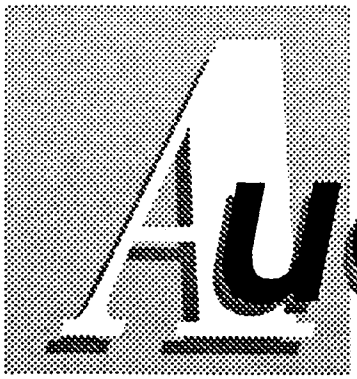

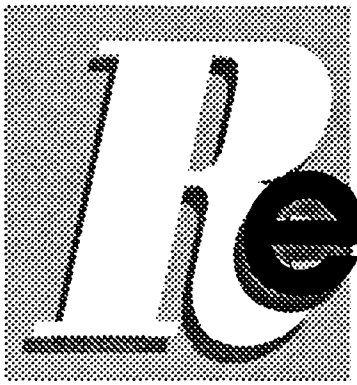

OFFICE OF THE INSPECTOR GENERAL

OPERATIONS AT THE DEFENSE MEGACENTER ST. LOUIS, MISSOURI

Report No. 95-211 May 31, 1995

Department of Defense

Additional Copies

Copies of the report can be obtained from the Secondary Reports Distribution Unit, Audit Planning and Technical Support Directorate, at (703) 604-8937 (DSN 664-8937) or FAX (703) 604-8932.

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) 604-8939 (DSN 664-8939) or FAX (703) 604-8932. 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, contact the Defense Hotline by calling (800) 424-9098; by sending an electronic message to Hotline@DODIG.OSD.MIL; or by writing to the Defense Hotline, The Pentagon, Washington, D.C. 20301.1900. The identity of each writer and caller is fully protected.

Acronyms

DISA	Defense Information Systems Agency
DMC	Defense Megacenter
WESTHEM	Western Hemisphere

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

Report No. 95-211 May 31, 1995

MEMORANDUM FOR DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY

SUBJECT: Audit of the Operations at the Defense Megacenter, St. Louis, Missouri (Project No. 4RE-5034.01)

Introduction

We are providing this report for your information and use. We performed this audit in response to a request from the Inspector General, Defense Information Systems Agency (DISA), for assistance in reviewing the operations of the Defense megacenters. The report discusses the operations at the Defense Megacenter (DMC) St. Louis, Missouri. We also issued Audit Report No. 95-140, "Staffing Requirements for the Defense Megacenters," March 9, 1995, which discusses the personnel staffing requirements for the 16 Defense megacenters.

Audit Results

The DISA Western Hemisphere (WESTHEM) is taking adequate steps to ensure that DMC St. Louis operations are effective and efficient. DISA WESTHEM is evaluating, developing, and implementing policies and procedures for contingency planning, security controls, system software, fee-for-service and customer billings, customer identification, and computer operations. During the audit, we made suggestions to improve minor weaknesses in contract administration and administrative management. DMC St. Louis personnel agreed to develop and implement policies and procedures to correct those weaknesses.

Objective

The objective of the audit was to evaluate the efficiency and effectiveness of the operations at the DMC St. Louis, Missouri. Also, we announced an objective to review the management control program as it applies to the operations of the DMC St. Louis.

We did not evaluate the adequacy of the management control program at DMC St. Louis, because at the time of the audit, DISA WESTHEM was developing and implementing a management control program for each DMC.

Scope and Methodology

Audit Scope and Methodology. We evaluated applicable policies, procedures, guidelines, directives, and instructions relating to the operations at DMC St. Louis. We reviewed documentation, dated February 1993 through March 1995, on procedures for security, contracting, computer operations, and customer relations and services. We used judgmental sampling methods to verify whether control techniques were in place and effective to safeguard assets from loss, impairment, or misuse. We did not rely on computer-processed data or statistical sampling procedures to achieve the audit objective.

Audit Period, Standards, and Potential Benefits. We performed the audit from May 1994 through March 1995 at the organizations listed in Enclosure 2. We performed this economy and efficiency audit in accordance with auditing standards issued by the Comptroller General of the United States as implemented by the Inspector General, DoD. As previously discussed, we did not test the management controls. Enclosure 2 lists the organizations visited or contacted during the audit.

Prior Audits and Other Reviews

We identified numerous General Accounting Office and Inspector General, DoD, audits that related to general and operational controls at Defense megacenters. The two audit reports below relate to the review of general controls at DMCs. Enclosure 1 provides a summary of additional audit reports.

Inspector General, DoD, Audit Report No. 94-060, "General Controls for Computer Systems at the Information Processing Centers of the Defense Information Services Organization," March 18, 1994. The report concludes that the general controls over the operations and physical protection of Defense Information Services Organization information processing centers at Denver, Columbus, and Indianapolis were adequate. However, the audit identified weaknesses in that the centers at Denver, Columbus, and Indianapolis had not established:

- requirements for conducting periodic reviews of automated data processing security and for analyzing management controls over automated data processing operations;

- centralized authority over all automated data processing security policies and safeguards; and

- controls over access to computer rooms, equipment, sensitive documents and forms, and application programs.

The report recommends that the Directors of the Defense Information Services Organization in Denver, Columbus, and Indianapolis assign responsibility for security control and oversight to the information system security officer for the Case Management Control System, obtain and implement an automated control for password changes, and schedule periodic tests of the physical security plan

and retain evidence of testing. Management concurred with recommendations for corrective actions and implemented the necessary management controls to correct weaknesses.

Audit Background

Defense Information Systems Agency's Designation as Central Manager of Defense Information Infrastructure. The Defense Management Report Decision 918, September 15, 1992, designated the Defense Information Systems Agency as the central manager for the Defense Information Infrastructure. In that capacity, DISA is responsible for information technology security, standards, long-haul communications, telecommunications certification, and data processing facilities. DISA established the Defense Information Services Organization,[1] now DISA Western Hemisphere, to manage the data processing facilities and to provide information technology services to DoD customers. In 1993, DISA developed and coordinated, with the FY 1993 Commission on Base Closure and Realignment, the DoD Data Center Consolidation Plan (the Consolidation Plan), dated July 16, 1993, to consolidate data processing facilities into 16 Defense megacenters that will provide centralized information processing to DoD customers. DISA WESTHEM efforts to consolidate the facilities into 16 Defense megacenters began in the fourth quarter of FY 1993 with completion estimated for the fourth quarter of FY 1996.

Creation of the Defense Megacenter St. Louis, Missouri. The Consolidation Plan identified the Army Information Processing Center, St. Louis, Missouri, as one of the 16 Defense megacenters. On October 1, 1993, the U.S. Army Information Systems Command transferred responsibility for personnel at the Army Information Processing Center to DISA. On February 1, 1994, DISA assumed operational control over the Army Information Processing Center, and it officially became the DMC St. Louis.

The DMC St. Louis provides data processing services to the Army and Marine Corps and plans to service Air Force components. The DMC St. Louis processes data and computer applications in functional areas such as logistics, personnel, finance, and training. As of May 1994, DMC St. Louis serviced about 25,000 on-line end users.[2] In November 1995, when the transfer of Marine Corps and Air Force work load to DMC St. Louis is completed, the number of on-line end users will exceed 70,000.

[1]Formerly, Defense Information Technology Services Organization.
[2]The people ultimately using the applications, data, and output of the processing functions at the DMC St. Louis.

Discussion

At the time of the audit, DISA WESTHEM was evaluating, developing, and implementing policies, procedures, and processes, for contingency planning, security controls, and fee-for-service and customer billings at the Defense megacenters.

Contingency Planning for the Defense Megacenters. The Operations Directorate, DISA WESTHEM, in conjunction with the Service Center Directorate, DISA WESTHEM and legacy[3] information processing centers, is responsible for the contingency planning for all the Defense megacenters. The contingency planning includes identifying and contracting for a computer data processing site that will be used for back up and recovery of computer processing, in case a defense megacenter is unable to operate. DISA WESTHEM is scheduled to have a single backup computer data processing site operational by July 1995.

Security Controls Over the Operations at DMC St. Louis. DISA established the Information Security Task Force (Task Force) on April 29, 1994, to enhance information security so that the DMCs could provide the required level of protection for the customers' data and application systems. Additionally, the Task Force performed security readiness reviews at each DMC. The security readiness reviews included reviews of the controls over physical security, for example, entry control, base perimeters, building, and card access system; and logical security, for example, operating software integrity and installation and implementation of the access control program (security software). The Task Force completed the security readiness review for the DMC St. Louis in March 1995. During May 1995, the Task Force will establish milestones for actions to correct identified weaknesses.

Procedures for Changing Operating Systems Software and Utilities. The DMC St. Louis did not maintain a centralized software change control log to document the source, date, purpose, and nature of changes to the operating system software. Without documented justification for changing system software, the potential exists for the software to be compromised. The Task Force included a review of procedures for changes to software as part of the security readiness reviews.

Fee-for-Service and Customer Billings for DISA WESTHEM Customers. DISA WESTHEM is developing the fee-for-service, unit cost process. In FY 1995 DISA WESTHEM will send notional billings to introduce the DoD customers, except for Army, to the billing procedures under the fee-for-service program. Notional billings show the customer the total cost of service received based on set rates and usage; however, the customer pays only the amount agreed upon in the service-level agreement. Customers will not pay for actual services received until the fee-for-service program is fully implemented in FY 1996.

---

[3]A legacy information processing center is a center for which data processing work will be transferred to a defense megacenter.

Customer Identification at DMC St. Louis. At the time of the audit, DISA WESTHEM was implementing standard codes to better identify specific customers on automated invoices. Implementing the standard codes will help ensure successful implementation of the fee-for-service program at DISA WESTHEM.

Computer Operations at the DMC St. Louis. We limited the review of computer operations to the controls over property accountability. The controls over property accountability are adequate to verify that property is accounted for and safeguarded from theft, loss, impairment, or misuse. We inventoried the major equipment items in the computer room and did not identify significant problems.

Observations and Suggestions to Correct Minor Weaknesses at DMC St. Louis

During conferences with management officials at DMC St. Louis, we discussed minor weaknesses in contract administration and overall management at DMC St. Louis. Observations and suggested improvements are discussed below.

Contract Administration Policies and Procedures at DMC St. Louis. DMC St. Louis had not established local policies and procedures for contracts administered at DMC St. Louis. Specifically DMC St. Louis:

- overpaid $11,170 for maintenance cost for equipment that was no longer in use, but had not been deleted from the maintenance contract,
- did not collect $3,100 in penalties when the contractor did not repair and return computer equipment to operations according to contract schedule, and
- did not verify that the contractor performed $2.2 million in scheduled preventive and engineering change maintenance tasks.

As a result, the contractor is not meeting the terms of the contract with DMC St. Louis. We suggested that DMC St. Louis develop and implement policies and procedures for contract administration. DMC St. Louis management agreed to develop and implement policies and procedures to monitor contractor support.

Policies and Procedures at DMC St. Louis. Management officials at DMC St. Louis have developed policies and procedures for administrative and operational functions. However, most of those policies and procedures are not documented. We suggested that DMC St. Louis managers document standard policies and procedures for the functions performed at DMC St. Louis.

We appreciate the cooperation and courtesies extended to the auditors. If you have any questions on this audit, please contact Ms. Mary Lu Ugone, Audit Program Director, at (703) 604-9529 (DSN 664-9529), or Ms. Cecelia Miggins, Audit Program Manager, (703) 604-9542 (DSN 664-9542). Enclosure 3 lists the report distribution. Audit team members are listed inside the back cover.

David K. Steensma

David K. Steensma
Deputy Assistant Inspector General
for Auditing

Enclosures

Summary of Prior Audit Reports

In addition to the prior audits discussed in the report, we identified the following audit reports that discuss the controls at information processing centers.

General Accounting Office Report No. GAO\AIMD-94-12 (OSD Case No. 9276-D), "Financial Management: Strong Leadership to Improve Army's Financial Accountability," December 22, 1993. The report discusses the weaknesses in systems that account for and report the Army disbursements and inadequate controls over automated data processing of financial and logistics information. The report recommends that DoD and Army:

o ensure compliance with policies and procedures established to provide control over disbursements,

o improve computer hardware and software security, including disaster contingency plans at automated data processing centers, and

o develop and implement a comprehensive plan for improving financial management operations at the organizations.

Management partially concurred with the recommendations and started developing policies to correct the identified weaknesses.

Inspector General, DoD, Report No. 95-066, "Controls over Application Software Supporting the Navy's Inventories Held for Sale (NET)," December 30, 1994. The report discusses material weaknesses in the operating system that caused the integrity of applications to be compromised. The report recommends that general controls be strengthened over the security software; the operating system; and the Computer Associates, Incorporated, Integrated Data Management System data base for the test and production systems supporting the applications. The Navy and the Defense Information Systems Agency concurred with the recommended actions and estimated a completion date of May 1995 for corrective measures.

Inspector General, DoD, Audit Reports at Defense Finance and Accounting Service Organizations. The reports listed below discuss deficiencies in implementing and controlling security software for an operating system. In addition, the reports discuss the need to strengthen controls over the operating system and security software. The deficiencies would allow any knowledgeable user to gain access into pay data, and to add, modify, or destroy them, or enter erroneous data (accidentally or intentionally), without leaving an audit trail. The reports recommend the development and implementation of additional regulatory compliance, enhanced management controls, formal control procedures, additional training for security personnel, and compliance with established security regulations. Management concurred with the recommendations for corrective action and established the Information Security Task Force to correct the weaknesses.

Audit Reports Reviewed as Part of Prior Audit Coverage

o Inspector General, DoD, Report No. 94-065, "Controls over Operating Systems and Security Software Supporting the Defense Finance and Accounting Service," March 24, 1994.

o Inspector General, DoD, Report No. 93-133, "Controls over Operating Systems and Security Software Supporting the Defense Finance and Accounting Service," June 30, 1993.

o Inspector General, DoD, Report No. 93-002, "Controls over Operating Systems and Security Software Supporting the Defense Finance and Accounting Service," October 2, 1992.

Organizations Visited and Contacted

Department of the Army

Aviation and Troop Command, St. Louis, MO
Information Systems Command, Fort Ritchie, MD
Information Systems Support Command, Fort Belvoir, VA
Director of Information Management, Fort Carson, CO
Director of Information Management, Fort Hood, TX
Charles Melvin Price Support Installation Contract Division, Granite City, IL

Defense Organization

Defense Information Systems Agency, Washington, DC
Defense Information Systems Agency, Western Hemisphere, Fort Ritchie, MD
Defense Megacenter St. Louis, St. Louis, MO

Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense (Comptroller)
  Deputy Under Secretary of Defense (Comptroller/Management)
  Deputy Under Secretary of Defense (Comptroller/Program/Budget)
Assistant to the Secretary of Defense (Public Affairs)
Director, Defense Logistics Studies Information Exchange

Department of the Army

Auditor General, Department of the Army

Department of the Navy

Assistant Secretary of the Navy (Financial Management and Comptroller)
Auditor General, Department of the Navy

Department of the Air Force

Assistant Secretary of the Air Force (Financial Management and Comptroller)
Auditor General, Department of the Air Force

Other Defense Organizations

Director, Defense Contract Audit Agency
Director, Defense Information Systems Agency
  Director, Defense Information Systems Agency, Western Hemisphere
    Director, Defense Megacenter St. Louis
Director, Defense Logistics Agency
Director, National Security Agency
Inspector General, Central Imagery Office
Inspector General, National Security Agency

Non-Defense Federal Organizations and Individuals

Office of Management and Budget
Technical Information Center, National Security and
International Affairs Division, General Accounting Office

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 National Security, Committee on Appropriations
House Committee on Government Reform and Oversight
House Subcommittee on National Security, International Affairs, and Criminal Justice, Committee on Government Reform and Oversight
House Committee on National Security

Audit Team Members

This report was produced by the Readiness and Operational Support Directorate, Office of the Assistant Inspector General for Auditing, DoD.

Thomas F. Gimble
Mary Lu Ugone
Cecelia Miggins
Hugh G. Cherry
Rhonda Ragsdale
Kimberly Slater
Nancy C. Cipolla
Cristina Maria H. Giusti