Audit Report

OFFICE OF THE INSPECTOR GENERAL

VENDOR PAYMENTS - OPERATION MONGOOSE

Report No. 96-134 May 30, 1996

DISTRIBUTION STATEMENT A
Approved for Public Release
Distribution Unlimited

Department of Defense

Additional Copies

To obtain additional copies of this audit report, contact the Secondary Reports Distribution Unit of the Analysis, 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 of the Analysis, 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:

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

Defense 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

CAPS	Computerized Accounts Payable System
DFAS	Defense Finance and Accounting Service
DMDC	Defense Manpower Data Center
FAR	Federal Acquisition Regulation
IG	Inspector General
SAACONS	Standard Army Automated Contracting System
SRD1	STANFINS Redesign-1
STANFINS	Standard Army Financial System

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

May 30, 1996

MEMORANDUM FOR DIRECTOR, DEFENSE FINANCE AND ACCOUNTING SERVICE

SUBJECT: Audit Report on Vendor Payments - Operation Mongoose (Report No. 96-134)

We are providing this report for your review and comment. The audit was made in support of Operation Mongoose. This is one in a series of reports on the review of vendor payment and contracting systems.

DoD Directive 7650.3 requires that all unresolved issues be resolved promptly. Management comments on a draft of this report were considered in preparing the final report. The management comments conformed to the requirements of DoD Directive 7650.3. However, Recommendation A.1.e., was not addressed. Therefore, we request that the Defense Finance and Accounting Service comment on the recommendation by June 28, 1996.

We appreciate the cooperation extended by the Defense Finance and Accounting Service staff. Questions on the audit should be directed to Mr. Christian Hendricks, Audit Program Director, at (703) 604-9140 (DSN 664-9140) or Mr. Carl Zielke, Audit Project Manager, at (703) 604-9147 (DSN 664-9147). Copies of the report will be distributed to the Defense Finance Accounting Service. See Appendix E for the report distribution. The audit team members are listed inside the back cover.

Robert J. Lieberman
Assistant Inspector General
for Auditing

Office of the Inspector General, DoD

Report No. 96-134 **May 30, 1996**
(Project No. 5FG-5016)

Vendor Payments - Operation Mongoose

Executive Summary

Introduction. This audit was performed in support of Operation Mongoose. On June 30, 1994, the Deputy Secretary of Defense approved the establishment of Operation Mongoose, jointly staffed by personnel from the Defense Finance and Accounting Service (DFAS), the Defense Manpower Data Center, and the Inspector General (IG), DoD. Executive oversight and direction are provided by the Under Secretary of Defense (Comptroller), and the project is led by DFAS.

The purpose of Operation Mongoose is to develop and operate a fraud detection and prevention unit to minimize fraudulent attack against DoD financial assets.

The IG, DoD, is working with the DFAS and the Defense Manpower Data Center to develop a prototype system to identify transactions that are indicative of potential fraud. There are 11 systems in the prototype, which will be built in 5 phases with each phase adding systems to the prototype. In this audit we included two systems, the Computerized Accounts Payable System and the Standard Army Financial System Redesign-1 at Columbus, Ohio. Our audit focused on the effectiveness of computer routines designed to identify fraudulent vendor payments, and on management controls over vendor payments at the DFAS Columbus Center, Columbus, Ohio. This is one in a series of reports on the five phases of the prototype system.

Audit Objectives. The objectives of this audit were to evaluate the effectiveness of management controls over payments to vendors. We applied computer matching techniques to disbursing transactions to identify irregularities indicative of fraud. We also evaluated management controls over systems designed to prevent and detect erroneous vendor payments.

Audit Results. Operation Mongoose is making progress in identifying ways to improve controls over vendor payments, but developing effective mechanisms has proven to be difficult. Test results showed that 10 of the initial 25 computer routines designed by the Operation Mongoose Team to detect fraudulent vendor payments in the Computerized Accounts Payable System and the Standard Army Financial System Redesign-1 at DFAS Columbus Center could not be relied on to detect potential fraud. Of the 10 ineffective routines, 6 could be more effective in detecting fraud if data formats were standardized, edit controls were incorporated into the system software, and operating procedures were improved and enforced. Four of the initial routines developed by the Operation Mongoose Team were based on incorrect assumptions, three of the four have been dropped from further consideration, and the fourth routine has been redesigned and will be subject to further review. Duplicate payment numbers were used because they were streamlined payments. Streamlined payments are directly processed through the disbursement system, bypassing validation controls in the Computerized Accounts Payable System. The effective routines identified $208,404 in actual and potential duplicate payments and overpayments; however, no potentially fraudulent payments were identified. We could not validate 110 (15 percent) of the 750 vendor payments because accounting technicians did not follow local sign-out

procedures and could not locate the contract payment files. As a result, we could not determine whether potential fraudulent payments occurred on the 110 vendor payments. Taken together, however, the test results corroborated that management controls over vendor payments need to be made more effective and the routines developed under Operation Mongoose can assist DFAS toward that end (Finding A).

Security over automated payment records needed strengthening. Of 1,110 users given authorized access to the local area network with access to the vendor payment system, 681 did not have an assigned password. Without an assigned password, any employee can sign onto the system and assign his or her own password. Some users were given access to automated payment records that allowed them to add, delete, and change records without leaving an automated audit trail. Therefore, fraudulent payments could be processed without detection by the system (Finding B).

Potential Benefits of Audit. The audit identified $97,878 in actual duplicate payments and overpayments, and $110,526 in potential duplicate payments and overpayments. We notified the DFAS Columbus Center's accounts receivable section of these payments for their research and collection action. These potential monetary benefits were identified from a limited sample of transactions that we reviewed while analyzing the 25 computer routines. Implementing our recommendations will also improve management controls over access to vendor payment data.

Summary of Recommendations. We recommend that the Director, DFAS, establish standardized input formats and implement edit checks in the Computerized Accounts Payable System and the Standard Army Financial System Redesign-1. We also recommend that the Director, DFAS Columbus Center, establish procedures to ensure that all vendor payments are processed through the Computerized Accounts Payable System, that data are properly safeguarded from compromise, and missing contract payment files are reconstructed.

Management Comments. The management comments were generally responsive. The Defense Finance and Accounting Service agreed to establish standardized input formats and implement edit checks in the Computerized Accounts Payable System and the Standard Army Financial System Redesign-1. This will be accomplished through system software change requests and the Computerized Accounts Payable System consolidation project estimated to be complete in June 1996. Management disagreed that the Computerized Accounts Payable System needs edit checks to identify duplicate contract numbers between databases. We clarified this issue in our audit response in Part I. Management agreed to use the original payment file to validate payments, but disagreed that the original invoice was needed to support vendor payments if the invoice is researched. We agreed with management's alternative solution. Management agreed to implement the recommendations to properly safeguard data from compromise and located the 110 missing contract payment files. Management did not provide comments on one recommendation. See Part I for a complete discussion of management comments and Part III for the complete text of those comments.

Audit Response. Management did not comment on the recommendation to process a system software change request to incorporate an edit check into the disbursement system to ensure that the electronic funds transfer number is entered into the correct data field. Accordingly, we ask that the Defense Finance and Accounting Service comment on that recommendation in response to this report by June 28, 1996.

Table of Contents

Part I - Audit Results

Audit Background

This audit was performed in support of Operation Mongoose. On June 30, 1994, the Deputy Secretary of Defense approved the establishment of Operation Mongoose, jointly staffed by personnel from the Defense Finance and Accounting Service (DFAS), the Defense Manpower Data Center (DMDC), and the Inspector General (IG), DoD. Executive oversight and direction are provided by the Under Secretary of Defense (Comptroller), and the project is led by DFAS.

On August 5, 1994, the Deputy IG, DoD, and the Under Secretary of Defense (Comptroller) agreed to a concept of operations for Operation Mongoose. The purpose of Operation Mongoose is to develop and operate a fraud detection and prevention unit to minimize fraudulent attack against DoD financial assets. The project targets areas such as civilian, military, and vendor payments. This audit is limited to vendor payments made by the DFAS Columbus Center, Columbus, Ohio, in FY 1994.

In September and October 1994, representatives from the DFAS, the DMDC, and the IG, DoD, met to identify fraud indicators for vendor contract and payment systems in DoD. The indicators were used to develop computer routines for identifying irregular and fraudulent vendor payments. In December 1994, we began developing and testing computer routines against vendor payment data from the Computerized Accounts Payable System (CAPS) and the Standard Army Financial System (STANFINS) Redesign-1 (SRD1) at the DFAS Columbus Center. We made visits to the DFAS Columbus Center from January 9, 1995, through May 5, 1995, to document the payment process and test 25 computer routines for detecting irregular and fraudulent vendor payments.

Agency Responsibility. After a meeting of the DFAS, the DMDC, and the IG, DoD, in May 1995, a memorandum of understanding was drafted to clarify the responsibilities of each agency, as follows.

o The DFAS will coordinate and research the activities of Operation Mongoose and assist in determining the fraud indicators; when the indicators are accepted, DFAS will review the results of the computer runs for potential fraud.

o The DMDC will assist in determining the fraud indicators and will provide computer and programming support.

o The IG, DoD, will review the vendor payment systems, assist in determining the fraud indicators, and assess the reliability of data for Operation Mongoose.

o The IG, DoD, will issue a report on the effectiveness of the automated routines after completing each review. This is the first in a series of reports.

Plans for Operation Mongoose. During this audit, IG, DoD, personnel worked with DFAS and DMDC to develop a prototype system for identifying irregular and fraudulent vendor payment transactions. The final prototype will include 11 systems for vendor contracts and payments. The prototype will be built in five phases. The first phase of the prototype includes the DFAS Columbus Center's CAPS and SRD1. The Standard Army Automated Contracting System (SAACONS) is also included in the first phase; however, the DFAS Columbus Center does not maintain a SAACONS data base. The other eight systems will be included in the next four phases. CAPS contains the payment data and computes payments, and the SRD1 system disburses checks and maintains critical disbursement data. This audit focused on vendor payment data in the CAPS and SRD1 systems and on management controls over vendor payments made at the DFAS Columbus Center.

Development of Computer Routines. Initially, computer routines for tests at the DFAS Columbus Center were developed only for CAPS data. However, we found that SRD1 disbursement data were also needed to collect all vendor payments for the DFAS Columbus Center. Therefore, we changed the computer routines to test the fraud indicators against data in the CAPS and SRD1 systems.

Site and System Selection. Of the 11 vendor systems identified by Operation Mongoose, CAPS was selected for initial review. Of the 42 sites using the CAPS vendor payment system, the DFAS Columbus Center was selected as the initial test site because it had complete data submissions for FY 1994, its annual vendor payments totaled more than $1 billion, and its personnel understood the system.

Potential Benefits of Audit. The audit identified $97,878 in actual duplicate payments and overpayments and $110,526 in potential duplicate payments and overpayments. We notified the DFAS Columbus Center's accounts receivable section of these potential monetary benefits for their research and collection action. These payments were identified from a limited sample of transactions that we reviewed while analyzing the 25 computer routines. Implementing our recommendations will also improve management controls over access to vendor payment data.

Audit Objectives

The objectives of this audit were to evaluate the effectiveness of management controls over payments to vendors. We applied computer matching techniques to disbursing transactions to identify irregularities that indicated potential fraud. We also evaluated management controls over systems designed to prevent and detect erroneous vendor payments.

Audit Scope Limitations

We did not perform a complete test of streamlined payments in the SRD1 system. In FY 1994, streamlined payments totaled $346 million. For streamlined payments, accounting technicians bypass the CAPS process and enter the payment transactions directly into the SRD1 for disbursement action. Normally, vendor payments are entered into the CAPS before being processed through the SRD1. If the payment data are not entered into the CAPS by the accounting technician, the CAPS system will not have a record of the payment. The CAPS includes validation controls that do not reside in the SRD1, which prints and disburses checks. Because of a programming error, our evaluation of streamlined payments was limited. The DMDC is testing streamlined payment data for the DFAS Columbus Center. At other sites, we will perform complete testing of streamlined vendor payments.

Finding A. Fraud Indicators

Progress is being made in developing improved controls over vendor payments, but the task has proven difficult. Test results showed that 10 of the initial 25 computer routines developed by Operation Mongoose were ineffective as tools for detecting fraudulent vendor payments in the Computerized Accounts Payable System (CAPS) and the Standard Army Financial System (STANFINS) Redesign-1 (SRD1) at the DFAS Columbus Center. Of the 10 routines, 6 could be more effective if data formats were standardized, the system software had improved edit checks, and local operating procedures were improved and followed. Four routines were based on incorrect assumptions, three were dropped from further consideration, and the fourth has been redesigned. Duplicate payment numbers were used because streamlined payments bypassed the controls in CAPS. In FY 1994, streamlined payments totaled $346 million of the $1 billion in vendor payments for CAPS and SRD1. The effective routines identified $208,404 in actual and potential duplicate payments and overpayments. Personnel at the DFAS Columbus Center could not locate 110 (15 percent) of the 750 contract files we requested because sign-out procedures had not been followed. As a result, we could not determine whether fraudulent payments occurred on those 110 vendor payments. Taken together, the test results corroborate the need to continue strengthening controls over vendor payments.

Review of Vendor Payment Process for Potential Fraud

Vendor Payment Process. The vendor payment process has four phases: inputting, processing, verifying, and disbursing. Contract information is received at the DFAS Columbus Center from various systems and transferred into one of six CAPS data bases by the DFAS Columbus Center's control section; mailed contracts are input by the commercial pay section. The six data bases are:

- o the Defense Commissary Agency,
- o the Defense Logistics Agency,
- o the Defense Reutilization Marketing Service,
- o the Department of Defense Dependent Schools,
- o the Military Departments, and
- o miscellaneous.

The invoices and receiving documents are received in the mail section, where they are reviewed for completeness. If the documents are not complete, they

are returned to the vendor. After the documents are reviewed by the mail clerks, they are sorted and sent to the commercial pay section. In the commercial pay section, the accounting technician pulls the contract file and matches the invoice and the receiving report to the contract for validation. The accounting technician then enters the data into CAPS, computes the payment, and produces a summary voucher. The contract payment file contains a paper copy of the contract and contract modifications, each invoice and receiving report, and any other correspondence related to the contract. Except for fast-pay contracts, invoices are not paid until the contract, the invoice, and the receiving report are received and validated. The CAPS active payment file retains information on the contract and each payment until 90 days after the final payment is made to the vendor. The final payment is indicated in the payment record with an "f" in the payment number field. After 90 days, records are automatically transferred to the history file and are deleted from the active payment file.

Transmittal letters are printed each day identifying the payments that were made that day in contract number sequence by due date. Each transmittal letter lists up to 20 payments. When the vouchers with the supporting documentation are received in the control section, the vouchers and documentation are matched to the transmittal letters. Each voucher is then compared to the upload file in the CAPS data base by contract number, payment number, and payment amount. When that comparison is completed, CAPS creates the diskette used to enter the data into SRD1. The control section then enters the data on the diskette into SRD1 and files the vouchers by due date for cash management.

One day prior to payment, the control section obtains a listing from the SRD1 of all payments due on the next payment date. The payment documentation is matched to the SRD1 listing and sent to the disbursing and collection division to support the disbursing request. The check numbers and disbursing office voucher numbers are assigned and the official vouchers and checks are printed by SRD1. When the checks have been issued by SRD1, the control team downloads the payment data from SRD1 and uploads the data into CAPS. This transfer of check information to CAPS updates that data base with disbursement data, such as the check number, disbursing officer voucher number, and date of payment.

Streamline payments and fast payment procedures are two practices used to expedite the disbursement process. Streamline payments are processed directly to the disbursement system (SRD1), bypassing validation controls in the CAPS. The payment information is then transferred from SRD1 to CAPS after the payment.

According to the Federal Acquisition Regulation (FAR), Part 13.301, "The fast payment procedure allows payment under limited conditions to a contractor prior to the Government's verification that supplies have been received and accepted." The procedure provides for payment for supplies based on the contractor's submission of an invoice that delivery has been completed according to terms of the purchase agreement.

Analysis of Computer Routines

Our analysis of the 25 computer routines showed that 10 were ineffective and 15 were effective. If the corrections identified during our tests are made, 22 of the 25 routines would detect irregular or potentially fraudulent payments in the CAPS and SRD1 systems.

Ineffective Computer Routines. The 10 computer routines were ineffective for several reasons. Six routines could be effective if:

- o Data were input into CAPS and SRD1 in a standardized format.
- o All streamlined payment data in SRD1 were input into CAPS.
- o The CAPS record had a field that identified fast-pay contracts.
- o CAPS records did not show that multiple final payments had been made on the same contract in CAPS.

Three computer routines identified between 904 and 1,509 transactions that did not identify potentially fraudulent payments. Based on our examination of some of those payment transactions and discussions with accounting technicians, each voucher examiner processes numerous payments to the same vendor. Because this was a common practice, those routines listed too many transactions to review economically. Therefore, those routines were not evaluated further at the DFAS Columbus Center. A fourth routine identified contracts with an award date of FY 1992 or earlier for which one or more payments had been made in FY 1994. These were considered by the Operation Mongoose Team as old contracts with current payments, a potential fraud indicator. However, this was a common practice at the DFAS Columbus Center. The fourth routine has been redesigned to identify contracts awarded before FY 1993 with a break in payments of 1 or more years. The intent is to identify fraudulent payments on old contracts that have been inactive or closed for several years. We will evaluate the effectiveness of the routine at the other activities.

Issues Affecting Computer Routines

The large number of mismatches produced by the 10 ineffective computer routines had 3 main causes: a lack of data standardization, inadequate edit controls, and operational procedures that were either inadequate or were not followed.

Data Standardization. In the CAPS files, the contractor's name, address, and other data fields used to test data validity were not standardized. Accounting technicians entered CAPS data in many different formats. Street, st., road, rd., company, Co., incorporated, and Inc. were examples of nonstandardized data in the CAPS data base. Personnel at the DFAS Columbus Center are instructed to

enter information into the CAPS as documented in the contract; however, vendors' addresses in each contract are not always shown in the same format. This caused mismatches in our tests of the computer routines.

Edit Checks. CAPS software did not contain adequate edit checks to ensure that data were reliable. The General Accounting Office guidance, "Assessing the Reliability of Computer-Processed Data," September 1990, defines data reliability as "a state that exists when data are sufficiently complete and error free to be convincing for their purpose and context."

For reliability, edit checks are needed to ensure that each contract number is unique and does not appear in more than one of the six vendor payment data bases, that each payment address meets a standardized format, and that each payment number is unique. Because those controls were not implemented, an excessive number of transactions were identified as potentially fraudulent payments. Therefore, validation of several hundred transactions listed by some computer routines as potentially fraudulent or irregular payments was uneconomical.

The CAPS and SRD1 did not validate the transactions transferred between the two systems for dollar amounts and transaction totals. Without this validation, transactions could be changed, added, or deleted when transferred between systems without being detected. To ensure that transactions and amounts are not changed, added, or deleted, the dollar amounts and transaction totals should be electronically checked during each transfer of data between systems.

CAPS automatically assigns the payment number to each payment, but in SRD1, the payment number is manually assigned by the accounting technician. When a payment is initiated in CAPS, the SRD1 system uses the same payment number. Payments are streamlined to reduce manual data entry and expedite payments. When the payment is streamlined, it bypasses CAPS and is input directly into SRD1, and two payments with the same payment number may appear in the SRD1. If this occurs, CAPS will not accept the duplicate payment number, and the check information will not be transferred from SRD1 to CAPS. If an accounting technician discovers that the transaction was not electronically transferred, he or she will manually enter it into the CAPS. In FY 1994, the DFAS Columbus Center processed $346 million in streamlined payments. Therefore, all payments should be processed through CAPS before being input into SRD1. This will ensure that each payment has a unique payment number.

Operational Procedures. Operational procedures were inadequate or were not followed by accounting technicians. At the DFAS Columbus Center, payments were sent to vendors with addresses shown on the invoice that differed from the addresses shown on the contracts. The chief of the commercial payments division issued a memorandum, dated February 25, 1994, which stated:

> In accordance with our Defense Finance and Accounting Services - Headquarters Audit and Federal Acquisition Regulation, we will begin returning invoices to vendors as improper when the "Remit-to" address is different from the "Remit-to" address on the contract or purchase order.

> Therefore, as part of our mission, effective March 29, 1994, we must return invoices to vendors when the "Remit-to" address does not match the contract or purchase order.
>
> Please refer to . . . paragraph 52.232-25 (a) (4) (vi) of the FAR which states, "Name and address of the Contractor official to whom payment is to be sent must be the same as that in the contract or in a proper notice of assignment."

Before the memorandum was issued, payments were made to addresses other than those shown on the contract. As of March 29, 1994, managers instructed employees to issue a form letter to the vendor when the remit-to address on the invoice did not agree with the remit-to address shown on the contract. The form letter would require the remit-to address to be changed, through a contract modification, to agree with the remit-to address on the invoice. Otherwise, the vendor would have to resubmit the invoice with a revised remit-to address that agreed with the address shown on the contract. Although the same remit-to address is required to appear on the invoice and the contract, procedures should also require that data be input into the CAPS records in a standardized format. A standardized format is required to perform computer matching tests.

Sign-Out Procedures. Controls over file management were weak because personnel did not follow sign-out procedures. Personnel at the DFAS Columbus Center could not locate 110 (15 percent) of 750 contract payment files that we requested because accounting technicians did not follow sign-out procedures. At the DFAS Columbus Center, personnel are required to sign out the file folders when removing them from storage. Personnel at the DFAS Columbus Center emphasized the need to file contract folders properly, but gave priority to processing payments. We tried unsuccessfully to verify the payment information by other means.

Effective Routines. We determined that 15 computer routines were effective and would detect fraudulent transactions at the DFAS Columbus Center. Appendix C describes these 15 computer routines. One computer routine identified 123 payments that had duplicate contract numbers and payment numbers in the CAPS data base. This routine accounted for $161,824 of the $208,404 in actual and potential duplicate payments and overpayments. These payments were made because accounting technicians were not required to research the history files to determine whether payments had already been made. If the technicians could not locate the original hard copy file, a dummy contract payment file was created. Payments were also made on duplicate invoices. Accounting technicians should be required to:

- o research the payment history files before processing vendor payments,
- o use original files instead of creating dummy files, and
- o make payments only on original invoices.

We also identified 10 occurrences of duplicate check numbers that negated proper accountability for those payments. This occurred because the transaction number of the electronic funds transfer was not entered into the correct data

field in the automated record. An edit check should be programmed into the SRD1 application software to ensure that the transaction number of the electronic funds transfer is entered into the correct data field.

Conclusions

We found no instances of fraud in our review of vendor payments selected by the computer routines as irregular transactions occurring at the DFAS Columbus Center. However, we identified $208,404 in actual and potential duplicate payments and overpayments. Test results for six computer routines were not useful because data formats were not standardized, edit checks were lacking, and operational procedures were inadequate or were not followed. Clearly there is an unacceptable risk of fraud that needs to be addressed.

Recommendations, Management Comments, and Audit Response

A.1. We recommended that the Director, Defense Finance and Accounting Service:

a. Establish procedures to standardize the formats for entering contract and payment data in vendor payment systems.

Management Comments. Management concurred stating that the existing weaknesses in CAPS will be corrected through the CAPS consolidation project which is estimated to be completed in June 1996.

b. Establish a procedure that requires all vendor payments to be processed through the Computerized Accounts Payable System before being processed through the Standard Army Financial System Redesign-1.

Management Comments. Management concurred stating that procedures will be changed through the CAPS consolidation project. The estimated completion date is June 1996.

c. Process system software changes to the Computerized Accounts Payable System, establishing:

(1) A data field to identify fast-pay contracts and show the date when receiving reports are due. Also, allow payments on fast-pay contracts to be processed showing that a receiving report has not been obtained.

Management Comments. Management concurred stating that procedures will be changed through the CAPS consolidation project. The estimated completion date is June 1996.

(2) Edit checks to:

(a) Identify duplicate contract numbers between data bases.

Management Comments. Management nonconcurred stating that duplicate contract numbers are not a problem with CAPS.

Audit Response. The same (duplicate) contract numbers were on the active contract data base and the history contract data base. As a result, duplicate payments occurred when the history contract data base containing completed contracts had not been checked before making a payment on the same contract on the active contract data base. We considered this condition to be duplicate contract numbers because a contract is normally purged from the active contract payment data base and is to be moved to the history contract payment data base only after the final payment has made or indicated. When research had not been performed, duplicate payments occurred. Accordingly, technicians need to research history files before making vendor payments. However, the management response to recommendation A.2.b. should preclude duplicate payments and negate the need for an automated edit check of duplicated contract numbers in the active and history contract payment data bases.

(b) Prevent duplicate payment numbers and multiple final payment indicators from being entered for the same contract number.

Management Comments. Management concurred stating that they adjusted the operating procedures in October 1995. They believe that the CAPS consolidation project will fully resolve the weakness identified. The estimated completion date is June 1996.

d. Process a system software change request to incorporate into the Computerized Accounts Payable System and the Standard Army Financial System Redesign-1 a validation of the dollar amounts and transaction totals to ensure the accurate transfer of data between the two systems.

Management Comments. Management concurred stating a system change request was submitted on October 31, 1995.

e. Process a system software change request to incorporate into the Standard Army Financial System Redesign-1 an edit check to ensure that the electronic funds transfer number is entered into the correct data field.

Management Comments. The Defense Finance and Accounting Service did not comment on this recommendation. We request that the Defense Finance and Accounting Service provide comments in their response to the final report on this recommendation.

A.2. We recommend that the Director, Defense Finance and Accounting Service, Columbus Center:

a. Enforce compliance with procedures requiring that:

(1) Payment addresses be changed only when supported by a contract or contract modification.

Management Comments. Management concurred stating that it has reiterated the existing policy on contract payment addresses; specifically, that such addresses can only be changed through a contract modification. Completed on February 20, 1996.

(2) Electronic funds transfer numbers be correctly entered.

Management Comments. Management concurred stating that all personnel that input Electronic Funds Transfer (EFT) data verify with the financial institution that the routing data on the Vendor Payment Enrollment Form (SF 3881) is correct. Effective April 1996 the EFT administrative functions will be transferred to the Disbursing Directorate. The estimated completion date is April 30, 1996.

b. Establish a procedure requiring accounting technicians to research all payment history files before making payment, use only the original payment file instead of creating a dummy file, and make payments only on original invoices.

Management Comments. Management concurred on using the original payment file for a payment, but nonconcurred on only using original invoices to make payments. They stated that there is existing policy that directs the accounting technicians to research payment history files before making payments. All vendor payment personnel have been instructed to use the original payment file for processing. Both Defense Finance and Accounting Service draft guidance, as well as Army regulations, encourage the use of fax invoices. Additionally, companies that normally fax invoices as their regular way of doing business are not expected to do differently for the government. Completed on February 20, 1996.

Audit Response. We agree that facsimile invoices can be used if adequate research is performed on the active and history payment data bases to prevent duplicate payments.

c. Direct supervisors to ensure that accounting technicians complete the sign-out form when removing contract payment folders from storage.

Management Comments. Management concurred stating that they have reemphasized both the current guidance on this subject and the importance of sign-out forms for proper contract documentation control. Completed on February 20, 1996.

d. Locate or reconstruct the 110 missing payment files in order to avoid duplicate or fraudulent payments that could result because of missing payment information.

Management Comments. Management concurred stating that all 110 files that were unavailable during the audit have been reviewed for duplicate and/or fraudulent payments. No instances of fraudulent or duplicate payments were found. Completed on February 20, 1996.

Finding B. Security Over Vendor Payment Data

Management of security over vendor payment data needs strengthening. Access to data was not effectively controlled because security reports were not provided to supervisors. Therefore, accounting technicians could process fraudulent payments without leaving traceable evidence.

System Security Environment

System security is a two-level process requiring both user identifications and passwords. Novell is the local area network software used to communicate with the CAPS data bases. Users must log onto the Novell system before logging onto CAPS. The CAPS records are stored on six data bases in an unlocked room near the accounting technicians' area. The accounting technicians use CAPS to validate and process vendor payment data. CAPS application security limits the users' ability to access that data. Payment data are transferred onto diskette to the SRD1 on the mainframe computer at the DFAS Columbus Megacenter, which is a controlled environment. As with Novell and CAPS, access to SRD1 data on the mainframe computer requires user identifications and passwords.

To designate an assigned system user, a supervisor must complete a system access request approving the user's level of access and need to use various data bases. The security officer then assigns a user identification number and the user inputs a password. Novell can allow users to perform specific actions: read, write, create, erase, modify, and scan. When a password is assigned to a user, system access is protected. When an individual is assigned access to Novell, anyone can establish a password under that user's name. Therefore, an individual must establish a password immediately after being assigned as a user; otherwise, another employee could sign onto the system in the name of another individual who is an assigned user.

Control Over Payment Data

Management control of security over vendor payment data needs strengthening. Supervisors did not periodically review access to Novell, CAPS, and SRD1. The security officer did not send reports on assigned users to supervisors to ensure that user access was removed when no longer needed. In addition, automated records were not properly safeguarded from compromise.

Control Over Access to Novell. The security officer did not provide key reports to supervisors so they could properly control access to Novell. Out of

1,110 assigned users of Novell, 681 (61 percent) did not have passwords. Also, 186 (43 percent) of the 429 users with passwords had not accessed the system during the previous 3 weeks or more. When Novell was initially installed, all potential users were given access, regardless of need. The security officer for Novell can provide various reports to management on assigned users. Two key reports are "Users and Their Directory Assignments" and "Users That Have Not Accessed Their Account For More Than Three Weeks." Although the reports were available, the security officer did not distribute them to supervisors. The security officer should distribute the security reports to the appropriate supervisors at least monthly in order to properly control access to Novell.

CAPS User Access. Management had not implemented adequate safeguards over CAPS data. The CAPS data bases contain vendor contract and payment data. To gain access to CAPS data, a user must input a user identification and password. Fifty-five CAPS users had the full range of update, delete, and change capabilities and could access more than one data base. Full capability allows a user to change the remit-to address before transferring the payment request to the SRD1 for payment, then delete the record from the system. While the CAPS generates a list of deletions, supervisors did not retain those listings. However, the control section is also provided copies of the lists. To effectively safeguard CAPS data from compromise, the appropriate supervisor should review, initial, and retain a record of all deletions.

Use of SuperQuery. Management did not have an adequate audit trail for changes and deletions to the SRD1 records. Fifty-five employees had access to SuperQuery, a software utility program that allows a user to update, insert, and erase data sets without leaving an audit trail in the data base. According to managers at the computer center, personnel were using SuperQuery to modify production files. SuperQuery allows accounting technicians to process payments through the SRD1 without leaving an audit trail in the system. Managers at the computer center recognized the need to limit access to SuperQuery and issued a memorandum on May 17, 1995, stating: "Per the Central Design Activity, no user should be using SuperQuery to do their job. The SRD1 system is an on-line system and changes to the database files should be done using normal programmed methods."

On May 19, 1995, access to SuperQuery was limited to three individuals: the SRD1 system administrator and two backup system administrators. Although this significantly improved the access control over SRD1 data, an audit trail should be maintained on all activity related to financial records, especially disbursement records. To accomplish this, DFAS should request a system software change to require that the SRD1 system retain an automated copy of all changes and deletions of vendor payment records that produce payments, and ensure that access to that data is fully safeguarded.

Control Over Data Records and Backup Tapes. Management did not effectively control access to the computer server files and did not make proper use of off-site storage. During our visit, we noted conditions in the file server room that needed attention. The door was propped open to allow hot air to dissipate. The room houses the data bases that contain the automated vendor payment records for CAPS. Tapes containing vendor payment data for CAPS

were stacked on the floor next to the computers. An off-site storage facility for backup files was not being used. However, on September 15, 1995, a supervisor told us that as of July 1995, the backup tapes were being stored off-site. If a local disaster occurred, backup files would be needed to restore lost records. To effectively control access to the computer servers' files, management needs to properly cool and secure the room, or place the files in another location that is properly cooled and provides adequate security.

Conclusions

Safeguards over access to vendor payment and disbursement data were inadequate because management oversight needs strengthening. Security reports were not distributed to supervisors to ensure that users with access to automated payment data had a valid need for it. The door to the room containing the payment data was normally left open because the facility was not properly cooled. Management should establish effective safeguards and oversight practices to ensure that all vendor payment and disbursement records are properly protected. Because the DFAS Columbus Center is one of more than 300 paying activities within DFAS, all vendor payment activities should be thoroughly reviewed to ensure that controls over financial records are effective.

Recommendations, Management Comments, and Audit Response

B.1. We recommend that the Director, Defense Finance and Accounting Service:

a. Perform detailed security reviews of all vendor payment activities to ensure that controls over access to financial data and records are effective.

Management Comments. Management concurred stating that they implemented corrective action to control and monitor access to financial data and records on November 15, 1995.

b. Request a system software change to the Standard Army Financial System Redesign-1 to retain a copy of all changes and deletions of vendor payment records that produce payments, and ensure that access to those data is fully safeguarded.

Management Comments. Management partially concurred stating that access to the server and tape storage is a previously identified weakness and will be corrected through the implementation of the CAPS consolidation project.

Management disagreed that deletions from CAPS were not being reviewed. The estimated completion date is June, 1996.

Audit Response. We did not state that deletions from CAPS were not being reviewed, but that users with access to SuperQuery could delete records in the SRD1 without leaving an audit trail.

B.2. We recommend that the Director, Defense Finance and Accounting Service, Columbus Center:

a. Establish effective access controls to ensure that all users with access to vendor payment and disbursing data have a valid need for that level of access. Ensure that software such as SuperQuery is tightly controlled, that the appropriate supervisor reviews and signs each request to use SuperQuery, and that a record of each use is retained.

Management Comments. Management concurred stating a survey of all users that had access to the update, delete, and change data was reassessed on February 23, 1996. Supervisors were asked to approve/disapprove that access based on current need. As a result, 11 users were disapproved. Supervisors were reminded to review the level of access required whenever employees are hired, change positions, etc. Completed on February 23, 1996.

b. Require the system security officer to distribute the reports, "Users and Their Directory Assignments" and "Users That Have Not Accessed Their Account For More Than Three Weeks" to managers of all Novell users.

Management Comments. Management concurred stating that the report "Users and Their Directory Assignments" is received twice a year and reviewed by the Terminal Area Security Officer. The report "Users That Have Not Accessed Their Account for More Than Three Weeks" is now being distributed to the appropriate Section Chief upon receipt from the Defense Finance and Accounting Service Financial Systems Activity - Columbus, Ohio. Completed on March 6, 1996.

c. To effectively control access to the computer servers' files, either properly cool and secure the room where the servers' files are located, or find another location that is properly cooled and provides adequate security.

Management Comments. Management concurred stating that a request has been forwarded to the Resource Management Directorate and to the Plans and Management Directorate requesting relocation of the file servers to a more secure and climate controlled room with cipher lock access to preclude unauthorized access to the file servers. The estimated completion date is September 30, 1996.

Part II - Additional Information

Appendix A. Scope and Methodology

Scope and Methodology

Vendor Payments. We evaluated vendor payment transactions in the CAPS and SRD1 systems at the DFAS Columbus Center. CAPS validates and processes vendor payments, and SRD1 prints and disburses checks. Our selection criteria for this audit was vendor payments for which checks were issued in FY 1994. In FY 1994, the DFAS Columbus Center disbursed more than $1 billion in vendor payments through CAPS. In CAPS and SRD1, we also evaluated management controls designed to prevent and detect erroneous vendor payments. Our field work was performed primarily at the DFAS Columbus Center.

Audit Universe. DFAS has about 300 activities that pay vendors. We evaluated CAPS and SRD1 only at the DFAS Columbus Center because:

- the DFAS Columbus Center had completed its data submissions to DMDC for FY 1994,
- vendor payments for FY 1994 totaled over $1 billion, and
- personnel had a good understanding of the systems.

Request for Data. The Project Management Office for Operation Mongoose sent memorandums to the DFAS vendor paying activities to request disbursement data for FY 1994. The data were sent to the DMDC at Monterey, California, and loaded on a mainframe computer.

Use of Computer-Processed Data. Based on the 15 fraud indicators jointly determined by the DFAS, the DMDC, and the IG, DoD, the DMDC developed 25 computer routines to identify potentially fraudulent payments made to vendors by the DFAS Columbus Center during FY 1994. In January 1995, we visited the DFAS Columbus Center to identify high-risk areas for testing. During the visit, we documented the processing of financial documents received by the Center.

The FY 1994 CAPS disbursement data from the DFAS Columbus Center were loaded on the computer at DMDC. The IG, DoD, with DFAS and DMDC, developed fraud indicator routines for the data. The DMDC used a software package, Statistical Analysis Software, to develop the logic for analyzing and extracting payment records that matched the fraud indicators. Based on our work at the DFAS Columbus Center, the logic was modified several times.

To validate the payments, we took the DMDC reports showing potentially fraudulent payment transactions and compared them to the supporting documents. We compared each listed invoice to the receiving documents and the contract, including contract modifications. To further validate the invoices and payments, we contacted vendors,

contracting officers, disbursing officers, and the U.S. Postal Service. We also contacted post offices to verify that payments were mailed to post office boxes rented by the vendors receiving the payments. To verify payment records, we made inquiries to the SRD1, CAPS, and Dun and Bradstreet, and we requested copies of checks from the U.S. Treasury. At the conclusion of our audit, we summarized the results and documented management controls and system weaknesses.

System Security. This review included access security to vendor payment data via Novell, CAPS, and SRD1. Interviews were held with various security officers to access the hardware and software security controls. Testing was then performed to evaluate the safeguards. This included security reports from Novell to identify inactive user accounts.

Audit Period, Standards, and Locations. We performed this audit during the period January through May 1995. The audit was performed in accordance with auditing standards issued by the Comptroller General of the United States as implemented by the IG, DoD. Accordingly, we included such tests of management controls as were considered necessary. Appendix D lists the organizations visited or contacted during the audit.

Management Control Program

The DFAS Columbus Center complied with the implementation requirements of the DoD management control program. DoD Directive 5010.38, "Internal Management Control Program," April 14, 1987, requires DoD organizations to implement a comprehensive system of management controls that provides reasonable assurance that programs are operating as intended and to evaluate the adequacy of the controls.

Scope of Review of Management Control Program. To evaluate management's compliance with DoD Directive 5010.38, we compared the requirements of the Directive to the management control program at the DFAS Columbus Center. We also reviewed the Annual Statement of Assurance issued by the DFAS Columbus Center's financial services directorate, and obtained other reports related to the management control program.

Adequacy of Management Controls. The FY 1994 Annual Statement of Assurance reported four open material management control weaknesses for the commercial payments division from the FY 1993 Annual Statement of Assurance; three of these weaknesses had been corrected, and one still required corrective action. This weakness was corrected in FY 1995. We found no additional material control weaknesses during this audit.

Adequacy of Management's Self-Evaluation. DFAS Columbus Center officials identified commercial payments as an assessable unit and, in our opinion, correctly identified the risk associated with commercial payments as high.

Appendix B. Prior Audits and Other Reviews

No audits of the CAPS system have been performed in the past 5 years. We coordinated the audit with the Army Criminal Investigative Command, the Naval Investigative Service, the Air Force Office of Special Investigations, the Defense Criminal Investigative Service, and the Federal Bureau of Investigations to identify any prior work on fraud-related cases. The investigative agencies had developed computer modeling techniques, but not to the extent of Operation Mongoose.

Appendix C. Description of Computer Routines

Effective Routines

1. **Same contract numbers and same payment numbers.**

   Purposes: To identify payments with the same contract numbers and same payment numbers to detect duplicate payments.

   Results: Total of 270 observations; 4 observations analyzed.

   Causes: No on-line history check for duplicate contract numbers; payments are made from duplicate documentation.

   Suggestions: This routine should be in CAPS and used at each site.

2. **Streamlined payment addresses in SRD1 are not equal to payment addresses in CAPS.**

   Purpose: To identify payments with addresses that were altered before the information was transferred to CAPS.

   Results: Total of 76 observations; 4 observations analyzed.

   Cause: CAPS version 2.1 retained only the latest vendor address. A CAPS revision now allows more than one address.

   Suggestion: This routine should be used at each site.

3. **Streamlined payment amount of check in SRD1 not equal to amount in CAPS.**

   Purpose: To identify an alteration in the amount of the check issued when the data were transferred to CAPS.

   Results: Total of 18 observations; 4 observations analyzed.

   Cause: CAPS automatically assigns the payment number, while data are manually entered into SRD1 by accounting technicians.

   Suggestions: All payments should be processed through CAPS first. This routine should be in CAPS and used at each site.

4. **Amount of check in SRD1 differed from amount in CAPS.**

Purpose: To identify altered check amounts.

Results: Total 4 observations; 1 observations analyzed.

Cause: Error by the voucher examiner.

Suggestion: This routine should be used at each site.

5. **Payments with a control group's user identification number or manager's identification number.**

Purpose: To identify payments entered by individuals with overwriting capabilities.

Results: Total of 199 observations; 7 observations analyzed.

Cause: This is not an unusual occurrence at the DFAS Columbus Center.

Suggestion: This routine should be used at each site.

6. **Payments without a check amount.**

Purpose: To identify payments with the check amounts deleted.

Results: Total of 0 observations; 0 observations analyzed.

Suggestion: This routine should be used at each site.

7. **Payments without check numbers.**

Purpose: To identify payments for which the check number was deleted.

Results: Total of 0 observations; 0 observations analyzed.

Suggestion: This routine should be used at each site.

8. **Duplicate check numbers.**

Purpose: To identify checks with previously used check numbers.

Results: Total of 10 observations; 1 observation analyzed.

Cause: Electronic funds transfers to the same vendor were recorded with the same check number.

Suggestions: Establish an automated edit check. This routine should be used at each site.

9. **Payments without contract numbers.**

Purpose: To identify payments with the contract numbers deleted.

Results: Total of 1 observation; 1 observation analyzed.

Cause: Leading zeroes in the contract number.

Suggestion: This routine should be used at each site.

10. **Payments with invalid vendor names or without vendor names.**

Purpose: To identify invalid payments.

Results: Total of 0 observations; 0 observations analyzed.

Suggestion: This routine should be used at each site.

11. **Payments without addresses.**

Purposes: To identify payments with the addresses deleted or payments made to individuals for pickup.

Results: Total of 0 observations; 0 observations analyzed.

Suggestion: This routine should be used at each site.

12. **Payments without voucher numbers or document numbers.**

Purpose: To identify payments for which voucher numbers or document numbers had been removed.

Results: Total of 0 observations; 0 observations analyzed.

Suggestion: This routine should be used at each site.

13. **Payments with negative check amounts.**

Purpose: To identify payments with negative check amounts.

Results: Total of 0 observations; 0 observations analyzed.

Suggestion: This routine should be used at each site.

14. **Duplicate invoice numbers.**

Purpose: To identify duplicate payments.

Results: Total of 0 observations; 0 observations analyzed.

Suggestion: This test should be performed at each site.

15. **Payments made without showing a voucher examiner.**

Purpose: To identify payments made without the voucher examiner identified.

Results: Total of 0 observations; 0 observations analyzed.

Suggestion: This routine should be used at each site.

Ineffective Routines

1. **Payments shown in SRD1, but not shown in CAPS.**

Purpose: To identify payments made by SRD1, bypassing CAPS safeguards.

Results: Total of 395 observations; 25 observations analyzed.

Causes: Payment data were improperly deleted or not input into CAPS.

Suggestions: Strengthen controls over deletions and streamlined payments. This routine should be used at each site.

2. **Payment addresses in SRD1 that differ from payment addresses in CAPS.**

Purpose: To identify payments sent to an unauthorized payee.

Results: Total of 1,288 observations; 51 observations analyzed.

Causes: CAPS version 2.1 altered the historical records when the contract record was updated. The data format is not the same in both systems.

Suggestions: Establish standardized data formats. CAPS has been revised to allow multiple vendor addresses. This routine should be used at each site.

3. **Payees' names in SRD1 that differ from payees' names in CAPS.**

Purpose: To identify payments in which the payees' names were altered and the checks were sent to unauthorized payees.

Results: Total of 725 observations; 4 observations analyzed.

Causes: CAPS version 2.1 altered the historical records when the contract record was updated. The data format is not the same in both systems.

Suggestions: Establish standardized data format. CAPS has been revised to allow multiple vendors' names. This routine should be used at each site.

4. **Missing check numbers.**

Purposes: To identify breaks in the sequence of check numbers and to identify deleted check numbers.

Results: Total of 6,599 observations; 1 observation analyzed.

Cause: Payments included those made for other divisions, such as travel.

Suggestion: This routine should be used at each site.

5. **Trends for fast-pay transactions.**

Purpose: To identify high-risk fast-pay transactions in CAPS.

Results: Total 299 observations; 2 observations analyzed.

Cause: CAPS has no specific fast-pay indicator.

Suggestions: Modify CAPS software to identify fast-pay contracts. This routine should be used at each site.

6. **Contracts awarded before FY 1993 with payments made in FY 1994.**

Purpose: To identify fraudulent payments made on inactive contracts.

Results: Total of 5,468 observations; 38 observations analyzed.

Causes: On multi-year service or maintenance contracts, delivery order numbers were not entered by voucher examiners.

Suggestions: This computer routine will be modified to identify contracts awarded prior to FY 1993 with a break in payment of 1 or more years. This routine should be used at each site.

7. **Invoices paid on closed contracts.**

Purpose: To identify fraudulent payments made on closed contracts.

Results: Total of 684 observations; 10 observations analyzed.

Causes: Contracts were improperly closed. Contracts were subsequently modified to increase the contracted amounts.

Suggestions: Enforce compliance with procedures. Change the CAPS to allow one final payment. This routine should be used at each site.

8. **Same voucher examiner for multiple payments on the same contract.**

Purpose: To identify a pattern of payments made by the same individual.

Results: Total of 1,509 observations; 6 observations analyzed.

Cause: This is not an unusual occurrence.

Suggestion: This routine should not be used at the other sites.

9. **Same voucher examiner for multiple payments on the same contract, for check amounts greater than $0.**

Purpose: To identify a pattern of payments made by an individual.

Results: Total of 1,509 observations; 0 observations analyzed.

Cause: This is not an unusual occurrence.

Suggestion: This routine should not be used at the other sites.

10. **Same voucher examiner shown for 15 or more payments to the same vendor.**

Purpose: To identify payment patterns of voucher examiners and vendors.

Results: Total of 904 observations; 0 observations analyzed.

Cause: This is not an unusual occurrence.

Suggestion: This routine should not be used at the other sites.

Appendix D. Organizations Visited or Contacted

Department of the Army

Criminal Investigations Command, Falls Church, VA

Department of the Navy

Naval Criminal Investigative Service, Washington, DC

Department of the Air Force

Air Force Office of Special Investigations, Washington, DC

Other Defense Organizations

Defense Finance and Accounting Service, Arlington, VA
- Defense Finance and Accounting Service Center, Cleveland, OH
- Defense Finance and Accounting Service Center, Columbus, OH
- Defense Finance and Accounting Service Center, Denver, CO
- Defense Finance and Accounting Service Center, Indianapolis, IN
- Defense Finance and Accounting Service Center, Kansas City, MO

Defense Information Systems Agency, Columbus, OH
Defense Logistics Agency
- Defense General Supply Center, Richmond, VA

Defense Manpower Data Center, Monterey, CA

Non-Defense Federal Organizations

Department of Labor, Washington, DC
Department of Transportation, Washington, DC
Department of the Treasury, Washington, DC
Federal Bureau of Investigations, Washington, DC
Inspector General, House of Representatives, Washington, DC
Social Security Administration, Baltimore, MD

Appendix E. Report Distribution

Office of the Secretary of Defense

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

Department of the Army

Assistant Secretary of the Army (Financial Management and Comptroller)
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 Finance and Accounting Service
Director, Defense Logistics Agency
Director, National Security Agency
  Inspector General, National Security Agency
Inspector General, Defense Intelligence Agency

Non-Defense Federal Organizations

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

Part III - Management Comments

Defense Finance and Accounting Service Comments

DEFENSE FINANCE AND ACCOUNTING SERVICE
1931 JEFFERSON DAVIS HIGHWAY
ARLINGTON, VA 22240-5291

MEMORANDUM FOR ASSISTANT INSPECTOR GENERAL FOR AUDITING,
DEPARTMENT OF DEFENSE

SUBJECT: Draft Report on Vendor Payments - Operation Mongoose
(Project No. 5FG-5016)

I am responding to the subject Draft Audit Report concerning the management controls over vendor payments at the Defense Finance and Accounting Service-Columbus Center (DFAS-CO).

The DFAS-CO response is attached. We partially agree with the draft report findings and recommendations. The enclosed comments outline specific actions by the DFAS-CO.

We appreciate the opportunity to comment on the draft report. My point of contact for this issue is Mr. Dennis Schilcher and may be reached at (703) 607-3935.

Michael E. Wilson
Deputy Director, Customer
Service and Performance
Assessment

Attachment

Final Report Reference

DEFENSE FINANCE AND ACCOUNTING SERVICE
COLUMBUS CENTER RESPONSE TO
DoDIG DRAFT REPORT ON
VENDOR PAYMENTS - OPERATION MONGOOSE
(PROJECT NO. 5FG-5016) JANUARY 8, 1996

FINDING A:

Page 5

Test results showed that 10 of the 25 computer routines were ineffective as tools for detecting fraudulent vendor payments in the Computerized Accounts Payable System (CAPS) and the Standard Army Financial System (STANFINS) Redesign-1 (SRD1) at the DFAS-Columbus Center. Of the ten routines, six could be more effective if data formats were standardized, the system software had improved edit checks. and the local operating procedures were improved and followed. Four routines were based on incorrect assumptions, three were dropped from further consideration, and the fourth has been redesigned. Duplicate payment numbers were used because streamlined payments bypassed the controls in CAPS. In FY94, streamlined payments totaled $346 million of the $1 billion in vendor payments for CAPS and SRD1. The effective routines identified $208,404 in actual and potential duplicate payments and over payments. Personnel at DFAS-CO could not locate 110 (15 percent) of the 750 contract files we requested because sign-out procedures had not been followed. As a result we could not determine whether fraudulent payments occurred on those 110 vendor payments.

Page 10

Recommendation A.1. Recommend that the Director, Defense Finance and Accounting Service:

a. Establish procedures to standardize the formats for entering contract and payment data in vendor payment systems. **CONCUR.** Existing weaknesses in CAPS will be corrected through the CAPS consolidation project. (Estimated completion date 6/96).

b. Establish a procedure that requires all vendor payments to be processed through the CAPS before being processed through the STANFINS Redesign-1. **CONCUR.** Procedures will be changed through the CAPS consolidation project. (Estimated completion date 6/96).

c. Process system software changes to the CAPS, establishing:

(1) A data field to identify fast-pay contracts and show the date when receiving reports are due. Also, allow payments on fast-pay contracts to be processed showing that a receiving report has not been obtained. **CONCUR.** Procedures will be changed through the CAPS consolidation project. (Estimated completion date 6/96).

(2) Edit checks to:

(a) Identify duplicate contract numbers between data bases. **NON-CONCUR.** We do not agree that duplicate contract numbers are a problem with CAPS.

(b) Prevent duplicate payment numbers and multiple final payment indicators from being entered for the same contract number. **CONCUR.** We adjusted procedures in October 1995 and we believe that the CAP consolidation project will fully resolve the weakness identified. (Estimated completion date 6/96).

d. Process a system software change request to incorporate into the CAPS and the STANFINS Redesign-1 a validation of the dollar amounts and transaction totals to ensure the accurate transfer of data between the two systems. **CONCUR.** A SCR was submitted on October 31, 1995.

Recommendation A.2.a.1.

Enforce compliance with procedures requiring that payment addresses be changed only when supported by a contract or contract modification. **CONCUR.** Management has reiterated the existing policy relevant to contract payment addresses; specifically, that such addresses can only be changed through a contract modification. Completed date: February 20, 1996.

Recommendation A.2.a.2.

Enforce compliance with procedures requiring that electronic funds transfer numbers be correctly entered. **CONCUR.** All personnel that input Electronic Funds Transfer (EFT) data verify with the financial institution that the routing data on the Vendor Payment Enrollment Form (SF 3881) is correct. Effective April 1996 the EFT administrative functions will be transferred to the Disbursing Directorate. Estimated completion date: April 30, 1996.

Recommendation A.2.b.

Establish a procedure requiring accounting technicians to research all payment history files before making payment, use only the original payment file instead of creating a dummy file, and make payments only on original invoices. **CONCUR** on using original payment file for payments. **NONCONCUR** on only using original invoices to make payments.

There is existing policy that directs the accounting technicians to research payment history files before making payments. All vendor pay personnel have been instructed to use the original payment file for payment processing.

Final Report Reference

Both Defense Finance and Accounting Service draft guidance, as well as Army regulations, encourage the use of fax invoices. Additionally, companies that normally fax invoices as their regular way of doing business are not expected to do differently for the government. Completed date: February 20, 1996.

Recommendation A.2.c.

Direct supervisors to ensure that accounting technicians complete the sign-out form when removing contract payment folders from storage. **CONCUR.** Management has reemphasized the current guidance on this subject and the importance of sign-out forms for proper contract documentation control. Completed date: February 20, 1996.

Recommendation A.2.d.

Locate or reconstruct the 110 missing payment files in order to avoid duplicate or fraudulent payments that could result because of missing payment information. **CONCUR.** Commercial Payments located and researched all 110 files on the list on February 20, 1996. All 110 payment files that were unavailable during the audit have been reviewed for duplicate and/or fraudulent payments. No instances of fraud have surfaced and no duplicate payments were found. Completed date: February 20, 1996.

FINDING B:

Management of security over vendor payment data needs strengthening. Access to data was not effectively controlled because security reports were not provided to supervisors. Therefore, accounting technicians could process fraudulent payments without leaving traceable evidence.

Page 14

Recommendation B.1. Recommend that the Director, Defense Finance and Accounting Service:

Page 16

a. Perform detailed security reviews of all vendor payment activities to ensure that controls over access to financial data and records are effective. **CONCUR.** We implemented corrective action to control and monitor access on November 15, 1995.

b. Request a system software change to the Standard Army Financial System Redesign-1 to retain a copy of all changes and deletions of vendor payment records that produce payments, and ensure that access to those data is fully safeguarded. **PARTIALLY CONCUR.** We do not agree that deletes from CAPS were not being reviewed. Access to server and tape storage is a previously identified weakness that will be corrected through the implementation of the CAPS consolidation project. (Estimated completion date 6/96).

Final Report Reference

B.2.a.

Recommendation B.2.

Establish effective access controls to ensure that all users with access to vendor payment and disbursing data have a valid need for that level of access. Ensure that software such as SuperQuery is tightly controlled, that the appropriate supervisor reviews and signs each request to use SuperQuery, and that a record of each use is retained. **CONCUR.** On February 23, 1996, a survey of all users that had access to the update, delete, and change data was reassessed. Supervisors were asked to approve/disapprove that access based on current need. As a result, 11 users were disapproved. The remaining 42 are supervisors and higher-graded accounting technicians. Supervisors were reminded to assess the level of access required whenever employees are hired, change positions, etc.

SuperQuery software is controlled by the Disbursing Systems Branch, Financial Quality Division of the Disbursing Directorate. No Commercial Payments employees have access to SuperQuery. Completed date: February 23, 1996.

B.2.b.

Recommendation B.2.a.

Require the system security officer to distribute the reports, "Users and their Directory Assignments" and "Users that have not Accessed their Account for More than Three Weeks" to managers of all Novell users. **CONCUR.** The report "Users and Their Directory Assignments" is received twice a year and reviewed by the Terminal Area Security Officer. The report "Users That Have Not Accessed Their Account for More Than Three Weeks" is now being distributed to the appropriate Section Chief Upon receipt from Defense Finance and Accounting Service Financial Systems Activity-Columbus. Completed date: March 6, 1996.

B.2.c.

Recommendation B.2.b.

To effectively control access to the computer servers' files, either properly cool and secure the room where the servers' files are located, or find another location that is properly cooled and provides adequate security. **CONCUR.** A request has been forwarded to Resource Management Directorate and to Plans and Management Directorate requesting relocation o file servers to a more secure and climate controlled room with cipher lock access to preclude unauthorized access to the file servers. Estimated completion date: September 30, 1996.

Audit Team Members

This report was prepared by the Finance and Accounting Directorate, Office of the Assistant Inspector General for Auditing, DoD.

F. Jay Lane
Chris Hendricks
Carl Zielke
Rob Dieter
Geoff Weber
Kelly Young
Ivette Reick
Monica Noell
Traci Sadler

INTERNET DOCUMENT INFORMATION FORM

A . Report Title: Vendor Payments – Operation Mongoose

B. DATE Report Downloaded From the Internet: 12/01/99

C. Report's Point of Contact: (Name, Organization, Address, Office Symbol, & Ph #): **OAIG-AUD (ATTN: AFTS Audit Suggestions)**
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-2884

D. Currently Applicable Classification Level: Unclassified

E. Distribution Statement A: Approved for Public Release

F. The foregoing information was compiled and provided by:
DTIC-OCA, Initials: __VM__ **Preparation Date 12/01/99**

The foregoing information should exactly correspond to the Title, Report Number, and the Date on the accompanying report document. If there are mismatches, or other questions, contact the above OCA Representative for resolution.