Evaluation Report

OFFICE OF THE INSPECTOR GENERAL

VENDOR PAYMENTS-OPERATION MONGOOSE, FORT BELVOIR DEFENSE ACCOUNTING OFFICE AND ROME OPERATING LOCATION

Report No. 97-052

December 23, 1996

DEPARTMENT OF DEFENSE

Additional Copies

To obtain additional copies of this evaluation 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 Evaluations

To suggest ideas for or to request future evaluations, 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 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
DAO	Defense Accounting Office
DFAS	Defense Finance and Accounting Service
DMDC	Defense Manpower Data Center
DoDAAC	Department of Defense Activity Address Code
FAR	Federal Acquisition Regulation
IG	Inspector General
ISSA	Information Systems Selection and Acquisition Agency
OMB	Office of Management and Budget
OPLOC	Operating Location
SAACONS	Standard Army Automated Contracting System
STANFINS	Standard Army Financial System

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

December 23, 1996

MEMORANDUM FOR DIRECTOR, DEFENSE FINANCE AND ACCOUNTING SERVICE

SUBJECT: Evaluation Report on Vendor Payments-Operation Mongoose, Fort Belvoir Defense Accounting Office and Rome Operating Location (Report No. 97-052)

We are providing this evaluation report for information and use. The evaluation was made in support of Operation Mongoose. This report is the second in a series of reports on the review of vendor payments and contracting systems. Management comments on a draft of this report were considered in preparing the final report.

Comments on the draft of this report conformed to the requirements of DoD Directive 7650.3 and left no unresolved issues. As a result of management comments, we deleted draft Recommendation A.4. Therefore, no additional comments are required.

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

David K. Steensma

David K. Steensma
Deputy Assistant Inspector General
for Auditing

Office of the Inspector General, DoD

Report No. 97-052 **December 23, 1996**
(Project No. 5FG-5016.01)

Vendor Payments-Operation Mongoose, Fort Belvoir Defense Accounting Office and Rome Operating Location

Executive Summary

Introduction. This evaluation 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, 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 Inspector General, 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. The prototype will be built in 5 phases and include 11 systems when complete. We reviewed three systems, the Standard Army Automated Contracting System, the Computerized Accounts Payable System, and the Standard Army Financial System Redesign-1 at Fort Belvoir, Virginia. Our evaluation focused on the effectiveness of computer routines designed to identify fraudulent vendor payments and on management controls over vendor payments made at the Defense Accounting Office, Fort Belvoir, Virginia, during FY 1995. Operations at the Defense Accounting Office Fort Belvoir were transferred to the Rome Operating Location, Rome, New York, in October 1995. Accordingly, we reviewed the controls over payments at the Rome Operating Location, where the Defense Accounting Office Fort Belvoir was consolidated. This report is the second in a series of reports on vendor payments under Operation Mongoose.

Evaluation Objectives. The objectives were to evaluate the effectiveness of computer routines designed to identify fraud and to evaluate management controls over payments to vendors. We applied computer matching techniques to disbursing transactions to identify irregularities indicative of potential fraud. We also evaluated management controls over systems designed to prevent and detect erroneous vendor payments. Due to the impending closure of the Defense Accounting Office at Fort Belvoir and the anticipated consolidation to the Rome Operating Location, New York, we did not perform a review of the management control program at Fort Belvoir, Virginia.

Evaluation Results. Operation Mongoose has shown steady progress in developing computer routines for detecting irregular and fraudulent vendor payments. Test results showed that 23 computer routines produced useful results; 29 computer routines would have been more effective in detecting fraud if a payment type code for adjustments had been established and previously recommended changes concerning data standardization, streamlined payments, and identification of fast-pay contracts were implemented; and 2 computer routines were ineffective and were eliminated. Also, one large contract

was inappropriate for the Computerized Accounts Payable System. Accordingly, the computer routines that require changes should not be used at other sites until the identified problems are corrected (Finding A).

Management of security over payment data at the DFAS Rome Operating Location did not comply with DoD security policy. As a result, unauthorized users could compromise or manipulate data without risk of detection (Finding B).

Management controls at the DFAS Rome Operating Location needed improvement because a material weakness was identified related to computer security controls over access to vendor payment data. Implementation of the recommendations in this report will improve management controls to prevent unauthorized users from compromising or manipulating data without detection. See Part I for a discussion of evaluation results.

Summary of Recommendations. We recommend processing a software change request to the Computerized Accounts Payable System; obtaining contract modification data needed for testing fraud indicator routines; and discontinuing testing specific accounting and disbursing systems until identified problems are corrected. We also recommend that the DFAS Rome Operating Location implement DoD policy on security requirements for the three systems and develop and implement a contingency plan.

Management Comments. DFAS agreed with all but two of our recommendations. DFAS disagreed that the payment responsibility for contract DAHC94-91-C0002 should be transferred, because the number of invoices received monthly has been decreased from between 150 and 200 to only 2. DFAS also disagreed with requiring that all large contracts be paid using the Mechanization of Contract Administration Services system. See Part I for complete discussion of management comments and Part III for the complete text of management comments.

Evaluation Response. DFAS adequately addressed the deficiencies noted in the report. Based on DFAS comments, we deleted the recommendation requiring all large contracts be paid using the Mechanization of Contract Administration Services system.

Table of Contents

Executive Summary i

Part I - Evaluation Results

Evaluation Background 2
Evaluation Objectives 3
Finding A. Fraud Indicators 4
Finding B. Security Over Vendor Payment Data 11

Part II - Additional Information

Appendix A. Evaluation Process
Scope and Methodology 18
Organizations and Individuals Visited or Contacted 19
Management Control Program 20
Appendix B. Prior Evaluations and Other Reviews 21
Appendix C. Description of Computer Routines 23
Appendix D. Report Distribution 37

Part III - Management Comments

Defense Finance and Accounting Service Comments 40

Part I - Evaluation Results

Evaluation Background

This evaluation 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 evaluation is limited to vendor payments made by the Defense Accounting Office, Fort Belvoir, Virginia (DAO Fort Belvoir), in FY 1995 and security over automated payment records at the Rome Operating Location (OPLOC), Rome, New York.

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 by comparing data in vendor payment systems to data in contracting systems and vice versa. In July 1995, we began developing and testing computer routines against contract data from the Standard Army Automated Contracting System (SAACONS). In October 1995, 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 DAO Fort Belvoir. We made visits to the DAO Fort Belvoir and the Rome OPLOC from July 1995 through May 1996, to document the payment process and to test the 54 computer routines for detecting irregular and fraudulent vendor payments.

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

o The DFAS will coordinate and research the activities of Operation Mongoose and will 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 computer routines after completing each review. This report is the second in a series of reports on vendor contracting and payment systems.

Plans for Operation Mongoose. IG, DoD, personnel worked with DFAS and DMDC as Operation Mongoose in developing a prototype system to identify irregular and fraudulent vendor payment transactions. The prototype will be built in five phases and will include 11 vendor contract and payment systems when completed. At the conclusion of testing, Operation Mongoose will establish priority of implementing the computer routines into the vendor payment systems. The first phase of the prototype included the CAPS and SRD1 systems at the DFAS Columbus Center, Columbus, Ohio. The second phase of the prototype included the CAPS and SRD1 systems at the DAO Fort Belvoir and the SAACONS at the Directorate of Contracting, Fort Belvoir, Virginia. The SAACONS contains contracting data that are forwarded to the CAPS. CAPS contains the payment data and computes payments, and the SRD1 system disburses checks and maintains disbursement data.

Development of Computer Routines. The 54 computer routines used to test the vendor payments made by the DAO Fort Belvoir in FY 1995 were developed by Operation Mongoose for SAACONS, CAPS, and SRD1 data submitted by the DAO Fort Belvoir to the DMDC at Monterey, California. Of the 54 routines, 21 had been previously developed to test payments made in the CAPS and SRD1 systems at DFAS Columbus Center.

Site and System Selection. Of the 42 sites using the CAPS vendor payment system, we selected the DAO Fort Belvoir for review because it used the SAACONS contracting system. Also, the DAO Fort Belvoir used the CAPS vendor payment system and SRD1 disbursing system. In FY 1995, the DAO Fort Belvoir processed about $342 million in vendor payments.

Evaluation Objectives

The evaluation objectives were to evaluate the effectiveness of computer routines designed to identify fraudulent activity and to evaluate management controls over payments to vendors. We applied computer matching techniques to contracting and disbursing transactions to identify irregularities that indicated potential fraud in the CAPS and SRD1 systems. We also evaluated management controls over systems designed to prevent and detect erroneous vendor payments. This evaluation focused on vendor payment data in the CAPS and SRD1 systems, contract data in the SAACONS data base at Fort Belvoir, and management controls over vendor payments made by the DAO Fort Belvoir in FY 1995. See Appendix A for a complete discussion of the evaluation scope and methodology and the review of the management control program. See Appendix B for a summary of prior coverage related to the evaluation objectives.

Finding A. Fraud Indicators

Operation Mongoose has shown steady progress in developing computer routines for detecting irregular and fraudulent vendor payments. Test results showed that 23 computer routines produced useful results; however, 31 of the 54 computer routines did not produce the expected results in detecting irregular or fraudulent vendor payments in the CAPS and the SRD1 at the DAO Fort Belvoir. Of the 31 routines, 29 will produce useful results when a payment type code for adjustments is established and when previously recommended changes concerning data standardization, streamlined payments, and identification of fast-pay contracts are implemented. Fort Belvoir DAO accounting technicians bypassed system edit checks in order to expedite payments on a large contract. Because system edit checks were bypassed, duplicate payments could be processed and not detected. Further, changes to the vendor payment systems are needed to make observations produced by computer routines more effective for detecting potentially fraudulent payments.

Review of Vendor Payment Process for Potential Fraud

Contracting. The Directorate of Contracting at Fort Belvoir, Virginia, receives requisitions from tenant and nontenant organizations for material and services. Generally, fund citations on the requisitions determine which disbursing office will make payments on the contracts. Therefore, contracts issued by the Directorate of Contracting at Fort Belvoir may not have been paid by the DAO Fort Belvoir. After the Directorate of Contracting awarded the contracts that were to be paid by the DAO Fort Belvoir, contract information was downloaded from the SAACONS to a diskette. The Directorate of Contracting sent its SAACONS diskette, along with a hard copy of each contract, to the DAO Fort Belvoir. Since the closure of the DAO Fort Belvoir in October 1995, the Directorate of Contracting at Fort Belvoir uses File Transfer Protocol to electronically send the SAACONS contract data to the Rome OPLOC.

Vendor Payments. The vendor payment process has four phases: inputting, processing, verifying, and disbursing. The Fort Belvoir SAACONS contract information was formerly copied onto a diskette and was uploaded into the CAPS. The Commercial Accounts Payable Division manually input into the CAPS the hard copy contracts that other organizations mailed to the DAO Fort Belvoir.

The accounting technicians received the invoices and receiving documents and reviewed them for completeness. If the documents were not complete, the technicians returned the documents to the vendor. After the technicians reviewed the documents, the documents were sorted alphabetically. In the Commercial Accounts Payable Division, technicians pulled the hard copy contract files and matched the invoices and the receiving reports to contracts for validation. The technicians then entered the data into CAPS, computed the payments, and produced summary vouchers. Each contract payment file

contained a hard copy of the contract and all contract modifications, each invoice and receiving report, and any other correspondence related to the contract. Except for fast-pay contracts, invoices were not paid until the contract, the invoice, and the receiving report were received and validated. The CAPS active payment file retained information on the contract and each payment for at least 90 days after the final payment was made to the vendor. After 90 days, the contract payment data were transferred to the history file and purged from the active file. The final payment was indicated in the payment record with an "f" in the payment type field.

In the Commercial Accounts Payable Division, transmittal letters were printed each day, identifying the payments that were to be made that day in contract number sequence by due date. Each transmittal letter listed up to 20 payments. When the vouchers with the supporting documentation were received by a technician in the Commercial Accounts Payable Division, the technician matched vouchers and documentation to the transmittal letters. Each voucher was then compared to the upload file in the CAPS data base by contract number, payment number, and payment amount. When that comparison was completed, the technician prompted CAPS to create the diskette used to enter the data into SRD1. The technician would then upload the data on the diskette into SRD1 for the vouchers to be paid that day.

One day before payment, the technician would obtain a list from the SRD1 of all payments due the next payment date. The technician matched payment documentation to the SRD1 list and sent the documentation to the Disbursing Division to support the disbursing request. The SRD1 system assigned the check numbers and disbursing office voucher numbers, and the official vouchers and checks were printed by SRD1. After the SRD1 issued checks, a technician would download the payment data from SRD1 to a diskette and upload the data into CAPS. This transfer of check information to CAPS updated it with disbursement data, such as the check number, disbursing officer voucher number, and date of payment.

Streamlined payments and fast payment procedures are two practices used to expedite the disbursement process. Streamlined payments are processed directly to SRD1, bypassing critical validation controls in the CAPS. After payments are made, the SRD1 payment information is transferred to CAPS. During FY 1995, the DAO Fort Belvoir processed 32,288 payments totaling $342 million. Of those payments, 5,887 payments totaling $28.2 million were streamlined payments processed directly into SRD1 at the DAO Fort Belvoir.

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 contractor submission of an invoice that delivery has been completed according to terms of the purchase agreement. However, because there is no fast payment indicator, we were unable to identify these transactions.

The U. S. Treasury. At the end of each week, every Disbursing Division at each DAO transmits a "Level 8" report, a summary of the week's

disbursements, to their respective DFAS centers. The report details the series of checks and disbursing office voucher numbers printed for that week and the dollar total disbursed for that series. On a monthly basis, each DAO reports the check number series, disbursing office voucher numbers, and the disbursing dollar totals directly to the U.S. Treasury. In addition, the DAO reports voided, canceled, and mutilated checks to the U.S. Treasury.

Analysis of Computer Routines

Our analysis of the 54 computer routines showed that 31 did not produce expected results. If corrections identified during our tests are made, 52 of the 54 routines would detect potential fraudulent payments in the CAPS and SRD1 systems. We eliminated two routines from further consideration because they were based on incorrect assumptions.

Computer Routines That Did Not Produce Expected Results. The 31 computer routines did not produce expected results for several reasons. Twenty-nine routines will produce useful results when:

- o data are input into CAPS and SRD1 in a standardized format,
- o edit checks are implemented to ensure data integrity,
- o operational procedures are established and enforced,
- o a payment type code is established for adjustments, and
- o data submissions included all contract modification data.

The IG, DoD, Report No. 96-134, "Vendor Payments-Operation Mongoose," May 30, 1996, addressed the causes of the first three reasons why expected results were not achieved and provided appropriate recommendations to DFAS.

Routines That Produced Useful Results. Of the 54 computer routines, 23 did produce useful results and would detect potentially fraudulent transactions. See Appendix C for a description of those computer routines.

Issues Affecting Computer Routines

The large number of transactions erroneously listed by the 31 computer routines had five main causes: lack of data standardization, inadequate edit checks, operational procedures that were either inadequate or not followed, lack of a payment type code to identify adjustments, and lack of crucial data submitted to

Operation Mongoose. Furthermore, CAPS cannot effectively process payments for large contracts due to a lack of effective edit checks and should not make payments on large contracts as a matter of policy.

Data Standardization. In the CAPS files, the contractor name, address, and other data fields used to test data validity were not standardized resulting in erroneously identified fraudulent transactions. 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. Standard operating procedures instruct personnel at the DAO Fort Belvoir to enter information into the CAPS exactly as documented in the contract; however, vendors addresses in each contract are not always shown in the same format. Those inconsistencies caused mismatches during our tests of the computer routines. This problem was previously identified in the IG, DoD, Report No. 96-134 at the DFAS Columbus Center; therefore, this report contains no recommendations on standardized data.

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 within valid parameters and that each vendor name and address meet a standardized format. Because the DFAS has not implemented those controls, Operation Mongoose incorrectly identified large numbers of transactions as potentially fraudulent payments. For example, one routine incorrectly identified over 3,000 transactions as potentially fraudulent. This problem was previously identified in the IG, DoD, Report No. 96-134; therefore, this report contains no recommendations on edit checks.

For the transactions transferred by diskette between the CAPS and SRD1, accounting technicians did not validate dollar amounts and transaction totals. Without this validation, transactions could be changed, added, or deleted without being detected in the transfer between systems. To ensure that transactions and amounts are not changed, added, or deleted, the dollar amounts and transaction totals should be electronically compared during each transfer of data between systems. This problem was previously identified in IG, DoD, Report No. 96-134; therefore, this report contains no recommendations on transaction totals.

Operational Procedures. Operational procedures were lacking. Personnel at the DAO Fort Belvoir sent payments to vendors with names and addresses shown on the invoice that differed from the names and addresses shown on the contracts. The DAO Fort Belvoir had not established procedures to require that data be input into CAPS in a standardized format. Procedures in the Federal Acquisition Regulation 32.905(e)6 require that the same vendor name and address appear on both the invoice and the contract; however, technicians at the

DAO Fort Belvoir did not follow that requirement. A standardized format is essential for Operation Mongoose to perform efficient computer matching tests. This problem was previously identified in the IG, DoD, Report No. 96-134; therefore, no recommendation is made in this report.

Of 32,288 vendor payments made in FY 1995 by the DAO Fort Belvoir, 5,887 (18 percent) were streamlined into SRD1, bypassing CAPS. Those payments were made principally by four organizations outside the DAO: the Army Judge Advocate General; the Army Directorate of Information Management; the Research and Development Center; Fort Belvoir; and the DeWitt Army Hospital. Because such a large number of streamlined payments were made in FY 1995, we were unable to fully analyze the results of the fraud indicator relating to streamlined payments.

Payment Adjustment Code. Accounting technicians entered adjustments into CAPS that were not identified by a specific payment code designation. To adjust obligated amounts on line items or to manually close contracts in CAPS, technicians were instructed to enter an adjustment record using much of the data in a prior payment as a reference. Because CAPS does not have a payment type code to identify the records as adjustments to previous payments, the transactions could be misinterpreted as duplicate payments by the computer routines designed by the Operation Mongoose Team.

Data Submissions to Operation Mongoose. Operation Mongoose did not receive crucial data needed for the successful performance of the fraud indicator routines. The submission of SAACONS contract data by Fort Belvoir did not contain all modification information related to contracts previously awarded. Data were submitted only for contract modifications that occurred within the same fiscal year quarter as the contract award date. The lack of modification data caused the number of observations to increase substantially on five fraud indicators relating to SAACONS, ranging from 582 observations to 5,481 observations. Accordingly, all contract modification data should be obtained by the DFAS for Operation Mongoose testing of fraud indicators.

System Edit Checks for Large Contracts. The CAPS edit checks cannot effectively process payments for large contracts with numerous payments. One large contract (DAHC94-91-C0002) for procurement of the Reserve Component Automation System had total payments in excess of $534 million since contract award in September 1990. Due to the volume of transactions, technicians in the Commercial Payments Division of the DAO could not adequately process payments for the contract. One request for payment of $3.7 million was accompanied by 148 DD Forms 250, "Material Inspection and Receiving Reports." The technicians at the DAO Fort Belvoir could not verify the validity of those payments in an efficient manner. Due to limitations of the CAPS, partial payments on this contract were coded as final payments in order to expedite processing in the system. Because of that coding, edit checks did not compare current payments to all prior payments on the contract. Therefore, this contract should be transferred to the Mechanization of Contract Administration Services system at the DFAS Columbus Center, Columbus, Ohio, because it has the capability to more efficiently process large contracts of this size.

Conclusions

When IG, DoD, recommendations in this report and in Report No. 96-134 are implemented, 52 out of 54 computer routines will be useful in detecting potentially fraudulent transactions. Accordingly, no additional CAPS and SRD1 sites should be selected for Operation Mongoose testing with those routines until identified problems are corrected. The DFAS agreed to correct the problems previously reported in IG, DoD, Report No. 96-134. However, those actions had not yet been completed prior to this evaluation.

Recommendations, Management Comments, and Evaluation Response

Deleted Recommendation. As a result of management comments, we deleted draft Recommendation A.4. and renumbered draft Recommendation A.5. to A.4.

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

1. Process a system software change to the Computerized Accounts Payable System, establishing a payment type code for adjustments to payment records.

Management Comments. DFAS concurred stating a system software change to Computerized Accounts Payable System will be made through the Computerized Accounts Payable System Consolidated Project. The estimated date of completion for the software change is December 31, 1997.

2. Obtain contract modification data needed for testing fraud indicator routines.

Management Comments. DFAS concurred stating that payment offices do not receive contract modifications in an automated interface. Payment offices manually input modifications into the payment systems. The estimated completion date to send the modification data to Operation Mongoose must be determined by the contracting proponent for Standard Army Automated Contracting System at Fort Lee, Virginia.

Evaluation Response. The intent of this recommendation was to identify the future need for the contract modification data for all contracting systems, including the Standard Army Automated Contracting System. We consider management comments responsive and no further comments are required.

3. Transfer payment responsibility for contract DAHC94-91-C0002 to the Mechanization of Contract Administration Services system, Defense Finance and Accounting Service Columbus Center, Columbus, Ohio.

Management Comments. DFAS stated that only contracts administered by Defense Contract Management Command are paid in the Mechanization of Contract Administration Services system. Also, since the IG, DoD, visit, much work has been done, both in research and in making the contract easier to pay. The contract is administered by the Information Systems Selection and Acquisition Agency (ISSA). ISSA now only sends two invoices monthly.

Evaluation Response. The management action taken for this contract should correct the deficiencies identified and satisfies the intent of the recommendation. The intent of the recommendation was to ensure adequate controls over contract payments, because the Computerized Accounts Payable System could not effectively process the high volume of payments on this large contract.

4. Discontinue Operation Mongoose testing of the Computerized Accounts Payable System and Standard Army Financial System Redesign-1 systems until identified problems are corrected.

Management Comments. DFAS concurred with the intent of the recommendation stating that discontinuance of testing should be based on an analysis weighing cost versus benefits versus erroneous data. Further, with new versions of CAPS coming on-line and changes that were made to SRD1, continued efforts of detecting fraud in the new CAPS and SRD1 are necessary.

Evaluation Response. We agree with management comments. The costs versus benefits were considered when we recommended further testing be discontinued until the identified changes have been implemented.

Finding B. Security Over Vendor Payment Data

Management of security over payment data at the Rome OPLOC did not comply with security policy in DoD Directive 5200.28, "Security Requirements for Automated Information Systems." Access to data was not effectively controlled because policies had not been implemented that require security over access to data. Also, the security officer had not sent user access reports to supervisors to limit user access to payment records. Further, Rome OPLOC management had not developed and implemented a contingency plan. As a result, unauthorized users could compromise or manipulate data without risk of detection.

System Security Environment

The system security environment requires a two-level process consisting of user identifications and passwords. Novell is the local area network software used to communicate with the CAPS data bases. Users normally log on to the Novell system before logging on to CAPS. The CAPS records are stored on a single data base in a locked file server room. The Rome OPLOC accounting technicians use CAPS to validate and process vendor payment data. The application security in CAPS limits user ability to access that data. Technicians transfer payment data onto a diskette that is used to transfer the data to the SRD1 mainframe computer at Rock Island, Illinois. 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 access level and need to use various data bases. The security officer then assigns a user identification number, and the user creates a password. Novell allows users to perform specific actions: read, write, create, erase, modify, and scan. When a password is created by 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 on to the system using the name of another individual who is an assigned user.

DoD Directive 5200.28, enclosure 3, "Minimum Security Requirements," establishes minimum requirements for system security. Key requirements include the following.

- Establish accountability for each person having access to the system.

- Establish access so that each user has access to all the information to which the user is entitled, but no more.

o Ensure that data integrity is in place to detect and minimize inadvertent modification or destruction of data, and detect and prevent malicious destruction or modification of data.

o Establish a contingency plan in accordance with OMB Circular A-130, "Management of Federal Information Resources," December 12, 1985.

Access to the data bases should be based on the functional responsibility of the user in conjunction with proper segregation of duties. Novell allows users to perform specific actions when using CAPS: read, write, create, erase, modify, and scan. CAPS is the application that generates the payment transaction. When a password and access rights are properly assigned to a user, data are protected.

Security Over Payment Data

Security Policy. Management of security over payment data at the Rome OPLOC did not comply with security policy in DoD Directive 5200.28. Access to data was not effectively controlled because policies had not been implemented that require security over access to data. Also, the security officer had not yet sent user access reports to supervisors to limit user access to payment records. Further, Rome OPLOC management had not developed and implemented a contingency plan.

Control Over Access to Vendor Payment Data. Rome OPLOC management had not established effective control over access to vendor payment data. The lack of access control for the Novell, CAPS, and SRD1 systems could affect the overall reliability of the payment data.

Novell. The network configuration at the Rome OPLOC allowed all (41) users to access vendor payment data files. Users could erase, modify, create, write, and read. Lack of controlled access was previously documented in "Computerized Accounts Payable System/Integrated Automated Travel System OPLOC Issues Meeting," June 23, 1995, prepared by DFAS Indianapolis Center Financial Systems Activity personnel:

> Both IATS [Integrated Automated Travel System] and CAPS functionals and installers have expressed concern about security of our data due to the user's ability to exit to DOS from Windows. The application requires that users have delete rights to the data directories--if they're logged in they can delete files. The Novell Filer utility lets you recover deleted files easily if you have a disgruntled employee with a password do something like this. You also have tape backups. . . . If you can't trust the user, take away his or her access.

Because the Novell configuration does not prevent users from gaining access to all vendor payment files and from deleting and changing the data, the Novell and CAPS need to be configured to allow only authorized users access to the payment records.

CAPS. Rome OPLOC 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. Five employees had access to the password table that allowed full access to CAPS. Only the security officer and an alternate should have access to the password table. The security officer should prevent access to the security table for all other employees. To ensure proper segregation of duties, those employees with access to the password table should be removed from CAPS functional capabilities. Additionally, of the 41 users, 1 employee who had been terminated still had user access because the Rome OPLOC had not implemented procedures for removing terminated employees from CAPS. In February 1996, the Rome OPLOC established procedures to remove user access for terminated employees.

SRD1. Access to SRD1 transactions were not properly controlled. Seven users had access rights that allowed them to input and approve payment transactions that allowed a disbursement to be made by a single person. Additionally, six users had access levels that were inconsistent with their job responsibilities.

User Access Reports. The security officer did not send the access reports on assigned users to their supervisors. As a result, no one was reviewing to see if user access was needed.

The Rome OPLOC became operational in June 1995. Because it was newly opened, the Rome OPLOC did not have a copy of the DoD Directive 5200.28 security policy, and the security officer had not sent reports on assigned users to supervisors to ensure that access was consistent with the functional responsibilities. Because supervisors did not receive the reports, they were unable to determine whether user access for Novell, CAPS, and SRD1 was appropriate. The security officer at the Rome OPLOC stated that he planned to provide reports on user access to supervisors to periodically review user access and to remove access when he was informed by a supervisor that access was no longer required for an employee.

Contingency Plan. Rome OPLOC management did not have a contingency plan in place to effectively recover computer records in the event of a disaster in accordance with OMB Circular A-130, Appendix II, "Contingency Plans." In addition, the Rome OPLOC was not using the off-site storage facility for backup files. Management stated that it planned to store backup tapes in a fireproof vault; however, as of May 17, 1996, the vault was not being used. OMB Circular A-130 requires agencies to establish policies and assign responsibilities to assure that appropriate contingency plans are developed, tested, and maintained by end users of information technology. Such plans should be consistent with disaster recovery and continuity of operations plans maintained by the installation at which the application is processed.

If a local disaster occurred, backup files would be needed to restore lost records. To ensure that vendor payment data are recovered and that records are restored, the Rome OPLOC needs to use the off-site location to store backup files.

Conclusions

The Rome OPLOC needs to ensure the overall reliability of the CAPS and SRD1 systems to provide for a more effective Operation Mongoose program. Safeguards over access to vendor payment data need strengthening to prevent the compromise or manipulation of data by unauthorized users without risk of detection. Further, Rome OPLOC management must implement security policies to prevent unauthorized access to payment records and to ensure that a contingency plan is developed and implemented.

Recommendations, Management Comments, and Evaluation Response

B. We recommend that the Deputy Director for Systems Administration, Rome Operating Location, Rome, New York, Defense Finance and Accounting Service, implement the security procedures as described in DoD Directive 5200.28, "Security Requirements for Automated Information Systems," March 21, 1988, as they relate to data. Specific actions should include:

1. Establish procedures to ensure that users with access to vendor payment and disbursing data have a valid need for that level of access.

Management Comments. DFAS concurred with the recommendation stating the minimal number of individuals needed to maintain the password file, and the security table will be assigned. Procedures to remove terminated employees will be completed by November 1, 1996. In addition, DFAS corrected the inappropriate access levels where users both input and certified disbursements.

2. Modify the Computerized Accounts Payable System and Novell interface to preclude unauthorized access to production files.

Management Comments. DFAS concurred in principle with the recommendation, stating that the Computerized Accounts Payable System W 1.0 will begin fielding in 1996 and is estimated to be completed in 1998.

3. Distribute user access listings to supervisors on a periodic basis to verify access rights.

Management Comments. DFAS concurred and stated it implemented the recommendation by monthly distribution of the access list.

4. Develop and implement a contingency plan in compliance with guidance in Office of Management and Budget Circular A-130, "Management of Federal Information Resources," December 12, 1985, that includes off-site storage of backup tapes.

Management Comments. DFAS concurred stating the plan will be completed by December 31, 1996.

Part II - Additional Information

Appendix A. Evaluation Process

Scope and Methodology

Vendor Payments. We evaluated vendor payment transactions in the CAPS and SRD1 at the DAO Fort Belvoir. 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 1995. In FY 1995, the DAO Fort Belvoir disbursed $342 million in vendor payments. We also evaluated the management controls at the Rome OPLOC designed to prevent and detect erroneous vendor payments in CAPS and SRD1. Our field work was performed at the DAO Fort Belvoir and the Rome OPLOC.

Evaluation Universe. DFAS has about 300 vendor payment activities. We selected the SAACONS, CAPS, and SRD1 at the DAO Fort Belvoir as our test site because:

o the DAO Fort Belvoir had completed its data submissions to Operation Mongoose for FY 1995,

o the geographic proximity of the DAO Fort Belvoir allowed for multiple visits, and

o less travel and temporary duty costs were incurred.

Evaluation Scope Limitations. The DAO Fort Belvoir was scheduled to consolidate with the Rome OPLOC in May 1996. The original consolidation date would have enabled the IG, DoD, to complete the analysis of the CAPS and SRD1 functions at Fort Belvoir before the consolidation and to make recommendations to DFAS regarding the reviewed systems. However, due to loss of key personnel at the DAO Fort Belvoir, the consolidation date was accelerated to October 1995. To review payment documentation, we visited the Rome OPLOC, where the related documents had been transferred. Accordingly, we evaluated the effectiveness of the computer routines and the computer security of the general system controls at the Rome OPLOC. Although the DAO Fort Belvoir was consolidated at the Rome OPLOC, the Directorate of Contracting and the related SAACONS data base remained at Fort Belvoir.

The SAACONS quarterly contracting data submitted to Operation Mongoose did not contain complete contract modification information. Operation Mongoose received contract modification data only if the modifications were issued in the same fiscal year quarter as the award date of the contract. Data supporting the contract modifications issued in subsequent periods were not obtained. Our review of the data showed that 5 of the 13 SAACONS routines would have been

more effective if all of the contract data had been obtained. Therefore, all contract modification data will be required in future quarterly data submissions to DMDC.

Request for Data. The Project Management Office for Operation Mongoose sent memorandums to the DFAS vendor paying activities and contracting activities to request contracting and disbursement data for FY 1995. The data were sent to the Operation Mongoose at Monterey, California, and were loaded on a mainframe computer.

Use of Computer-Processed Data. In July 1995, we visited the DAO Fort Belvoir and the Directorate of Contracting at Fort Belvoir, Virginia, and developed 31 computer routines. In addition, we used 23 computer routines that we had previously developed and used at the DFAS Columbus Center, Ohio.

CAPS disbursement data from the DAO Fort Belvoir for FY 1995 were loaded on the mainframe 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.

To validate the payments shown on the DMDC reports of potentially fraudulent or improper payment transactions, we compared the payments to the supporting documentation. 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, disbursing officers, and the U.S. Postal Service. To verify payment records, we made inquiries to the SRD1, CAPS, and SAACONS. We also requested copies of questionable checks from the U.S. Treasury and verified check cancellations with the U.S. Treasury. At the conclusion of our evaluation, we summarized the results, recommendations, and needed changes to the fraud indicators.

Files Moved to the Rome OPLOC. When the DAO Fort Belvoir closed in October 1995, the vouchers for FYs 1994 and 1995 were sent to the Rome OPLOC. The FY 1995 vouchers were maintained by voucher number sequence in filing cabinets at the Rome OPLOC.

Evaluation Period and Standards. This evaluation was performed from July 1995 through May 1996 in accordance with auditing standards implemented by the Inspector General, DoD. The evaluation did not rely on statistical sampling procedures.

Organizations and Individuals Visited or Contacted

Contacts During the Evaluation. We visited or contacted individuals within the DoD. Further details are available upon request.

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 the Management Control Program. We reviewed the adequacy of management controls over vendor payments at the Rome Operating Location. Specifically, we reviewed management controls over user access to payment records. Because the Rome OPLOC became operational in June 1995, we did not assess management's self evaluation of those controls.

Adequacy of Management Controls. We identified a material management control weakness for the Rome OPLOC as defined by DoD Directive 5010.38. Controls were not adequate to ensure compliance with security procedures described in DoD Directive 5200.28. Managers did not review user access listings, access levels did not coincide with job descriptions and a contingency plan had not been implemented.

Recommendation B., if implemented, will improve the Rome OPLOC controls over access to vendor payment data. A copy of the report will be provided to the senior official responsible for management controls in DFAS.

Appendix B. Prior Evaluations and Other Reviews

During the last 5 years, the Inspector General, DoD, issued two reports discussing vendor payments by the Defense Finance and Accounting Service.

Inspector General, DoD

Inspector General, DoD, Report No. 96-134, "Vendor Payments-Operation Mongoose," May 30, 1996. This report was the first in a series of reports under Operation Mongoose. The audit was performed on the CAPS at the DFAS Columbus Center, Columbus, Ohio. The report states that 10 of the 25 computer routines developed by Operation Mongoose to identify fraudulent payments could not be relied on to detect potential fraud. The report further states that 6 of the 10 ineffective routines could be effective if data formats were standardized, edit controls were incorporated into the software, and operating procedures were improved and enforced. Also, security over automated payment records needed strengthening. Access to data was not effectively controlled because security reports were not provided to supervisors and because management did not effectively control access to computer files and did not make proper use of off-site storage. The report recommends that the Director, DFAS, establish procedures to standardize formats for entering data, require vendor payments to be entered into CAPS before processing in the SRD1 system, and process system changes to the CAPS. The report also recommends that the Director, DFAS, perform security reviews of all vendor payment activities and establish effective access controls over payment and disbursing data. DFAS Headquarters and DFAS Columbus Center generally agreed with the findings and recommendations. The CAPS consolidation project will correct five weaknesses, corrective action has been completed on nine recommendations, actions are still ongoing for two recommendations, and comments on one recommendation are still outstanding.

Inspector General, DoD, Report No. 96-030, "Vendor Payments at Defense Accounting Offices," November 30, 1995. This report discusses two DoD Hotline complaints alleging that duplicate payments were disbursed by the Defense Accounting Office Oakland, California. A review of vendor payment procedures at five DAOs showed weaknesses in the areas of processing vendor payments and methods of detecting duplicate payments. In addition, the data bases containing vendor payment transaction histories were incomplete and inadequate. The report also states that management did not effectively implement a management control program at the Defense Accounting Offices. The report recommends that the Under Secretary of Defense (Comptroller) direct the Director, DFAS, to accelerate the planned migration to a comprehensive vendor payment system and that DFAS establish procedures for improving oversight over contract balances and for transferring data and documentation during consolidation of the Defense Accounting Offices. The

report also recommends that DFAS periodically review the implementation of the management control program at Defense Accounting Offices and operating locations and improve oversight of the management control program. Management generally concurred with the findings and recommendations. Actions on twelve recommendations were completed as of December 1996. Corrective action is ongoing for the remaining two recommendations.

Appendix C. Description of Computer Routines

Useful Routines

1. **Duplicate check numbers in SRD1.**

   Purpose: To identify checks with previously used check numbers. This routine was previously used at the DFAS Columbus Center.

   Results: Total of 0 observations; 0 observations analyzed.

   Suggestion: This routine should be used at each site.

2. **Duplicate system document numbers.**

   Purpose: To identify payments for which the system document number was changed to another system document number to hide fraudulent activity.

   Results: Total of 0 observations; 0 observations analyzed.

   Suggestion: This routine should be used at each site.

3. **Payments without voucher numbers in SRD1.**

   Purpose: To identify payments in SRD1 for which voucher numbers were deleted. This routine was previously used at the DFAS Columbus Center.

   Results: Total of 0 observations; 0 observations analyzed.

   Suggestion: This routine should be used at each site.

4. **Payments without check numbers in SRD1.**

   Purpose: To identify payments in SRD1 for which the check number was deleted. This routine was previously used at the DFAS Columbus Center.

   Results: Total of 0 observations; 0 observations analyzed.

   Suggestion: This routine should be used at each site.

5. Payments without a check amount.

Purpose: To identify payments in SRD1 with the check amounts deleted. This routine was previously used at the DFAS Columbus Center.

Results: Total of 0 observations; 0 observations analyzed.

Suggestion: This routine should be used at each site.

6. Payments with invalid vendor names or without vendor names in SRD1.

Purpose: To identify invalid payments in SRD1. This routine was previously used at the DFAS Columbus Center.

Results: Total of 0 observations; 0 observations analyzed.

Suggestion: This routine should be used at each site.

7. Payments without addresses in SRD1.

Purpose: To identify payments with the addresses deleted in SRD1. This routine was previously used at the DFAS Columbus Center.

Results: Total of 0 observations; 0 observations analyzed.

Suggestion: This routine should be used at each site.

8. Payments made without showing a voucher examiner.

Purpose: To identify payments made in SRD1 without the voucher examiner identified. This routine was previously used at the DFAS Columbus Center.

Results: Total of 0 observations; 0 observations analyzed.

Suggestion: This routine should be used at each site.

9. Payments with negative check amounts in SRD1.

Purpose: To identify payments with negative check amounts in SRD1. This routine was previously used at the DFAS Columbus Center.

Results: Total of 0 observations; 0 observations analyzed.

Suggestion: This routine should be used at each site.

10. Valid DoD Activity Address Code (DoDAAC).

Purpose: To identify whether contract prefix is on the DoDAAC listing.

Results: Total of 0 observations; 0 observations analyzed.

Suggestion: This routine should be used at each site.

11. Valid contract fiscal year.

Purpose: To identify whether an old contract number had been used in the current fiscal year.

Results: Total of 0 observations; 0 observations analyzed.

Suggestion: This routine should be used at each site.

12. Valid contract number.

Purpose: To identify whether the contract had invalid characters in the last four characters of the contract number.

Results: Total of 0 observations; 0 observations analyzed.

Suggestion: This routine should be used at each site.

13. Duplicate check numbers in CAPS.

Purpose: To identify checks with previously used check numbers in CAPS.

Results: Total of 28 observations; 28 observations analyzed.

Cause: Technicians made adjustments in CAPS to correct errors and used the check number, check date, voucher number, etc., to reference the changed voucher.

Suggestions: Establish a payment type code to identify adjustment records. This routine should be used at each site.

14. Payments with invalid vendor names or no vendor names in CAPS.

Purpose: To identify invalid payments in CAPS.

Results: Total of 0 observations; 0 observations analyzed.

Suggestion: This routine should be used at each site.

15. Payments without addresses in CAPS.

Purposes: To identify payments with the addresses deleted in CAPS.

Results: Total of 0 observations; 0 observations analyzed.

Suggestion: This routine should be used at each site.

16. Payments made without showing a voucher examiner in CAPS.

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

Results: Total of 0 observations; 0 observations analyzed.

Suggestion: This routine should be used at each site.

17. Payments without contract numbers in CAPS.

Purpose: To identify payments in CAPS with the contract numbers deleted.

Results: Total of 0 observations; 0 observations analyzed.

Suggestion: This routine should be used at each site.

18. Payments with negative check amounts in CAPS.

Purpose: To identify payments with negative check amounts in CAPS.

Results: Total of 0 observations; 0 observations analyzed.

Suggestion: This routine should be used at each site.

19. Payments in SRD1 that were not in CAPS.

Purposes: To identify payments that were made in SRD1 that should have but did not have a corresponding payment in CAPS. This routine was previously used at the DFAS Columbus Center.

Results: Total of 1 observation; 1 observation analyzed.

Cause: Payment was in CAPS.

Suggestion: This routine should be used at each site.

20. Amount of check in SRD1 differed from amount in CAPS.

Purpose: To identify altered check amounts. This routine is the combination of two routines previously used at the DFAS Columbus Center.

Results: Total 2 observations; 2 observations analyzed.

Cause: Valid changes to payment amount.

Suggestion: This routine should be used at each site.

21. Invoices paid on closed contracts.

Purpose: To identify fraudulent payments made on closed contracts. This routine was previously used at the DFAS Columbus Center.

Results: Total of 95 observations; 95 observations analyzed.

Causes: Partial and final payments were input into CAPS on or near the same date, and the final payment was processed in SRD1 before the valid partial payments had been input into CAPS. One unusually large contract with hundreds of payments coded partial payments as final payments to expedite the payment process. That action was taken because CAPS could not efficiently handle the number of payments on this contract and caused excessive processing time.

Suggestions: Enforce compliance with procedures. This routine should be used at each site.

22. Payments without voucher numbers in CAPS.

Purpose: To identify payments in CAPS for which voucher numbers were deleted.

Results: Total of 25 observations; 11 observations analyzed.

Cause: CAPS data do not accurately reflect transaction history.

Suggestions: Enforce compliance with procedures to correctly upload data into CAPS. This routine should be used at each site.

23. Duplicate contract numbers in CAPS.

Purpose: To identify duplicate payments in CAPS.

Results: Total of 10 observations; 10 observations analyzed.

Cause: The checks were canceled, precluding duplicate payments.

Suggestion: This routine should be used at each site.

Routines That Require Changes to be Useful

1. **Duplicate invoice numbers in SRD1.**

   Purpose: To identify duplicate payments in SRD1.

   Results: Total of 168 observations; 155 observations analyzed.

   Causes: The Judge Advocate General, not the Commercial Accounts Payable Division, processed 152 of the observations. The date of the invoice was used incorrectly as the invoice number for billings on nonstandard contracts.

   Suggestion: This routine should be modified to include only the Commercial Accounts Payable Division and used at each site.

2. **Same contract numbers and same payment numbers in SRD1.**

   Purposes: To identify payments in SRD1 with the same contract numbers and same payment numbers to detect duplicate payments. This routine was previously used at the DFAS Columbus Center.

   Results: Total of 238 observations; 238 observations analyzed.

   Causes: Of the observations, 234 were payments made by the Judge Advocate General, not the Commercial Accounts Payable Division.

   Suggestions: This routine should be modified to include only the Commercial Accounts Payable Division payments and should be used at each site.

3. **Payments without valid voucher numbers.**

   Purpose: To identify payments in SRD1 for which voucher numbers had been removed or were invalid numbers.

   Results: Total of 1,274 observations; 1,274 observations analyzed.

   Cause: These observations were payments made by the Judge Advocate General, not the Commercial Accounts Payable Division.

   Suggestion: This routine should be modified to include only the Commercial Accounts Payable Division payments and should be used at each site.

4. **Payments without valid check numbers.**

   Purpose: To identify payments in SRD1 for which the check number was deleted or outside the expected range.

   Results: Total of 1,358 observations; 29 observations analyzed.

Cause: The check numbers were in SRD1. The data submission was incomplete.

Suggestion: This routine should be used at each site.

5. **Payments without contract numbers in SRD1.**

Purpose: To identify payments in SRD1 with deleted or invalid contract numbers. This routine was previously used at the DFAS Columbus Center.

Results: Total of 2,257 observations; 2,257 observations analyzed.

Cause: All payments represented processing of Judge Advocate General claims, not vendor payments. All Judge Advocate General claims were processed on nonstandard, numeric contract numbers. These payments were not made by the Commercial Accounts Payable Division.

Suggestion: This routine should be modified to include only the Commercial Accounts Payable Division payments and should be used at each site.

6. **Improper streamlined payments.**

Purpose: Identify those SAACONS contracts with foreign payments and compare with SRD1 payment data.

Results: Total of 0 observations; 0 observations analyzed.

Cause: Data submissions did not include fields needed for this routine.

Suggestion: Obtain needed data for routine. This routine should be used at each site.

7. **Duplicate invoice numbers in CAPS.**

Purpose: To identify duplicate payments with the same invoice number.

Results: Total of 859 observations; 96 observations analyzed.

Causes: Monthly invoices were received for quarterly payments. CAPS data do not accurately reflect transaction history.

Suggestion: This routine should not be used until quarterly payments of monthly invoices are identifiable.

8. **Payments without check numbers in CAPS.**

Purpose: To identify payments in CAPS for which the check numbers were deleted.

Results: Total of 34 observations; 9 observations analyzed.

Cause: Disbursement information in SRD1 was not uploaded to CAPS. CAPS data do not accurately reflect transaction history.

Suggestion: Procedures should be enforced. This routine should be used at each site.

9. Payments without a check amount in CAPS.

Purpose: To identify payments in CAPS with the check amounts deleted.

Results: Total of 16 observations; 16 observations analyzed.

Cause: Adjusting entry to close account. Prior payment data (check number, check date, etc.) are used for a reference when an adjustment is made. CAPS does not accurately reflect transaction history.

Suggestion: There should be a payment type code in CAPS to identify adjustment records. This routine should not be used until an adjustment code exists.

10. Payment addresses in SRD1 that differ from payment addresses in CAPS.

Purpose: To identify payments sent to an unauthorized payee. This routine was previously used at the DFAS Columbus Center.

Results: Total of 1,407 observations; 75 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: CAPS has been revised to allow multiple vendor addresses. This routine should not be used until data are standardized.

11. Payee names in SRD1 that differ from payee names in CAPS.

Purpose: To identify payments in which payee names were altered and the checks were sent to unauthorized payee. This routine was previously used at the DFAS Columbus Center.

Results: Total of 43 observations; 43 observations analyzed.

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

Suggestions: Establish standardized data format. CAPS has been revised to allow multiple vendor names. This routine should not be used until the data are standardized.

12. Manager/Supervisor approved payment in SRD1, not in CAPS.

Purpose: To identify those payments by individuals with delete and streamline authority.

Results: Total of 2,467 observations; 0 observations analyzed.

Remarks: Payments were routinely approved by managers and supervisors. Therefore, these observations were not reviewed.

Suggestion: This routine should be used at each site and should be reviewed for unusual patterns or on a sample basis.

13. Manager/Supervisor approved payment in CAPS, not in SRD1.

Purpose: To identify those payments made by individuals with delete and streamline authority.

Results: Total of 4,965 observations; 0 observations analyzed.

Remarks: Payments were routinely approved by managers and supervisors. Therefore, these observations were not reviewed.

Suggestion: This routine should be used at each site and should be reviewed for unusual patterns or on a sample basis.

14. Multiple Contractors with the same remit to address.

Purpose: To identify a potential diversion of funds or fraudulent activity by a vendor.

Results: Total of 2,896 observations; 660 observations analyzed.

Cause: Contractor name was the same; however, contractor addresses and other information were not standardized.

Suggestion: Standardize the remittance address format. This routine should not be used until data are standardized.

15. Different remit to address for the same vendor.

Purpose: To identify a potential diversion of funds or fraudulent activity by a vendor.

Results: Total of 8,228 observations; 0 observations analyzed.

Cause: The data format is not the same in both systems.

Suggestion: Data should be standardized at all CAPS sites. This routine should not be used until data are standardized.

16. Contracts awarded before FY 1993 with payments made in FY 1995.

Purpose: To identify fraudulent payments made on inactive contracts. This routine was previously used at the DFAS Columbus Center.

Results: Total of 1,124 observations; 49 observations analyzed.

Causes: The payments were on multiyear service or maintenance contracts; some receiving activities had not sent supporting documentation.

Suggestions: This routine should be modified to exclude delivery order contracts. This routine should be used at each site.

17. Payments made by high-risk employees.

Purpose: To identify potential fraudulent activity by an employee identified as high risk by auditors. This routine was previously used at the DFAS Columbus Center.

Results: Total of 3,624 observations; 0 observations analyzed.

Cause: Employees with higher access levels processed many payments as a routine business practice.

Suggestion: This routine should be used at each site and should be reviewed for unusual patterns or on a sample basis.

18. Payments where the records were changed.

Purpose: To identify payment records in one SRD1 file and to compare to another SRD1 file for payment record modifications.

Results: Total of 1,358 observations; 0 observations analyzed.

Remarks: Observations were not reviewed due to the significant number of observations.

Suggestion: This routine should be used at each site and should be reviewed for unusual patterns or on a sample basis.

19. Payments with high risk.

Purpose: To identify high-risk, streamlined payments.

Results: Total of 5,887 observations; 46 observations analyzed.

Cause: At least four Fort Belvoir tenant activities were processing precertified payments into SRD1, bypassing CAPS. Only 3 percent of streamlined payments were by the Commercial Accounts Payable Division.

Suggestion: This routine should not be used at the other sites, if streamlined payments are routinely processed.

20. Payments on contracts that should be but are not in SAACONS.

Purpose: To identify contracts containing the DoDAAC for the Fort Belvoir Directorate of Contracting that were paid in SRD1, but were not in SAACONS.

Results: Total of 5,481 observations; 64 observations analyzed.

Cause: Two other activities issued valid contracts under the Fort Belvoir DoDAAC; those contracts were not included on the SAACONS data base. Before submission of the SAACONS data, the SAACONS data base purged closed contracts, causing it to appear that those contracts were never in SAACONS.

Suggestion: This routine should be used at each site. However, Operation Mongoose should be aware that there are contracts that are manually produced that will not appear in the SAACONS.

21. Fast Payment contracts with a single payment over the limit.

Purpose: Fast Payment contracts paid with one payment over the limit.

Results: Total of 0 observations; 0 observations analyzed.

Cause: There is no Fast Payment indicator.

Suggestion: If a Fast Payment indicator can be identified, this routine should be used at each site.

22. Fast Payment contracts over the limit.

Purpose: To identify fast payment contracts in SAACONS and to find payments in SRD1 that are over the contract amount.

Results: Total of 0 observations; 0 observations analyzed.

Cause: The SAACONS data containing the Fast Payment indicator was not received in the data submission. SRD1 does not have a Fast Payment indicator.

Suggestion: If a Fast Payment indicator can be identified, this routine should be used at each site.

23. Fast Payment contracts near threshold.

Purpose: To identify contracts that were Fast Payment contracts and to identify in SRD1 those Fast Payment contracts for which the payments are greater than $23,000 but less than $25,000. This routine was previously used at the DFAS Columbus Center.

Results: Total of 0 observations; 0 observations analyzed.

Cause: There is no Fast Payment indicator.

Suggestion: If a Fast Payment indicator can be identified, this routine should be used at each site.

24. Comparison of vendor name.

Purpose: To compare the vendor name in SAACONS with the vendor name in SRD1.

Results: Total of 582 observations; 582 observations analyzed.

Cause: Contracts were paid to different officials of the particular contractor, to different vendors due to mergers, to parent companies, and to companies that were not on the contract. Some payment irregularities resulted from noncompliance with regulatory guidance, requiring modification of the contract prior to payment. Some observations were caused by incomplete modification data submitted to DMDC.

Suggestion: Enforce compliance with procedures and regulatory guidance. This routine should not be used until modification data are obtained.

25. Comparison of vendor address.

Purpose: To compare the vendor address in SRD1 with the vendor address in SAACONS.

Results: Total of 3,934 observations; 313 observations analyzed.

Cause: Payments were sent to addresses not shown in the remittance address in the contracting system. Some of the observations resulted from noncompliance with regulatory guidance, requiring modification of contracts prior to making payment. Also, data submission did not include some modification data.

Suggestion: Enforce compliance with procedures and regulatory guidance. Ensure submissions contain all contract modification data. This routine should be used at each site.

26. Comparison of contract modifications.

Purpose: To identify contract modifications in SAACONS and then in CAPS and SRD1.

Results: Total of 0 observations; 0 observations analyzed.

Cause: SAACONS data do not provide modifications to CAPS and SRD1. SRD1 and CAPS do not identify modification data.

Suggestion: This routine should not be used until all modification data are obtained.

27. Comparison of contract line item numbers.

Purpose: To identify SRD1 payments that were made on an invalid line item number for that same contract in SAACONS.

Results: Total of 651 observations; 0 observations analyzed.

Remark: Observations not reviewed due to incomplete modification data.

Suggestion: This routine should not be used until modification data are obtained.

28. Disbursements in excess of the contract amount.

Purpose: To compare the contract amount in SAACONS to the payments in SRD1 and to identify contracts that were overdisbursed.

Results: Total of 3,029 observations; 243 observations analyzed.

Cause: The overdisbursements were related to interest and freight charges. Many observations could have been avoided if all contract modification data had been submitted.

Suggestion: This routine should not be used until all contract modification data are obtained by DMDC.

29. Duplicate payment records in CAPS.

Purpose: To identify duplicate payments in CAPS.

Results: Total of 2,577 observations; 2,577 observations analyzed.

Cause: CAPS did not clearly reflect the status of the transactions.

Suggestion: This routine should not be used at the CAPS sites until transactions status is identifiable.

30. Old contracts with current payments.

Purpose: To identify duplicate payments in CAPS.

Results: Total of 157 observations; 0 observations analyzed.

Remark: This routine was also performed on SRD1 data; we did not review these observations due to data reliability and accuracy.

Suggestion: This routine should not be used at the CAPS sites until receiving activities and vendors send their documentation on a timely basis.

31. Invoices paid on closed contracts in CAPS.

Purpose: To identify duplicate payments in CAPS.

Results: Total of 157 observations; 0 observations analyzed.

Remark: This routine was also performed on SRD1 data; we did not review these observations due to lack of adherence to procedures.

Suggestion: This routine should not be used at the CAPS sites until procedures are complied with and payments are made in order.

Appendix D. 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

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

NOV - 1 1996

DFAS-HQ/FCC

MEMORANDUM FOR ACTING DIRECTOR, FINANCE AND ACCOUNTING DIRECTORATE, OFFICE OF THE INSPECTOR GENERAL, DEPARTMENT OF DEFENSE

SUBJECT: Response to DoDIG Draft Report "Vendor Payments-Operation Mongoose, Fort Belvoir Defense Accounting Office and Rome Operating Location," dated July 26, 1996 (Project No. 5FG-5016.01)

Attached are the comments to draft report. Please direct any questions concerning this matter to Mr. Jack Foust, DFAS-HQ/FCC, Commercial (703) 607-5030.

for Mr Elwell
Roger W. Scearce
Brigadier General, USA
Deputy Director for Finance

Attachments:
As stated

DEFENSE FINANCE AND ACCOUNTING SERVICE
COMMENTS ON DoD IG DRAFT REPORT, VENDOR
PAYMENTS-OPERATION MONGOOSE, FORT BELVOIR
DEFENSE ACCOUNTING OFFICE AND ROME OPERATING
LOCATIONS, DATED JULY 26, 1996

Finding A. Fraud Indicators (Page 11 of subject report):

RECOMMENDATION A.1: Process a system software change to the Computerized Accounts Payable System, establishing a payment type code for adjustments to payment records.

DFAS RESPONSE: Concur. Currently DFAS-IN is in the process of upgrading CAPS with a project called: CAPS Consolidated Project (CCP). Implementation began in October 1996 with software acceptance testing. Since payment type adjustment code is not contained in new CAPS we will review the results of Operation Mongoose at the locations with current CAPS and recommended a system change request to be included in the first update of the new CAPS. Expected completion date: December 31 1997.

RECOMMENDATION A 2: Obtain contract modification data needed for testing fraud indicator routines.

DFAS RESPONSE: Concur with the understanding that the payment office is not the focal point for this recommendation. Contract modifications do not post to the payment office by automated flow. They are manually input by the paying office upon receipt from the contracting office. Completion Date: Must be determined by proponent for SAACONS at Fort Lee, VA.

RECOMMENDATION A 3: Transfer payment responsibility for Contract DAHC94-91-C0002 to the Mechanization of Contract Administration Services system, Defense Finance Accounting Service Columbus Center, Columbus, Ohio. Any other large contracts similar to DAHC94-91-C0002 should be transferred to the Mechanization of Contract Administration Services system, Defense Finance Accounting Service Columbus Center, Columbus, Ohio.

DFAS RESPONSE Nonconcur. DFAS policy is that only contracts administered by Defense Contract Management Command (DCMC) are paid in MOCAS. All other contracts are paid at the accounting station supporting the ordering activity. Since the DoDIG visit, much work has been done, both in research and in making this

Final Report Reference

2

contract easier to pay. The contract is administered by the Information Systems Selection and Acquisition Agency (ISSAA). To better support our payment requirements, ISSAA now sends only two (2) invoices monthly:

a. One invoice for fixed costs as well as time and material, and

b. A second invoice for services. These services are actually documented on a series of delivery orders, and the delivery orders are summarized on the monthly invoice.

These two invoices replace the approximately 150-200 invoices being processed monthly at the time of the initial DoDIG visit.

The invoices are routed through the Reserve Component Automated System (RCAS)office prior to submission to Rome. The RCAS office certifies the propriety of the payment (receiving report function) as well as fund availability.

After thorough investigation, we determined this contract is best paid under CAPS at Rome. Further, this is the wish of the contract administrator who has exerted significant effort to make this contract easier (and "safer") for us to pay. We have decided to leave payment for this contract at Rome. No action required.

Deleted

RECOMMENDATION A 4: Establish guidance requiring that all large contracts be paid from the Mechanization of Contract Administration Services system, Defense Finance Accounting Service Columbus Center, Columbus, Ohio.

DFAS RESPONSE: Non-concur. The Federal Acquisition Regulation 42.205 Designation of the Paying Office; the Department of Defense Federal Acquisition Regulations System 242.205 Designation of the Paying Office; and the Department of Defense Directory of Contract Administration Services (CAS) Components Manual stipulate the exact method of determining the proper payment office for all contracts. Dollar value is one of many criteria used to determine the proper payment office.

The CAS Components Manual states that a contract must be administered by the Defense Contract Management Command (DCMC) in order to be assigned to DFAS-CO for payment in MOCAS. Action complete.

Final Report Reference

3

RECOMMENDATION A 5: Discontinue Operation Mongoose testing of the Computerized Accounts Payable System and Standard Army Financial System Redesign-1 systems until identified problems are corrected.

Renumbered to A.4. Page 10

DFAS RESPONSE: Concur with intent. However, the project of Operation Mongoose covers all types of government payments and is not restricted to only payments to commercial vendors. There have been many DFAS successes with Operation Mongoose in other areas such as Civilian Pay and Military Pay. We do recognize that there are some shortfalls with CAPS and SRD-1; however, before efforts are completely discontinued an analysis of cost versus benefit versus erroneous data needs to be performed in relation to the CAPS/SRD-1 problems. In addition, Operation Mongoose has refined fraud indicators and templates for the matches require ongoing research and review. With a new version of CAPS coming on-line in the near future and with changes that have already been made in SRD-1, continuing the effort of detecting fraud in the new CAPS and SRD-1 are necessary.

FINDING B. Security Over Vendor Payment Data (Page 16 of subject report):

RECOMMENDATION B 1: Establish procedures to ensure that users with access to vendor payment and disbursing data have a valid need for that level of access.

DFAS RESPONSE:

a. CAPS: We concur that users must have a valid need to access vendor payment and disbursing data. The access to the password file is controlled in Vendor Pay at the Rome OPLOC by one primary POC and two alternates. Due to the size of the work force and the extensive mission-related TDY, we need three people with this access, not two as recommended in the draft. With regard to the security table, we interpret this as access to the systems manager function, and that a primary and one alternate need access to this, again for the same reasons. We do not concur with the recommendation in the draft audit that only one person have access to this function. A backup person is essential in order to maintain continuity of operations. We concur that any terminated employee should be immediately deleted from the system. We consider it wise to have a clearing procedure established so that Systems Office is always notified when an

employee leaves. We will implement a procedure within the next sixty days. Completion Date: November 1, 1996.

b. SRD-1: We concur that the same employee should not be able to input and certify a transaction resulting in a disbursement. We concur that users' access levels should be consistent with their job responsibilities. Vendor Pay personnel that require SRD-1 have a set list of entry points depending upon their duties and this is requested by their supervisor for the Systems Office for input. The deficiencies in multiple access stated in subject report have been corrected. Completion Date: Completed.

RECOMMENDATION B 2. Modify the computerized Accounts Payable System and NOVELL interface to preclude unauthorized access to production files.

DFAS RESPONSE: Concur in principle. The upgrade of CAPS (CCP) (CAPS W1.0) will use a relational database management system maintained by a centralized data processing center. Users must have the necessary access level to obtain entry to the new processing environment. Users will no longer be able to gain direct access to the production files. The Software Acceptance Test for the new version of CAPS is currently being conducted at the Orlando Operating Location and should be in full production at that site in November 1996. Subsequent fielding of CAPS W1.0 will take place during the remainder of 1996 and continue to sometime in 1998. The new operating environment satisfies the intent of the recommendation. Completion Date 1998.

RECOMMENDATION B 3. Distribute user access listings to supervisors on a periodic basis to verify access rights.

DFAS RESPONSE: Concur. We have implemented this recommendation. On a monthly basis, we distribute the SRD-1 listing displaying entry points to supervisors to verify the priority of the system access by their staff. Modifications are made as required. Completion Date: Completed.

RECOMMENDATION B 4. Develop and implement a contingency plan in compliance with guidance in Office of Management and Budget Circular A-130, "Management of Federal Information Resources", December 12, 1985, that includes off-site storage of backup tapes.

5

DFAS RESPONSE. Concur. We are in the very early stages of standing up the OPLOC. We are in the process of working with DFAS-Indianapolis in regard to further development of an overall security plan. We do backup the network server on daily, weekly, and monthly basis. The weekly and monthly tapes are stored in a GSA approved fire-resistant safe. We do need to work on the off-site storage and hope to have this in place within the next ninety days. Completion Date: December 31, 1996.

Evaluation Team Members

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

F. Jay Lane
Christian Hendricks
Carl F. Zielke
John E. Byrd
Ralph W. Swartz
Robert M. Dieter
Geoffrey L. Weber
Kelly E. Young
Nancy C. Cipolla
Traci Y. Sadler