

A *udit*



R *eport*

CONTROLS OVER ELECTRONIC DOCUMENT MANAGEMENT

Report No. D-2001-101

April 16, 2001

**Office of the Inspector General
Department of Defense**

Form SF298 Citation Data

Report Date <i>("DD MON YYYY")</i> 16Apr2001	Report Type N/A	Dates Covered (from... to) <i>("DD MON YYYY")</i>
Title and Subtitle Controls Over Electronic Document Management		Contract or Grant Number
		Program Element Number
Authors		Project Number
		Task Number
		Work Unit Number
Performing Organization Name(s) and Address(es) OAIG-AUD (ATTN: AFTS Audit Suggestions) Inspector General, Department of Defense 400 Army Navy Drive (Room 801) Arlington, VA 22202-2884		Performing Organization Number(s) D-2001-101
Sponsoring/Monitoring Agency Name(s) and Address(es)		Monitoring Agency Acronym
		Monitoring Agency Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited		
Supplementary Notes		
Abstract On May 21, 1997, the Under Secretary of Defense (Comptroller) directed the move to a paper-free contracting process which would modernize the acquisition processes of contract writing, administration, finance, and auditing. The Defense Finance and Accounting Service (DFAS) initiated Electronic Document Management as part of the DoD Paper-Free Contracting Initiative. Electronic Document Management contributes to the initiative by digitizing paper documents and offering read-only access to official contracts and modifications, invoices, and accounting and finance documents. Personnel at DFAS Columbus rely on the information accessed from Electronic Document Management to make an average of 82,000 contract payments totaling \$6 billion each month (\$72 billion annually). The Director, DFAS Columbus, requested that we review Electronic Document Management to determine whether sufficient safeguards are in place to ensure the security of electronic contract data.		
Subject Terms		
Document Classification unclassified		Classification of SF298 unclassified

Classification of Abstract unclassified	Limitation of Abstract unlimited
Number of Pages 31	

Additional Copies

To obtain additional copies of this audit report, visit the Inspector General, DoD, Home Page at www.dodig.osd.mil/audit/reports or contact the Secondary Report Distribution Unit of the Audit Followup and Technical Support Directorate at (703) 604-8937 (DSN 664-8937) or fax (703) 604-8932.

Suggestions for Audits

To suggest ideas for or to request audits, contact the Audit Followup and Technical Support Directorate at (703) 604-8940 (DSN 664-8940) or fax (703) 604-8932. Ideas and requests can also be mailed to:

OAIG-AUD (ATTN: AFTS Audit Suggestions)
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-4704

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, DC 20301-1900. The identity of each writer and caller is fully protected.

Acronyms

DFAS	Defense Finance and Accounting Service
DITSCAP	DoD Information Technology Security Certification and Accreditation Process
DPSS	Defense Procurement Payment System
EDM	Electronic Document Management
MOCAS	Mechanization of Contract Administration Services



INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-4704

April 16, 2001

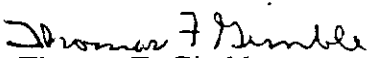
MEMORANDUM FOR DIRECTOR, DEFENSE FINANCE AND ACCOUNTING
SERVICE

SUBJECT: Audit Report on Controls Over Electronic Document Management
(Report No. D-2001-101)

We are providing this report for your information and use. We conducted the audit in response to a request from the Director, Defense Finance and Accounting Service Columbus, to determine whether sufficient safeguards are in place to ensure the accuracy of stored electronic contractual data within Electronic Document Management. We considered management comments on a draft of this report in preparing the final report.

DoD Directive 7650.3 requires that all recommendations be resolved promptly. The comments received from Defense Finance and Accounting Service were partially responsive. The comments on the draft of this report conformed to the requirements; however, additional comments are needed on Recommendation 3. We request that management provide additional details in comments to the final report by June 16, 2001.

We appreciate the courtesies extended to the audit staff. For additional information on this report, please contact Ms. Kimberley Caprio at (703) 604-9139 (DSN 664-9139) (kcaprio@dodig.osd.mil) or Mr. Eric Lewis at (703) 604-9144 (DSN 664-9144) (elewis@dodig.osd.mil). See Appendix C for the report distribution. The audit team members are listed inside the back cover.


Thomas F. Gimble
Acting
Deputy Assistant Inspector General
for Auditing

Office of the Inspector General, DoD

Report No. D-2001-101

(Project No. D2000FG-0057.02)

April 16, 2001

Controls Over Electronic Document Management

Executive Summary

Introduction. On May 21, 1997, the Under Secretary of Defense (Comptroller) directed the move to a paper-free contracting process which would modernize the acquisition processes of contract writing, administration, finance, and auditing. The Defense Finance and Accounting Service (DFAS) initiated Electronic Document Management as part of the DoD Paper-Free Contracting Initiative. Electronic Document Management contributes to the initiative by digitizing paper documents and offering read-only access to official contracts and modifications, invoices, and accounting and finance documents. Personnel at DFAS Columbus rely on the information accessed from Electronic Document Management to make an average of 82,000 contract payments totaling \$6 billion each month (\$72 billion annually). The Director, DFAS Columbus, requested that we review Electronic Document Management to determine whether sufficient safeguards are in place to ensure the security of electronic contract data.

Objectives. The audit objective was to determine whether the security of Electronic Document Management at DFAS Columbus was adequate. The audit included reviews of selected general controls, compliance with the Chief Financial Officers Act requirements, and the management control program as it related to the overall objective.

Results. Electronic Document Management access controls were not sufficient and could not provide reasonable assurance that data accumulated electronically and used by DFAS Columbus were secure. Specifically, DFAS security over Electronic Document Management needed improvement in password management, audit log configuration, Document Capture Center accountability, and convenience scanner control to adequately safeguard the security of electronically stored contractual data. Further, unless corrective actions are taken, data maintained in Electronic Document Management could be altered or misused without detection. These Electronic Document Management deficiencies identified in this audit were also identified in an August 1998 Electronic Document Management security test and evaluation performed by DFAS to accredit Electronic Document Management. However, the DFAS Electronic Document Management program office had the misconception that it did not need to correct all the identified findings after the DFAS Chief Information Officer granted accreditation to the program. Additionally, because of an administrative

oversight, the DFAS Chief Information Officer did not follow up on the reported findings to ensure that they were corrected. See the Finding section of the report for details on the audit results.

Summary of Recommendations. We recommend that the Director, DFAS, establish access controls that allow users to change passwords without any assistance, establish audit logs that can positively identify users and their actions, incorporate individual identification and authentication for operators of the high volume scanners within the Document Capture Center, and control access to the convenience scanners based on least privilege at DFAS Columbus. Additionally, we recommend that the Director, DFAS, conduct and document required security reviews as stated in the Electronic Document Management accreditation letter.

Management Comments. DFAS concurred with establishing access controls for users of Electronic Document Management that allow users to change passwords without any assistance. DFAS partially concurred with establishing audit log generation and maintenance into Electronic Document Management that can positively identify users and their actions. DFAS partially concurred with incorporating individual identification and authentication and an inactivity logout for operators of the high volume scanners within the Document Capture Center, stating that a contractor evaluation would identify the actions required to correct the problem. DFAS concurred with incorporating access controls to the Electronic Document Management convenience scanners based on least privilege, and an automatic inactivity user logout. DFAS concurred with conducting and documenting required reviews as stated in the Electronic Document Management accreditation letter. A discussion of management comments is in the Finding section of the report and the complete text is in the Management Comments section.

Audit Response. Management comments were generally responsive. However, the comments responding to the establishment of usernames and passwords and an inactivity logout feature on the high volume scanners were partially responsive. Since the contractor evaluation should have been completed, DFAS should state what corrective actions will be taken and when the actions will be accomplished. We request that the Director, DFAS, provide additional comments in response to the final report by June 16, 2001.

Table of Contents

Executive Summary	i
Introduction	
Background	1
Objectives	3
Finding	
Implementation of Security Safeguards Over Electronic Document Management	4
Appendixes	
A. Audit Process	
Scope	13
Methodology	14
Management Control Program Review	14
B. Prior Coverage	16
C. Report Distribution	17
Management Comments	
Defense Finance and Accounting Service, Chief Information Officer	19
Defense Finance and Accounting Service, Director, Contract Pay Services	21

Background

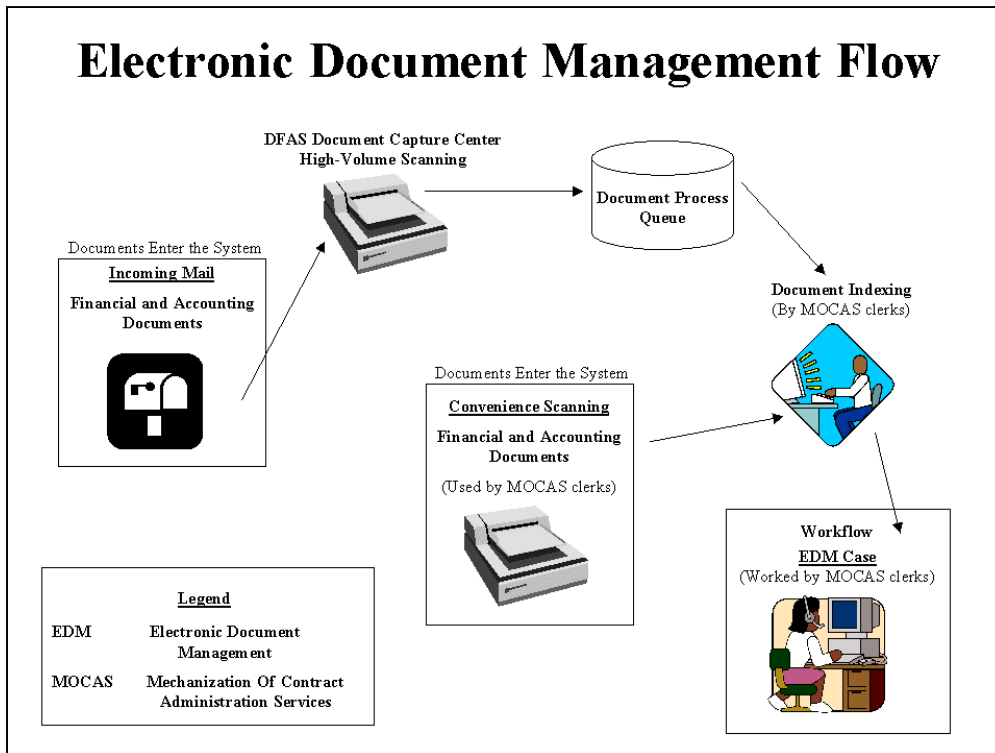
The Director, Defense Finance and Accounting Service (DFAS) Columbus, requested that we review Electronic Document Management (EDM) to determine whether sufficient safeguards are in place to ensure the security of electronically stored contractual data.

Paper-Free Contracting Initiative. On May 21, 1997, the Under Secretary of Defense (Comptroller) directed the move to a paper-free contracting process and stated the need to simplify and modernize the acquisition process in contract writing, administration, finance, and auditing.

Defense Finance and Accounting Service Columbus. To support the Paper-Free Contracting Initiative, DFAS began EDM at DFAS Columbus. DFAS contracted with Electronic Data Systems, Incorporated, to operate and maintain EDM. EDM was first implemented on a limited basis in June 1997 to reduce the amount of paper used and stored by DoD contracting personnel, reduce contract payment cycle time, improve efficiency, increase customer service, and comply with the DoD paper reduction initiative. DFAS plans to cancel EDM as a separate program and merge portions of it into the Defense Procurement Payment System (DPPS) before 2002. Accordingly, any deficiencies found in EDM that are incorporated into DPPS must be corrected before the transition to DPPS is undertaken.

Electronic Document Management. EDM digitizes paper documents received through the U.S. mail and offers online access to a large volume of financial and accounting documents, such as contracts, contract modifications, invoices, and receiving reports. The documents stored in EDM are protected under the Privacy Act and considered sensitive in nature. EDM was designed to allow the user to view, retrieve, move, and store official financial and accounting documents. Personnel at DFAS Columbus rely on the information accessed from EDM to make an average of 82,000 contract payments totaling \$6 billion each month (\$72 billion annually). As of August 2000, EDM stored approximately 4.6 million financial documents. EDM was fully implemented at DFAS Columbus for use with the Mechanization of Contract Administration Services (MOCAS) system in July 2000. MOCAS is a contract payment system used by DFAS in the administration and payment for hardware, supplies, and services.

EDM Process. The EDM system is an automated information system that consists of three subsystems: document capture, indexing, and workflow. The following figure illustrates the EDM process and flow of data.



Document Capture. The scanning for EDM is accomplished in the Document Capture Center at DFAS Columbus. The Document Capture Center receives paper documents such as contracts, contract modifications, invoices, and receiving reports through the U.S. mail, from DoD components and Government contractors. The Document Capture Center is secured with restricted access because the system servers are stored in that area. Document Capture Center clerks use high volume scanners to scan the documents into EDM. Document conversion software is used to convert the paper documents into digitized images. Once scanned and determined acceptable through quality assurance techniques, the images are forwarded into a document process queue for indexing by MOCAS clerks. The paper documents are stored for 90 days, then destroyed.

Indexing. The indexing process uniquely identifies each document within EDM. All MOCAS clerks who have access to EDM have the ability to index images into EDM. The MOCAS clerks review the image of the scanned document and manually enter the required index fields into EDM. Index fields

include such items as the contract number, invoice number, and receiving dates. After indexing, the image is electronically stored in a workflow folder for payment processing.

Workflow. EDM imaged documents are organized into workflow cases that require a specific task to be completed, such as the compilation of documents to prepare an invoice for payment. Images could also be stored for future use. Workflow allows for retrieval, viewing, and processing of documents within EDM by MOCAS clerks.

Convenience Scanners. DFAS Columbus installed convenience scanners within the three MOCAS payment divisions. The convenience scanners are located in an open area in each of the payment divisions and can be used by all MOCAS clerks. The convenience scanners are used to scan high priority documents so as to reduce the number of late payments by DFAS. When additional documents are needed to complete a transaction, the MOCAS clerk contacts the document originator and requests the document. High priority documents bypass the Document Capture Center and are directly received by the MOCAS clerk for processing through a convenience scanner. The MOCAS clerk indexes the image and completes the related tasks based on the type of document. The convenience scanners offer no limitation in the amount or the type of documents that the MOCAS clerks can input into EDM.

Objectives

The audit objective was to determine whether the security of Electronic Document Management at DFAS Columbus was adequate. The audit included reviews of selected general controls and compliance with the Chief Financial Officers Act requirements and the management control program as it related to the overall objective. Refer to Appendix A for discussion of the management control program.

Implementation of Security Safeguards Over Electronic Document Management

Access controls over EDM at DFAS Columbus were not sufficient to provide users with reasonable assurance that the electronic data maintained were accurate. Specifically, password management, audit log configuration, Document Capture Center accountability, and convenience scanner control needed improvement. DFAS first identified the EDM deficiencies in a 1998 security test and evaluation conducted to accredit the system; however, the EDM Program Manager did not correct the deficiencies. The DFAS Electronic Document Management program office had the misconception that they did not need to correct all the identified findings. Additionally, because of an administrative oversight, the DFAS Chief Information Officer did not conduct required reviews to determine whether the EDM Program Manager had corrected the deficiencies. As a result, data maintained in EDM may still be subject to undetected alteration or misuse.

Guidance for Securing EDM

DoD System Security Requirement. DoD Directive 5200.28, “Security Requirements for Automated Information Systems (AIS),” March 21, 1988, provides guidance on mandatory minimum automated information system security requirements. Specifically, the Directive requires that safeguards will be in place to ensure each person having access to an automated information system will be held accountable for his or her actions on that information system. The primary method for identifying users involves the individual user account and password to control access.

DoD System Certification and Accreditation Manual. DoD Manual 8510.1, “DoD Information Technology Security Certification and Accreditation Process (DITSCAP) Application Document,” July 31, 2000, (the accreditation process), establishes standards for certifying and accrediting the security of DoD systems throughout their life cycle. A certification is a comprehensive evaluation of the technical and nontechnical security features of an information technology system and other safeguards. The certification supports the accreditation process that determines whether a particular design and implementation meets a set of specified security requirements. The accreditation is a formal declaration by a designated approving authority that an information technology system is approved to operate in a particular security mode using a prescribed set of safeguards. Additionally, the designated approving authority assumes the overall responsibility for the security of the operation and ensures that all safeguards required in DoD Directive 5200.28 are implemented and maintained. The EDM security plan, August 7, 1998, stated that the DFAS Chief Information Officer is the designated approving authority.

DFAS System Security Guidance. DFAS Regulation 8000.1-R, “Information Management Corporate Policy,” May 21, 1999, describes DFAS information

security requirements and implementing instructions, including the requirement that all DFAS-owned automated information systems be certified and accredited in accordance with the “DFAS Certification and Accreditation Handbook,” March 6, 1998. The DFAS Handbook follows a similar process as that described in the DITSCAP. EDM was certified and accredited on August 7, 1998, using the DFAS Certification and Accreditation Handbook.

Access Controls for EDM

Access and physical controls at DFAS Columbus were not sufficient to provide reasonable assurance that the documents contained in EDM were accurate and could be relied on to set up payments within MOCAS. Access controls protect and control who can log on to a system; ensure that security mechanisms are in place to make decisions regarding access to resources; and, provide a capability to generate a reliable log of user actions. Physical security controls include steps to prevent tampering and intrusion. Specifically, EDM lacked the following controls.

- EDM users lacked the ability to independently change passwords.
- Audit logs were not properly configured to ensure security measures were working properly.
- The Document Capture Center lacked individual accountability for the scanning clerks.
- The convenience scanners lacked access controls based on least privilege¹ and physical security controls.

Password Management. Access to EDM is through password and username. Passwords are used to authenticate the user to ensure that only authorized personnel have access to EDM. However, password controls were not adequate because EDM users lacked the ability to change passwords without the assistance of the system administrator. According to National Computer Security Center Standard 002-85, “DoD Password Management Guide,” April 12, 1985, passwords should be changed on a periodic basis and users should be permitted to change their passwords without intervention by others to counter the possibility of undetected password compromise. In addition, users are to protect passwords from compromise and to avoid needless exposure of passwords. A password that has been compromised will allow an unauthorized user to have access to the system until passwords are changed and properly protected.

For EDM, the systems administrator generates the logon and passwords for the users and notifies the individuals of their new passwords. The system generated password is supplied by the EDM system administrator to the information system security officer, the terminal area security officer, and

¹ DoD Directive 5200.28 defines the concept of least privilege as that which grants users only enough access to the system(s) to complete their official duties.

finally to the user. Therefore, the passwords for EDM users have been exposed to others and are subject to compromise. DFAS should establish access controls for users of EDM that allow users to change passwords without any assistance.

Audit Log Configuration. Auditing logs are used to provide assurance that protection mechanisms are working as expected by capturing user actions. However, the EDM audit logs could not be relied on to capture user actions because the audit logs were not properly configured at DFAS Columbus. The National Computer Security Center Technical Guide 028, "Assessing Controlled Access Protection," May 25, 1992, states that the purpose of the audit log function for systems is to detect repeated attempts to bypass protection mechanisms, to monitor use of privileges, and to provide additional assurance that the protection mechanisms are working. The EDM audit logs were not capturing audit data because the audit function was not fully turned on. The EDM security test and evaluation stated that if the audit logs were fully turned on, the performance of EDM would be degraded.

Specifically, the audit log for the EDM system did not capture which user accessed the system; which files the user opened, deleted, or modified; what programs the user executed, and whether the user used or attempted to use files and programs to which the user was not granted access. Because the audit logs can not positively identify users and their actions, the audit logs are not effective in preventing or detecting potential abuse. DFAS should determine what safeguards can be put in place before EDM performance is degraded to the point where it is not cost-effective. In doing so, DFAS should establish EDM audit log generation and maintenance procedures that would positively identify users and their actions.

Document Capture Center Accountability. Access to the high-volume scanners in the Document Capture Center is through username and password. Passwords are used to authenticate the user to ensure that only authorized personnel have access to the high-volume scanners. However, DFAS allowed personnel in the Center to share the same username and password. DoD Directive 5200.28 states that individual accountability is required on all DoD information systems that hold sensitive information. Personnel in the Document Capture Center prepare documents for scanning and enter them into EDM. The Document Capture Center had 4 high-volume scanners and maintains a workforce of 34 people. Specific problems with the Document Capture Center are as follows.

- Each high-volume scanner had a single username and password for all 34 DFAS personnel that work within the Document Capture Center; therefore, the security controls could not tell which user performed specific transactions.

-
- For each workstation, the username and password had not been changed since EDM became operational on August 7, 1998. At times the passwords were posted on the workstations for training purposes; therefore, unauthorized personnel with access to the Document Capture Center could gain access to the high-volume scanners and enter transactions. DFAS personnel stated that passwords were changed in late November 2000 as a result of our audit.
 - Multiple incorrect sequential attempts to access the high-volume scanners could be made without the system locking the user out; therefore, unauthorized personnel could make repeated attempts to compromise passwords of the high volume scanners without being stopped.
 - During periods of inactivity there was no automatic system logoff; therefore, when a legitimate user leaves a workstation, unauthorized personnel would have access to the high-volume scanners and could enter documents.
 - The Document Capture Center had 34 authorized employees, but 200 additional people had key-cards that gave them access to the room; therefore, these 200 personnel could get access to the high-volume scanners and could enter transactions if other access controls were compromised.

Because of the ineffective access controls on the high-volume scanners, DFAS would not be able to affix individual accountability to any person for any inappropriate activity within the Document Capture Center. DFAS should incorporate individual identification and authentication and an inactivity logoff for operators of the high volume scanners.

Convenience Scanner Control. High priority contractual documents such as potential late payments can be entered into EDM by using the convenience scanners to accelerate the payment process. However, DFAS Columbus did not control access to the convenience scanners in order to limit who can enter documents into EDM. The convenience scanners lack access controls based on least privilege and physical security controls. According to DoD Directive 5200.28, access controls involve the input of user identification and passwords that are linked to predetermined access privileges and can be used to restrict access to specific system resources. Further, according to Federal Information Processing Standards Publication 31, "Guidelines for Automatic Data Processing Physical Security and Risk Management," June 1974, the lack of physical controls could result in the loss of data or program files. The following problems with controlling the convenience scanners were detected.

- Access to the convenience scanners was not based on least privilege, but was given to approximately 1,040 MOCAS clerks which allowed them to enter documents into EDM without any supervision to ensure that the documents were legitimate.

-
- The convenience scanners installed in DFAS Columbus had no physical controls to prevent unauthorized use by DFAS personnel.
 - During periods of inactivity there was no automatic system logoff; therefore, when a legitimate user left a workstation, unauthorized personnel could access the convenience scanners and could enter and index documents into EDM.

DFAS could not affix individual accountability for inappropriate use of the convenience scanners. Consequently, the lack of controls on convenience scanners would not permit DFAS to determine whether incorrect or improper modifications to contract data had been made. DFAS should incorporate access controls to the convenience scanners based on least privilege, physical controls to prevent unauthorized use, and an automatic inactivity user logout.

EDM Security Test and Evaluation

Access controls were not sufficient because the EDM program office did not correct deficiencies in password management, audit log configuration, Document Capture Center accountability, and convenience scanner control. DFAS first identified the EDM deficiencies in a 1998 security test and evaluation conducted to accredit EDM. The August 1998 EDM security test and evaluation report identified access control deficiencies in the same areas we identified in this audit and the August 1998 EDM risk assessment report identified possible solutions to the deficiencies that were reported in the security test and evaluation. However, the EDM Program Office did not correct all the deficiencies and had the misconception that it did not need to correct all the identified findings after the DFAS Chief Information Officer granted the accreditation. Additionally, because of an administrative oversight, the DFAS Chief Information Officer did not conduct the required reviews to determine whether the EDM Program Office had corrected the deficiencies.

According to the EDM accreditation letter, August 7, 1998, the program office was to fully implement all recommended countermeasures identified in the final risk assessment report. However, the program office did not implement all the necessary corrections to the access and physical controls that were identified. The accreditation letter also stated that the DFAS Chief Information Officer was to annually review the progress of the program office. However, the DFAS Chief Information Officer did not request any review to be performed in accordance with the accreditation letter. Our review of the EDM access controls confirmed that the same deficiencies still existed in password management, audit log configuration, Document Capture Center accountability, and convenience scanner control. This is the second time these EDM deficiencies have been identified, once in the EDM security test and evaluation, performed in May and June 1998, and again in this audit.

EDM Program Office Implementation of Security Corrections. Because the program office did not implement all the necessary corrections to the findings identified in the security test and evaluation completed on August 7, 1998, EDM

lacked assurance that misuse or unauthorized activities would be detected. The program office did not implement all the necessary corrections to the access controls because they believed that once the DFAS Chief Information Officer accredited EDM, it was not necessary to correct the findings in the security test and evaluation. The program office should correct the outstanding security test and evaluation findings in password management, audit logs, the Document Capture Center, and the convenience scanners.

DFAS Chief Information Officer Review of Security Corrections. In the August 7, 1998, EDM accreditation letter the DFAS Chief Information Officer stated that he would review the progress of the EDM program office to ensure that EDM deficiencies were corrected. However, because the DFAS Chief Information Officer did not review the progress of the EDM program office, the program office did not consider implementing all the identified countermeasures. DFAS Chief Information Officer personnel stated that it is their policy to conduct reviews to ensure that open security test and evaluation findings are closed. However, the EDM security reviews did not occur because of an administrative oversight. The DFAS Chief Information Officer should conduct and document required reviews as stated in the accreditation documentation.

Management Actions

Reaccreditation Efforts. EDM at DFAS Columbus was certified and accredited on August 7, 1998. This accreditation will expire on August 7, 2001. As of November 29, 2000, a DFAS Arlington² official indicated that reaccreditation efforts would be limited because the indexing and workflow subsystems of the EDM system may be incorporated into DPPS before 2002. Therefore, only the scanning portion of EDM would continue to be needed. DPPS is a DFAS initiative to consolidate DoD payment processes under one system. If DPPS incorporates the indexing and workflow portions of EDM, then reaccreditation efforts may not be necessary. However, components of EDM that will be incorporated into DPPS must have any deficiencies corrected to ensure that DPPS can be certified and accredited.

Efforts Taken by DFAS. DFAS is attempting to mitigate some of the password controls and convenience scanner weaknesses.

Password Improvements. Personnel at DFAS Arlington stated that they have implemented password controls on the local area network at DFAS Columbus. The password controls on the network include the requirement that all users use an eight-character password, with at least one number and one special character including upper and lower cases. Also, the passwords must be changed every 90 days. DFAS Arlington personnel stated that because users must log into the network before using EDM, the improved password controls on the network pass through to EDM.

² DFAS Arlington is the site of DFAS headquarters.

Although these changes are an improvement, they do not necessarily strengthen identification and authentication for the EDM user because specific logon and password controls for EDM have not changed. Because most personnel at DFAS Columbus have access to the local area network, it would still be possible for unauthorized personnel to gain EDM access even with the improvements to the network passwords. Without strong password controls, EDM remains vulnerable to unauthorized access and possible misuse or loss of system resources. Therefore, DFAS should develop access controls for users of EDM that allow users to change passwords without any assistance.

Convenience Scanner Modifications. DFAS Columbus has made improvements to limit access to the convenience scanners. At the time of our review, there were 14 convenience scanners installed within the 3 payment divisions at DFAS Columbus. Each convenience scanner is directly connected to a workstation that has the EDM application software loaded that any MOCAS clerk that had EDM access could use. However, the EDM project manager at DFAS Columbus implemented a separate scanning area for each of the three payment divisions. The new scanning areas are still in an open area, but with only 10 people in each division responsible for using the convenience scanners. The EDM project manager at DFAS Columbus has made a request to the systems administrator for the next system upgrade to include least privilege controls to be incorporated into the convenience scanner workstations, so that only authorized personnel have the ability to scan and index.

Although some policy improvements have been made regarding the use of the convenience scanners, workstations still remain in an open area without least privilege or physical controls to prevent unauthorized personnel from entering documents into the EDM system. DFAS should implement the proposed improvements in least privilege (as requested by the EDM project manager at DFAS Columbus) and incorporate physical controls into the convenience scanning area.

Summary

Access and physical controls for the EDM system at DFAS Columbus did not provide reasonable assurance that the documents contained in the system were adequately protected. As such, the EDM security weakness increased the risk for undetected alteration or misuse. Access controls over EDM were not sufficient to provide users of the system with reasonable assurance that electronic data used by DFAS Columbus were accurate.

Password controls were not adequate because EDM users lacked the ability to change passwords without the assistance of the system administrator; therefore, DFAS should establish access controls for users of EDM that allow users to change passwords without any assistance. The audit log feature for EDM was not fully turned on and could not positively identify users and their actions; therefore, DFAS should establish audit log generation and maintenance into EDM that can positively identify users and their actions. In the Document Capture Center, every high-volume scanner had a single username and password

for all personnel, multiple incorrect sequential attempts to logon could be made without the system locking the user out, and during periods of inactivity, the system did not automatically log the user out; therefore, DFAS should incorporate individual identification and authentication and an inactivity logout for operators of the high volume scanners. Access to the convenience scanners was based on access to EDM, not on least privilege, no physical controls existed to prevent unauthorized use, and during periods of inactivity the system did not automatically logout the user; therefore, DFAS should incorporate access controls into the convenience scanners based on least privilege, physical controls to prevent unauthorized use, and an automatic inactivity user logout.

DFAS Columbus should correct the outstanding security test and evaluation findings, which addresses the finding in this report. The DFAS Chief Information Office should conduct and document required reviews as stated in the accreditation documentation.

Recommendations, Management Comments, and Audit Response

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

1. Establish access controls for users of Electronic Document Management at the Defense Finance and Accounting Service Columbus that allow users to change passwords without any assistance.

DFAS Comments. DFAS concurred. DFAS will incorporate password change improvements when EDM Release 5.0 is deployed in July 2001. EDM Release 5.0 will provide users with the capability to change their password from the initially assigned generic password, and will require users to change passwords at least every 60 days.

2. Establish audit log generation and maintenance into Electronic Document Management at the Defense Finance and Accounting Service Columbus that can positively identify users and their actions.

DFAS Comments. DFAS partially concurred. DFAS stated audit tracking is very important to them, and they have taken actions to positively identify users. However, due to limitations in the EDM software, some users have inappropriate access and rights that can not be recorded by audit logs. DFAS will eliminate this limitation in a software release before December 31, 2001.

Audit Response. DFAS comments are responsive.

3. Incorporate individual identification and authentication and an inactivity logout for operators of the high volume scanners within the Document Capture Center at the Defense Finance and Accounting Service Columbus.

DFAS Comments. DFAS partially concurred. DFAS stated the software application controlling the high volume scanners was not designed to support individual identification and authentication or an inactivity logout feature. DFAS has asked the contractor to evaluate the establishment of an individual username and password as well as an inactivity logout feature. The contractor was to provide an estimate of the level of changes required by March 31, 2001. Until system improvements can be made, the users have been instructed to log off the scanners when not in use.

Audit Response. DFAS comments are partially responsive. Based on the anticipated completion of the contractor evaluation, DFAS needs to identify the specific corrective actions that will be taken and when the actions will be accomplished. We request that DFAS provide a completion date for the incorporation of individual identification and authentication and an inactivity logout for the operators of the high volume scanners in comments to the final report.

4. Incorporate access controls to the Electronic Document Management convenience scanners at the Defense Finance and Accounting Service Columbus based on least privilege, physical controls to prevent unauthorized use, and an automatic inactivity user logout.

DFAS Comments. DFAS concurred. DFAS stated they have developed initiatives to incorporate access controls for the EDM convenience scanners that include access only for designated users and the identification of those users. Identification of users will be incorporated in a future software release scheduled to occur before December 31, 2001. The automatic inactivity logout feature has been set at 2-3 hours; however, DFAS is reviewing this policy and will provide the contractor with a new inactivity logout setting. Additionally, DFAS has reduced the number of convenience scanners to three and incorporated procedural controls to control access to the convenience scanners.

5. Conduct and document required reviews as stated in the Electronic Document Management accreditation letter.

DFAS Comments. DFAS concurred. The DFAS Chief Information Officer stated they are improving processes and procedures to review system certification and accreditation status. The improvements include making modifications to the System Inventory Database to improve the process of capturing system accreditation status. The System Inventory Database is used to verify system accreditation status. Additionally, program managers and Information System Security Managers are required to update the System Inventory Database when system security changes occur. The improvement to the review process will be completed by October 2001.

Appendix A. Audit Process

Scope

Work Performed. We performed the audit at DFAS Arlington, Arlington, Virginia, and at DFAS Columbus, Columbus, Ohio, from August 2000 through January 2001. We reviewed how DFAS implemented access controls for EDM. We interviewed the DFAS Columbus EDM project manager and obtained a detailed understanding of EDM. We reviewed the security agreement, the security test and evaluation plan and results of the test, the certification and accreditation documentation, and the EDM Security Plan.

Limitations of Audit Scope. The audit was limited to the review of the general controls for the EDM system at DFAS Columbus. Based on our assessment of the general controls, we determined that a review of the application controls should not be conducted at this time. Previous reports on the Electronic Document Interchange and Electronic Document Access have been issued.

DoD-Wide Corporate-Level Government Performance and Results Act Goals. In response to the Government Performance and Results Act, the Secretary of Defense annually establishes DoD-wide corporate-level goals, subordinate performance goals, and performance measures. This report pertains to achievement of the following goal and subordinate performance goal:

- **FY 2001 DoD Corporate-Level Goal 2:** Prepare now for an uncertain future by pursuing a focused modernization effort that maintains U.S. qualitative superiority in key warfighting capabilities. Transform the force by exploiting the Revolution in Military Affairs, and reengineer the Department to achieve a 21st century infrastructure. **(01-DoD-2)**
- **FY 2001 Subordinate Performance Goal 2.5:** Improve DoD financial and information management. **(01-DoD-2.5)**

DoD Functional Area Reform Goals. Most major DoD functional areas have also established performance improvement reform objectives and goals. This report pertains to achievement of the following functional area objectives and goals:

- **Financial Management Area. Objective:** Strengthen internal controls. **Goal:** Improve compliance with the Federal Managers Financial Integrity Act. **(FM-5.3)**

-
- **Information Technology Management Area. Objective:** Ensure that DoD vital information resources are secure and protected. **Goal:** Assess information assurance posture of DoD operational systems. (ITM-4.4)

General Accounting Office High-Risk Area. The General Accounting Office has identified several high-risk areas in the Department of Defense. This report provides coverage of the Information Management and Technology and the Defense Financial Management high-risk areas.

Methodology

Use of Computer-Processed Data. We did not use computer-processed data to perform this audit.

Use of Technical Assistance. We did not use technical assistance to perform this audit.

Audit Type, Dates, and Standards. We performed this financial-related audit from August 2000 through January 2001 according to auditing standards issued by the Comptroller General of the United States, as implemented by the Inspector General, DoD. We used the General Accounting Office Federal Information Systems Control Audit Manual and the DoD Information Technology Security Certification and Accreditation Process as guides for conducting this general control review.

Contacts During the Audit. We visited or contacted individuals and organizations within DoD. Further details are available on request.

Management Control Program Review

DoD Directive 5010.38, "Management Control (MC) Program," August 26, 1996, and DoD Instruction 5010.40, "Management Control (MC) Program Procedures," August 28, 1996, require 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 the Review of the Management Control Program. We reviewed the adequacy of management controls in place for EDM. Specifically, we reviewed the implementation of DoD policies and procedures governing EDM. We reviewed management's self-evaluation applicable to those management controls.

Adequacy of Management Controls. We identified material management control weaknesses as defined by DoD Instruction 5010.40. Management controls were not adequate to ensure the accuracy of electronic transactions using EDM. All recommendations in this report, if implemented, will provide

the necessary controls for ensuring the accuracy of the electronic transactions. A copy of this report will be provided to the senior official responsible for management controls in the office of the Assistant Secretary of Defense (Command, Control, Communications and Intelligence); DFAS Arlington; and DFAS Columbus.

Adequacy of Management's Self-Evaluation. DFAS Columbus officials did not identify EDM as an assessable unit and, therefore, did not identify or report the material management control weaknesses identified by the audit. Also, had DFAS management been aware of the results of the EDM security test and evaluation and implemented corrective actions, a management control weakness could have been avoided.

Appendix B. Prior Coverage

General Accounting Office

GAO Report No. GAO/AIMD 99-107 (OSD Case No. 1835), “Information Security: Serious Weaknesses Continue to Place Defense Operations at Risk,” August 26, 1999

GAO Report No. GAO/AIMD 98-92 (no OSD case number was issued), “Information Security – Serious Weaknesses Place Critical Federal Operations and Assets at Risk,” September 23, 1998

Inspector General, DoD

Inspector General, DoD, Report No. D-2001-095, “General Controls Over the Electronic Data Interchange,” April 6, 2001

Inspector General, DoD, Report No. D-2001-029, “General Controls Over the Electronic Document Access System,” December 27, 2000

Inspector General, DoD, Report No. 98-057, “Defense Finance and Accounting Service Acquisition Program for the Electronic Document Management Program,” January 27, 1998

Inspector General, DoD, Report No. 98-013, “Second User Acceptance Test of the Electronic Document Management System at the Defense Finance and Accounting Service Operating Location Omaha, Nebraska,” October 24, 1997

Inspector General, DoD, Report No. 97-050, “Evaluation of Controls Over Workflow Applications Selected for Electronic Document Management,” December 17, 1996

Inspector General, DoD, Report No. 96-214, “Computer Security for the Federal Acquisition Computer Network,” August 22, 1996

Appendix C. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense (Comptroller)
Deputy Chief Financial Officer
Deputy Comptroller (Program/Budget)
Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)

Department of the Army

Auditor General, Department of the Army

Department of the Navy

Naval Inspector General
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

Defense Organizations

Director, Defense Finance and Accounting Service
Director, Defense Finance and Accounting Service Columbus

Non-Defense Federal Organizations and Individuals

Office of Management and Budget

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Governmental Affairs
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Committee on Government Reform
House Subcommittee on Government Efficiency, Financial Management, and Intergovernmental Relations, Committee on Government Reform
House Subcommittee on National Security, Veterans Affairs, and International Relations, Committee on Government Reform
House Subcommittee on Technology and Procurement Policy, Committee on Government Reform

Defense Finance and Accounting Service, Chief Information Officer Comments



DEFENSE FINANCE AND ACCOUNTING SERVICE

1931 JEFFERSON DAVIS HIGHWAY
ARLINGTON, VA 22240-5291
WWW.DFAS.MIL



DFAS-DT

APR 4 2001

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

SUBJECT: Audit Report on Controls Over Electronic Document Management
(Project No. D2000 FG-0057.02) (Formerly Project No. OFG-5106) dated
January 22, 2001

The Defense Finance and Accounting Service (DFAS) response regarding the audit report, Controls over Electronic Document Management, dated January 22, 2001, is attached. The response addresses the Chief Information Officer (CIO) response to Recommendation 5.

My point of contact for this action is Kim Ponder, DFAS-DTC (703) 607-3838.

Audrey Y. Davis
Director, Information and Technology

Attachment:
As Stated

**DFAS Chief Information Officer Comments on
Recommendation 5 to DOD IG Audit Report
(Project No. D2000FG-0057.02)
(Formerly Project No. 0FG-5106)**

Recommendation 5: Conduct and document required reviews as stated in the Electronic Document Management accreditation letter.

CIO Comments: Concur. DFAS-HQ is currently working on establishing processes and procedures to review system certification and accreditation status. For example, modifications are being made to the System Inventory Database (SID) to improve the process of capturing system accreditation status. The estimated completion date is October 2001, with a possibility of being completed before that date. The SID is an inventory of all DoD financial, accounting and DFAS administrative automated information systems. We use the SID to verify system accreditation status. Moreover, program/system managers and Information System Security Managers are required to update the SID with system changes. In accordance with DoDD 5200.28, dated March 21, 1988, DFAS will conduct periodic reviews of accredited systems safeguards.

Attachment

Defense Finance and Accounting Service, Director, Contract Pay Services Comments



**DEFENSE FINANCE AND ACCOUNTING SERVICE
COLUMBUS CENTER**
P.O. BOX 182317
COLUMBUS, OHIO 43218-2317

IN REPLY
REFER TO DFAS-BKF/CC

MAR 16 2001

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

SUBJECT: Management Response to DoD IG Audit Report on the Controls Over EDM (Project
No. D2000FG-005), dated January 22, 2001.

In response to your memorandum dated January 22, 2001, subject as above, comments
are provided for Recommendations 1 through 5 (see attachment).

If you have any questions, please contact Ms. Paula Denlinger, DFAS-BKFPC/CC, at
DSN 869-7372 or (614) 693-7372.

A handwritten signature in cursive script that reads "JoAnn Boutelle".

JoAnn Boutelle
Director, Contract Pay Services

Attachment
As stated

Audit Report on Controls Over Electronic Document Management
(Project No. D2000FG-0057.02) (Formerly Project No. 0FG-5106)

The EDM system is one facet of the overall payment process. The system must also interface with many automated systems prior to completion of the payment process and is subject to many systemic and procedural checks and balances to ensure payments are accurate and timely. All physical and logical access controls have been reviewed by the DFAS CIO and found to provide reasonable assurance that documents in the system were adequately protected. In cases where access could not be restricted due to system architecture or commercial off the shelf software (COTS), reasonable procedures and processes along with scheduled system technical refresh have or will be implemented. Further, DFAS management continually reviews the business suite of systems to determine optimal efficiencies. DFAS is evaluating the future use of EDM to complement the Defense Procurement Pay System (DPPS) and DFAS Corporate Database (DCD) prior to any decisions about EDM.

The following are the individual replies to the IG recommendations:

Recommendation 1.: Establish access controls for users of Electronic Document Management at the Defense Finance and Accounting Service Columbus that allows users to change passwords without any assistance.

Management Comments: Concur. Currently, the EDM system utilizes the Eastman Open Workflow Package with the Pace database as its engine. Due to the limitation of this product, EDM users are unable to reset or change their passwords. This is a known software limitation. The EDM Program Office recognized this limitation and has scheduled replacement of the Eastman software with an Oracle Workflow product which does not have this limitation in our Technical Refresh Release 5.0 scheduled for July 2001. The deployment of 5.0 Tech Refresh for EDM will incorporate an access control, specifically a password change feature, which will provide users with the capability to change or 'individualize' their password. The EDM helpdesk will continue to be the POC for resetting passwords. The user will be initially assigned a generic password but will have the capability to change it daily or as desired. In addition, the system will be set to require user's to change their passwords every 60 days.

Estimated Completion Date: The anticipated deployment date for EDM Release 5.0 is July 2001 for the MOCAS North Directorate. Following the successful deployment within the MOCAS North Directorate, the release will be installed within MOCAS South and West Directorates. The EDM Program office is responsible for monitoring implementation.

Recommendation 2. : Establish audit log generation and maintenance into Electronic Document Management at the Defense Finance and Accounting Service Columbus that can positively identify users and their actions.

Audit Report on Controls Over Electronic Document Management
(Project No. D2000FG-0057.02) (Formerly Project No. 0FG-5106)

Management Comments: Partially concur. While DFAS has not activated the Unix audit log feature, it would not provide the level of detail needed to track cases and/or maintain an adequate audit trail due to the use of the Eastman Workflow product scheduled for replacement in July 2001. As audit tracking is very important to DFAS, we have maximized the available audit controls of the Eastman Workflow product. We are using the EDM Case Task History of the workflow product, which positively identifies users and their actions. The actions recorded include the following: Task Name, Task Status, Task Role, Participant, Task Category, Created (date/time) and Started (date/time). The problem identified by the auditors occurs when "read-only" users are provided EDM "input" capability. When users have this type of access, they can update indexes or start cases when they should only have the capability to 'view' cases. An enhancement (CCR313) has been initiated which when developed will restrict access to 'read-only' for users strictly viewing cases and can only be accomplished after technical refresh of the Eastman Open Workflow COTS product.

Estimated Completion Date: This change is scheduled for programming after the implementation of EDM Release 5.0 in July of 2001. The current planned date for completion is December 31, 2001. The EDM Program Office is responsible for monitoring deployment.

Recommendation 3: Incorporate individual identification and authentication and an inactivity logout for operators of the high volume scanners within the Document Capture Center at the Defense Finance and Accounting Service Columbus.

Management Comments: Partially Concur. The Production Scan Monitor application that controls the Kodak high-volume scanners is designed to use a single, generic User ID that is known only to the scanner operators. Using a different ID would require a redesign of the EDM document capture subsystem. The identity of the scanner operator is not maintained within the EDM system, however, the identity of the scanner itself (called a station ID) is maintained for each document that is scanned, in addition to the scanner's station ID along with other information (endorsed) on each page scanned. To improve controls, we have asked the contractor to evaluate establishment of an individual user ID and password control feature as well as a timeout feature for the high volume scanners. In addition, EDM users have been instructed to logoff the high volume scanners when not in use. Also, no input can be made to the high volume scanners without the proper batch header sheets and access to the scanner for which the DCC control access. Note: Access to the overall area is limited to those with a need to enter and approved by the local Security Office

Estimated Completion Date: EDS is expected to provide an estimate of the level of change required for an individual user ID by March 31, 2001. Other procedural controls have been put in place March 9, 2001.

Audit Report on Controls Over Electronic Document Management
(Project No. D2000FG-0057.02) (Formerly Project No. OFG-5106)

Recommendation 4: Incorporate access controls to the Electronic Document Management convenience scanners at the Defense Finance and Accounting Service Columbus based on least privilege, physical controls to prevent unauthorized use, and an automatic inactivity user logout.

Management Comments: Concur. We acknowledge this control weakness; however, we have initiatives in process to incorporate access controls into the EDM convenience scanners at the Defense Finance and Accounting Service Columbus. These initiatives are geared towards restricting access to the EDM Convenience scanners to designated users only, and identifying EDM Convenience scanner users. In addition, DFAS Columbus has reduced the number of Convenience scanners from 8 to 3. Also, as a part of regular business practice, users are logging off following the completion of their scanning responsibilities.

In addition, there is an automatic inactivity user logout function within the EDM convenience scanners; however, it had been set for 2-3 hours to accommodate the production environment and to prevent user disruption during the scanning process. We are in the process of evaluating the settings for passive logouts.

Estimated Completion Date: DFAS Columbus will provide the recommended logout timeframe to the contractor NLT March 23, 2001. In addition, the identification of user input to the scanning operation will be added in a future release scheduled for completion December 31, 2001.

Recommendation 5: Conduct and document required reviews as stated in the Electronic Document Management accreditation letter.

Management Comments: Concur. According to the EDM accreditation letter, reviews need to be done when significant changes occur which affect system security. To date, baseline elements used to grant system security accreditation for EDM have not been changed but will differ after implementation of the Technical Refresh in July 2001.

Estimated Completion Date: The EDM Program Office will schedule an updated review of all security related issues to ensure material weaknesses in the current and refreshed software are identified and scheduled for correction after the rollout of the technical refresh planned for July 2001.

Audit Team Members

The Finance and Accounting Directorate, Office of the Assistant Inspector General for Auditing, DoD prepared this report. Personnel of the Office of the Inspector General, DoD, who contributed to the report are listed below.

F. Jay Lane
Salvatore D. Guli
Kimberley A. Caprio
Eric L. Lewis
Jacqueline J. Vos
Yolanda C. Watts
Troy R. Zigler
Stephen G. Wynne