IN

Defense Finance and Accounting Service-Denver Center, Denver, CO

* Effective September 7, 1993, the Defense Information Technology Services Organization and its local information processing activities were reorganized under the Defense Information Services Organization and its information processing centers.

Appendix F. Report Distribution

Office of the Secretary of Defense

Comptroller of the Department of Defense
- Deputy Comptroller (Management Systems)
  - Director, Management Improvement, Office of the Deputy Comptroller (Management Systems)
- Deputy Comptroller (Program/Budget)

Assistant Secretary of Defense (Command, Control, Communications and Intelligence)
Assistant to the Secretary of Defense (Public Affairs)

Defense Agencies

Director, Defense Finance and Accounting Service-Columbus Center
Director, Defense Finance and Accounting Service-Denver Center
- Director, Financial Systems Activity Directorate, Defense Finance and Accounting Service-Denver Center

Director, Defense Finance and Accounting Service-Indianapolis Center
Director, Defense Information Services Organization
- Director, Defense Information Services Organization, Information Processing Center, Columbus, Ohio
- Director, Defense Information Services Organization, Information Processing Center, Denver, Colorado
- Director, Defense Information Services Organization, Information Processing Center, Indianapolis, Indiana

Director, Defense Logistics Studies Information Exchange

Non-DoD Federal Organizations

Office of Management and Budget
U.S. General Accounting Office
- Information Management and Technology Division
- Technical Information Center, National Security and International Affairs Division

Chairman and Ranking Minority Member of Each of the Following Congressional Committees and Subcommittees:

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Governmental Affairs
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Committee on Government Operations
House Subcommittee on Legislation and National Security, Committee on Government Operations

Part IV - Management Comments

Defense Finance and Accounting Service

DEFENSE FINANCE AND ACCOUNTING SERVICE
DENVER CENTER
6760 E IRVINGTON PLACE
DENVER, COLORADO 80279

DFAS-FSADE

January 12, 1994

MEMORANDUM FOR DISO-UAR

SUBJECT: Response on Audit Report 2FD-2002

We are forwarding our management comments regarding Finding E of Audit Report (2FD-2002) on General Controls for Computer Systems at the Information Processing Centers of the Defense Information Services Organization.

Please be aware that we did not receive an audit outbriefing. This would have allowed us to comment and clarify some of the findings which were addressed in the report. We hope in the future these will be scheduled.

The FSADE point of contact is Ms. Carol Wadleigh, FSADE/R, DSN 926-7961.

Malcolm G. Parks
Director, Denver FSA

Attachment

Final Report Reference

Audit Report 2FD-2002

FSADE Management Comments on Finding E

Finding Discussion. Concur in Part. Disagree with discusion in IBM Superzap Utility Paragraph. The application software programmers are not authorized access to this utility. The DISO system software technical office is the only authorized user. To further clarify, Computer Associates personnel issue their system software maintenance releases in Superzap format. Application modules include system software utilities during compilation. Therefore, the compiled listings can show changes made by Superzap. However the reference applies to the system software accessed during compilation. The superzap utility changes do not apply to application development software changes.

Review of authorized Superzap users was performed 14 Dec 93 by the AIS Security Manager, DISO-UMIDS. No DJMS and DDMS application users are identified as authorized users.

The DFAS-FSA-DE has no record of having received an audit outbrief where some of the finding could have been addressed and either deleted or clarified. This is particularly applicable to the comments on use of the Superzap utility. Such outbriefs by auditors are customarily held and we hope in the future will be scheduled.

Recommendation 1a. Concur. The Denver FSA will perform a review to ensure all procedures, the same as or similar to those established in Joint Service Software Directorate Operating Instructions 205-3 are followed. Strong emphasis has been placed on the importance of proper certification move authorizations. The review will be accomplished as part of this years internal control review (30 Sept 94). Recommendation 1.

Recommendation 1b. Concur. DDMS controls are now in place to comply with this recommendation. Moves to production are controlled and completed by personnel outside of both the testing and programming branches. Each branch performs a distinct separate function (programming, testing, and moves to production). Completed July 1993. Recommendation 2.

Recommendation 1c. Concur. We have determined that Superzap is not authorized for use by the application development technical staff. It's use is limited to the DISO system software technical office. JSS-AC has not used the Superzap utility in a production environment in over 5 years and has no intention at this time of using it. It was used on a very limited basis prior to 1988 to prevent data from being written to the operator's console. A review of the current JSS proc and control libs (dated 4 Jan 94) shows no reference to this particular utility. Deleted

No one in the DDMS Development branch has the training or capability to use the Superzap utility. The "fixes' are to current releases of technical system utility software - not to DDMS programs.

Final Report Reference

Audit Report 2FD-2002

FSADE Management Comments on Finding E (cont.)

Recommendation 3.

Recommendation 2. Concur. The DFAS FSA-Denver will reemphasize to all development personnel the necessity to fully comply with the requirements of Joint Service Software Directorate Operating Instruction 205-3. All personnel will be briefed on the requirement for segregation of duties for programming, testing, and moving programs to production. They will also be briefed on the necessity and reason for the certifier to be a different individual than the programmer. Directorate level formal policy statements have been directed to be issued to convey policy to all levels. Verbal directive has already been accomplished. Estimated completion date: 15 Feb 1994.

Defense Information Systems Agency

Final Report
Reference

DEFENSE INFORMATION SYSTEMS AGENCY
701 S. COURT HOUSE ROAD
ARLINGTON, VA 22204-2199

IN REPLY REFER TO: AGA

25 January 1994

MEMORANDUM FOR INSPECTOR GENERAL, DEPARTMENT OF DEFENSE
ATTN: Director, Financial Management Directorate

SUBJECT: Audit Report on General Controls for Computer Systems at the Information Processing Centers of the Defense Information Services Organization (Project No. 2FD-2002)

Reference: DoDIG Memo, subject as above, 22 Nov 93

1. As requested by the referenced memorandum, the Defense Information Systems Agency (DISA) has reviewed the subject report, and our comments on Findings A through D are provided at enclosure 1.

2. We are not at liberty to comment on Finding E as it discusses Central Design Activity (CDA) functions no longer under the purview of DISA. However, in order to provide timely management comments to the draft, we asked the Defense Finance and Accounting Service (DFAS) to comment on this finding. Their comments are provided at enclosure 2.

Page 44

3. If you have questions on our response, the point of contact for this action is Ms. Sandra Leicht, Audit Liaison, DSN 222-5326 or commercial (703) 692-5326.

FOR THE DIRECTOR:

2 Enclosures a/s

RICHARD T. RACE
Inspector General

112 94

DISA COMMENTS ON DRAFT AUDIT OF GENERAL CONTROLS FOR COMPUTER SYSTEMS AT DISO IPCs (PROJECT NO. 2FD-2002)

1. **FINDING A:** Operational Improvements

a. **Recommendation 1:** Concur In Part

Planned Action: Although no formal quality assurance program is in place, production abnormal endings (ABENDS) have been tracked and analyzed on a daily basis for several years. Corrective actions are discussed with management and implemented as required. The DISA/DISO Computer Operations Directorate is planning to implement an automated restart/rerun executive software package that will automate ABENDS recovery. This software will reduce manual intervention in ABENDS handling.

Estimated Completion Date: 31 Mar 94

b. **Recommendation 2:** Concur

Planned Action: DISO will implement internal controls identified in recommendation 2 for improving management of preventive maintenance contracts.

Estimated Completion Date: 31 Mar 94

2. **FINDING B:** ADP Security Oversight

a. **Recommendation 1a:** Concur

Planned Action: A recertification review of the installation's computer systems will be conducted during FY94 as required by OMB Circular A-130, "Management of Federal Information Resources."

Estimated Completion Date: 30 Sep 94

b. **Recommendation 1b:** Concur

Planned Action: Director, DISO reported an open material weakness entitled "Operating System and Security Software Controls" in his FY93 Annual Assurance Statement, 27 Sep 93.

Estimated Completion Date: 31 Aug 94

c. **Recommendation 2:** Concur

Planned Action: The IPC Internal Management Control (IMC) Focal Point completed initial IMC Program training on 1 Nov 89. As required by the DISA IMC Program, periodic

refresher courses will be provided for all IPC managers on the IMC Program. The DISO IMC Focal Point will provide additional on-site training to the Indianapolis IPC managers and focal point in FY 1994.

Estimated Completion Date: 30 Apr 94

d. **Recommendation 3:** Concur

Planned Action: A personnel action transferring the employee responsible for security on the Case Management Control System (CMCS) to the Automated Information System (AIS) Security Office was completed on 12 Jan 94. This individual now reports directly to the AIS Security Officer for the Denver IPC, who will ensure all computer applications meet minimum AIS security requirements.

Estimated Completion Date: Action completed 12 Jan 94.

3. **FINDING C:** Controls Over Access

a. **Recommendation 1a:** Concur In Part

Planned Action: Although we concur with the finding, we do not concur with the recommendation. We are in the process of implementing an Automated Password Change Facility on all mainframe applications. This will force the users to change their password every 90 days and will ensure that the password conforms to the DoD standard.

Estimated Completion Date: The Automated Password Change Facility is scheduled to be on all mainframe applications by 30 Mar 94.

b. **Recommendation 1b:** Concur

Planned Action: Our Columbus IPC is a tenant activity on a Defense Logistics Agency (DLA) installation which is functioning under the DLA Physical Security Plan. This plan is tested regularly and observed deficiencies are documented and corrected. Copies of test reports will be obtained from the installation security office and retained.

Estimated Completion Date: 28 Feb 94

c. **Recommendation 2:** Nonconcur

Planned Action: There is no requirement for vendors' maintenance employees to have a security clearance because they do not have access to any classified information. Also, office instructions have been in place prior to 1986 that limit unescorted access to the computer facility to only those persons

Final Report Reference

with completed favorable national agency checks. Each vendors' maintenance employees needing unescorted access to the DISO-Denver Center computer facility does have a current national agency check. Confirmation on an annual basis is not performed as it is not a requirement of DoD 5200.2-R.

4. **FINDING D:** Environmental Protection

a. **Recommendation 1:** Concur

Planned Action: As a tenant organization of the Defense Finance and Accounting Service, Denver Center (DFAS-DE), the Denver IPC has submitted a request for overhead shutoff valves or control valves to be installed in the Computer Center. DFAS-DE is currently evaluating an environmental monitoring control system which may satisfy all requirements for heat detection systems reflected in the recommendation. If purchased, this equipment will be installed by DFAS-DE after the closure date for Lowry AFB.

Estimated Completion Date: Jul 94

b. **Recommendation 2:** Correct physical protection deficiencies listed in Appendix B. Concur

1) Caustic or flammable cleaning agents in the computer room are not kept in approved containers. Deleted

Planned Action: The IPC does have an approved storage container for caustic or flammable cleaning agents. Policies and procedures are in effect for the proper storage of cleaning agents. Deficiency closed 15 Dec 93.

2) The smoke/fire detection system in the computer room does not shut down or reverse the air flow of the ventilation system.

Planned Action: Work request submitted 10 Dec 93.

3) There is no smoke/fire detection system in the computer room's equipment cabinets. Deleted

Planned Action: All central processing units and peripherals are equipped with heat sensors which are alarmed at 130 degrees and trigger shut down of the equipment at 160 degrees. In addition, the computer room itself is equipped with smoke/heat detectors in the ceiling and floor. Deficiency closed 15 Dec 93.

4) There is no equipment in the computer room to exhaust smoke/combustion products directly to the outside atmosphere.

Final Report Reference

Planned Action: Work request submitted 10 Dec 93.

5) Alarms for air conditioning failure, airflow restriction, rising temperatures and humidity fluctuations cannot be heard outside the computer room.

Planned Action: Work request submitted 10 Dec 93.

6) No automatic fire dampers are installed in the building ductwork.

Planned Action: Work request submitted 10 Dec 93.

Deleted

7) No separate, secure communications lines are used for computer systems.

Planned Action: This deficiency applies only to the Hewlett-Packard 3000/70 Mini-Computer which does not process classified data. Nearly all processing is done "in-house" and the only data which is communicated outside the building is a small volume of data downloaded to National Guard life insurance carriers. This life insurance data is neither classified nor sensitive and is readily available from printed sources (we download it as a convenience to our users and to facilitate better service for the Guard members). Deficiency closed 15 Dec 93.

Deleted

8) Computer records can be accessed from unauthorized terminals.

Planned Action: This deficiency applies only to the Hewlett-Packard 3000/70 Mini-Computer. Because of the networked "virtual terminal" nature of our communications, it is not possible to verify actual physical terminal devices. However, the security software on the system verifies the user-ID, password, communications port/line and time of access. Deficiency closed 15 Dec 93.

Deleted

9) The information processing center's power supply is not monitored to detect electrical transients.

Planned Action: The computer facility is equipped with an uninterruptible power supply system. This system monitors electrical transients and is automatically activated whenever commercial power is interrupted. Deficiency closed 15 Dec 93.

Deleted

10) Some emergency exits from the computer room have no alarms.

Planned Action: All emergency exits were alarmed by Sep 91.

Final Report Reference

11) No records of software modifications are kept. Deleted

Planned Action: This deficiency addresses only the Hewlett-Packard 300/70 Mini-Computer and is incorrect. All software modifications are recorded on a standard "Work Request" form. All requests are approved by the Branch Chief, Division Chief, Director, and Director of the Information Processing Center. These forms are individually numbered and kept on file for over two years. Deficiency closed 15 Dec 93.

12) The computer's operating system does not disconnect inactive remote terminals. Deleted

Planned Action: This deficiency applies only to the Hewlett-Packard 3000/70 Mini-Computer. The nature of the on-line work performed by our users (data entry clerks) requires frequent cross-checking with records on other computers and in hard copy files and conferring with supervisors and co-workers. This cross-checking must be performed often while in the middle of screen-form updates. Disconnection of inactive terminals would result in major losses of data, losses of productivity, and would jeopardize the ability of DFAS-IN to meet legally mandated payment deadlines. Terminals left on-line after normal duty hours are automatically disconnected each evening, unless the application managers make special arrangements for their users to work overtime that night/weekend. Deficiency closed 15 Dec 93.

13) No surveillance or sensor devices are used in the computer room. Deleted

Planned Action: The computer facility is located in a building which is access controlled by a 24-hour security guard force. Entrance to the computer facility is restricted by an electronic, controlled access system which is in operation 24 hours a day, 7 days a week. The system requires the use of a magnetically encoded card and a personal code number to gain access to the computer room. The area surrounding the computer facility is monitored by a closed circuit television system. Deficiency closed 15 Dec 93.

14) Computer transmission lines are not checked for bugs, wiretaps, or connection of unauthorized terminals. Deleted

Planned Action: This deficiency is incorrect. Sensitive data is transmitted across encrypted communication lines where required, and access to these lines is limited by terminal-ID as well as user-ID and password. All incoming and outgoing dialup lines are constantly monitored for repeated failed access attempts. In addition, transactions dealing with sensitive data are limited by terminal-ID. That ID is verified, and problem incidents are logged and researched. These security checks are more than adequate for the sensitivity level of data

Final Report Reference

processed on this platform. Deficiency closed 15 Dec 93.

15) No physical inventories are made to account for all computer storage devices.

Planned Action: A 100% physical inventory was completed by Contractor (Peat Marwick) and Government employees in Jun 93.

Deleted

16) Standard test programs are not run frequently to check the validity of on-line software. Updates to vendor-supplied software are not authenticated upon receipt.

Planned Action: Installation verification programs are run after all new installs of software and exceptions are noted and corrected. On-line software, in addition to all other software, is installed using IBM's System Maintenance Procedure (SMP) wherever possible. SMP contains verification statements that require a specific code to be present to the existing production versions before the replacement of code takes effect. Tests are conducted with the new software in order to validate the change. Review of updates are accomplished in accordance with the Standard Operating Procedures which govern changes to production software. Deficiency closed 15 Dec 93.

17) Windows on the interior of the computer room do not have embedded wire support to prevent shattering.

Planned Action: Work request submitted 10 Dec 93.

Deleted

18) Unsuccessful attempts to use passwords are not recorded in computer-based audit records.

Planned Action: This deficiency addresses only the Hewlett-Packard 3000/70 Mini-Computer and is incorrect. All logon attempts are logged to the system log file (the security software's log file) and the system operator's console. Unsuccessful attempts are "flagged" for special attention. Deficiency closed 15 Dec 93.

Deleted

19) Computer users have no assurance that they are connected to the intended computer system instead of an unauthorized system.

Planned Action: This deficiency applies only to the Hewlett-Packard 3000/70 Mini-Computer. The HP-3000 has no front-end-processor to provide system identification prior to connection and the operating system has no means of providing such identification prior to logon. Upon successful logon, the user receives confirmation of the system and application module to which they are connected. Deficiency closed 15 Dec 93.