Audit Report

DISTRIBUTION STATEMENT A
Approved for Public Release
Distribution Unlimited

GENERAL CONTROLS OVER THE
ELECTRONIC DOCUMENT ACCESS SYSTEM

Report No. D-2001-029 December 27, 2000

Office of the Inspector General
Department of Defense

Additional Information and Copies

To obtain additional copies of this audit report, visit the Inspector General, DoD, Home Page at www.dodig.osd.mil or contact the Secondary Reports 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

ASD(C^3I)	Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
DEBX	Defense Electronic Business Exchange
DECC	Defense Enterprise Computer Center
DFAS	Defense Finance and Accounting Service
DISA	Defense Information Systems Agency
DITSCAP	DoD Information Technology Security Certification and Accreditation Process
EDA	Electronic Document Access
JECPO	Joint Electronic Commerce Program Office
MOCAS	Mechanization of Contract Administrative Services
MOU	Memorandum of Understanding
NIPRNET	Non-secure Internet Protocol Routing Network

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

December 27, 2000

MEMORANDUM FOR ASSISTANT SECRETARY OF DEFENSE (COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE)
DIRECTOR, DEFENSE FINANCE AND ACCOUNTING SERVICE
DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY

SUBJECT: Audit Report on General Controls Over the Electronic Document Access System (Report No. D-2001-029)

We are providing this report for your review and comment. We considered management comments on a draft of this report when preparing the final report.

The comments of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence; the Joint Electronic Commerce Program Office; and the Defense Finance and Accounting Service conformed to the requirements of DoD Directive 7650.3; however, additional comments are needed on Recommendations 1., 2.a., and 2.b. The comments should include expected completion dates for the corrective actions. Therefore, we request additional details in comments to the final report by February 27, 2001.

We appreciate the courtesies extended to the audit staff. Questions on the audit should be directed to 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.

Robert J. Lieberman
Assistant Inspector General
for Auditing

Office of the Inspector General, DoD

Report No. D-2001-029 **December 27, 2000**
(Project No. D2000FG-0057)

General Controls Over the Electronic Document Access System

Executive Summary

Introduction. The Joint Electronic Commerce Program Office (JECPO) initiated the Electronic Document Access (EDA) system as part of the DoD Paper-Free Contracting Initiative. EDA contributes to the initiative by digitizing paper documents and offering web-based read-only access to official contracting, finance and accounting documents. Personnel at the Defense Finance and Accounting Service (DFAS) Columbus rely on the EDA system to make more than 82,000 contract payments each month. The Director, DFAS Columbus, requested that we review the EDA system to determine whether sufficient safeguards are in place to ensure the security of electronically transmitted contractual data.

Objectives. The audit objective was to determine whether the security of the EDA system 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. The report discusses DFAS implementation of the EDA system as it applies to DFAS Columbus.

Results. The EDA system security controls were not sufficient and could not provide reasonable assurance that EDA data transmitted electronically and used by DFAS Columbus were secure. JECPO implementation of EDA and DFAS security for EDA needed improvement. Unless corrective actions are taken, EDA data could be altered or misused. See Appendix A for details on the management control program as it relates to controls over the EDA system.

Summary of Recommendations. We recommend that the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) (ASD(C^3I)) revise the Electronic Business/Electronic Commerce Strategic Plan to address security responsibilities and requirements. We recommend that the Director, JECPO, in coordination with DFAS and the Defense Information Systems Agency, develop the System Security Authorization Agreement to provide end-to-end security for EDA; incorporate all relevant elements as outlined in the DoD Information Technology Security Certification and Accreditation Process manual; develop and execute the EDA system test and evaluation to include all EDA users; and, incorporate security requirements and review guides within the Memorandums of Understanding with EDA document providers and users. We recommend that the DFAS Chief Information Officer complete the security training curriculum for information security managers. We recommend the Director, DFAS Columbus, require the information security

manager to document and execute a plan to implement and enforce all applicable security policies and safeguards over the Columbus systems; to develop access profiles for all personnel having access to EDA and DFAS Columbus systems; and, assess and provide the resources and training the information security manager needs to perform information security functions.

Management Comments. ASD(C^3I) concurred with revising the Electronic Business/Electronic Commerce Strategic Plan to address specific security responsibilities and requirements. JECPO concurred with developing the System Security Authorization Agreement for EDA in coordination with DFAS and DISA; developing and executing the EDA security test and evaluation; and, incorporating security requirements within Memorandums of Understanding and review guidelines with EDA document providers. DFAS concurred with the need for security training for information security managers; that the information security manager document and execute a plan for implementing security policies and safeguards; that the information security manager attend training on information security topics; and, that the Director, DFAS Columbus redirect or request additional resources for the information security manager. DFAS nonconcurred with developing EDA access profiles for users, stating that EDA access is read only. DFAS also nonconcurred with the existence of a management control weakness regarding the alteration and accuracy of EDA documents and the need for signatures on contracting documents. See the Finding section of the report for details on the management comments and the management comments section for the complete text of management comments.

Audit Response. Comments from ASD(C^3I) were responsive; however, they did not specify when a revision to the Electronic Business/Electronic Commerce Strategic Plan would be accomplished. We request that ASD(C^3I) provide the date in comments on the final report. Comments from JECPO were responsive on incorporating security requirements and review guidelines within the Memorandums of Understanding. JECPO comments on the development of the System Security Authorization Agreement are responsive. However, the comments did not provide a date when the agreement may be finalized, so we request that JECPO provide a completion date for the finalized agreement. JECPO comments on the development and execution of the EDA system test and evaluation are responsive. However, the comments stated that an EDA system test and evaluation was completed in September 2000 and that final recommendations would be reviewed and appropriate corrective actions would be implemented. The comments did not specify when those corrective actions would occur. We request that JECPO identify when they will be implemented. Comments from DFAS regarding completion of a security training curriculum in accordance with the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) June 29, 1998, memorandum on Information Assurance training are responsive. Although DFAS nonconcurred regarding the need for access profiles, the decision to review each person's system accesses meets with the intent of the recommendation. DFAS also nonconcurred that a material management control weakness existed. We believe that the nature of the issues identified clearly warrants reporting a material weakness.

Table of Contents

Background

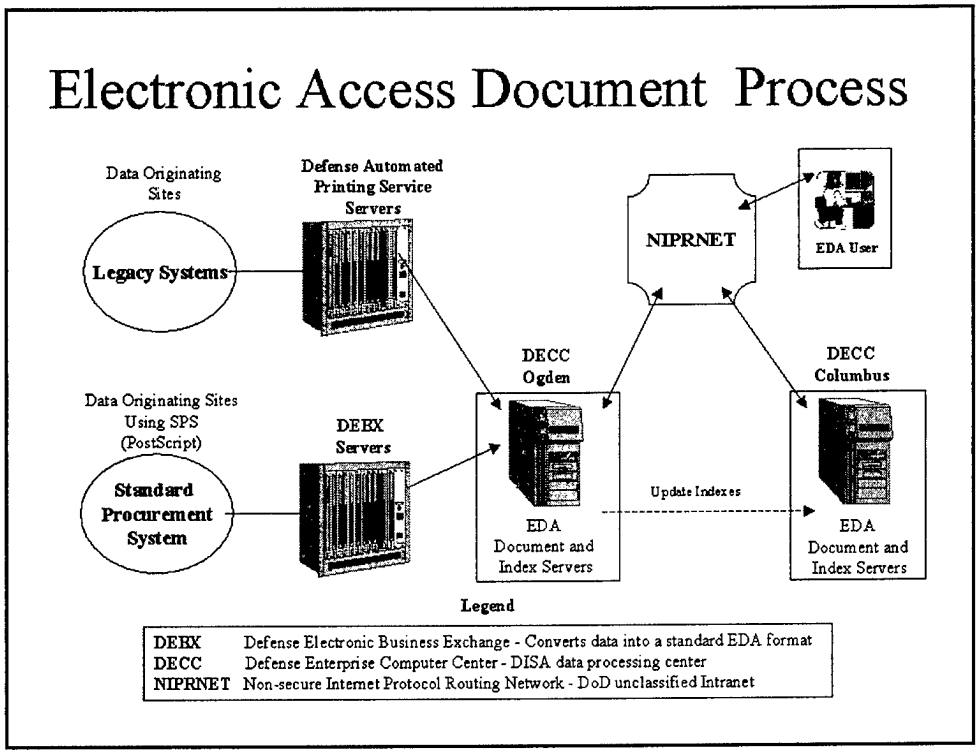
During their audit of the FY 1999 Air Force financial statements, the Air Force Audit Agency requested more than 11,000 paper documents from DFAS Columbus to support sampled electronic transactions. Subsequent to the Air Force audit, the Director, DFAS Columbus, requested that we review the Electronic Document Access (EDA) system to determine whether sufficient safeguards are in place to ensure the security of electronically transmitted contractual data and reduce hard copy verification requirements.

Paper-Free Contracting Initiative. On May 21, 1997, the Under Secretary of Defense (Comptroller) directed the implementation of a paper-free contracting process and stated the need to simplify and modernize the acquisition process in contract writing, administration, finance, and auditing. However, the Under Secretary's direction did not address security.

Joint Electronic Commerce Program Office. To support the Paper-Free Contracting Initiative, the Deputy Secretary of Defense, under Defense Reform Initiative Directive 43, "Defense-wide Electronic Commerce," May 20, 1998, directed the establishment of the Joint Electronic Commerce Program Office (JECPO) as an entity under the policy direction of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, (ASD(C^3I)), to integrate electronic commerce in the full DoD business cycle. On November 24, 1998, JECPO was chartered to implement electronic commerce within DoD. However, the charter did not address electronic commerce security.

Electronic Document Access. JECPO initiated EDA as part of the DoD Paper-Free Contracting Initiative to reduce the amount of paper used and stored by DoD contracting personnel, to reduce the contract payment cycle time, and to facilitate the sharing of information among DoD personnel. EDA contributes to the initiative by digitizing paper documents and offering web-based read-only access to official contracts and modifications, vouchers, Government bills of lading, and accounting and finance documents.

EDA System Process. The following figure illustrates the EDA process and flow of data within EDA.



Documents are entered into the EDA system from DoD contracting organizations. Currently, there are nine contracting organizations (data originating sites) that generate information for use in EDA. The contract documents are generated using the Standard Procurement System or legacy contract writing systems. For those organizations using the Standard Procurement System, PostScript printing software is used to send the data directly through the Defense Electronic Business Exchange (DEBX) for conversion into portable document format to the Defense Enterprise Computer Center (the computer center) at Ogden, Utah. For legacy systems, document files are sent to the Defense Automated Printing Service for conversion into portable document format. Once converted into portable document format, all of the file indexes generated by the Defense Automated Printing Service are sent to the computer center at Ogden for storage and queries from users. The computer center at Ogden maintains the file indexes for the Standard Procurement System files and Defense Automated Printing Service converted files. The computer center at Ogden transmits an updated index listing of the portable document format files every 2 hours to the computer center at Columbus, Ohio, for use by DFAS Columbus payment personnel.

EDA users include personnel from the data originating sites, such as procurement contracting officers, administrative contracting officers, DFAS payment personnel, and systems administrators. To access EDA, a DoD user network must have a connection through the Non-secure Internet Protocol Routing Network (NIPRNET), which is a DoD unclassified data

communications network. Local terminal area security officers are the liaison between the users and the computer center at Ogden and are responsible for requesting logons for DFAS employees with approval from their supervisor. The computer center personnel at Ogden assign and maintain the logons in the EDA system. Once a logon is assigned, the user may query either the computer center at Ogden or the computer center at Columbus EDA servers for EDA documents. The queried EDA server then displays a portable document format image of the electronically generated document to the user.

Objectives

The audit objective was to determine whether the security of the Electronic Document Access 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 and Appendix B for prior coverage.

Implementation of Security Safeguards Within the Electronic Document Access System

Security controls over the EDA system were not sufficient to provide users with reasonable assurance that data transmitted electronically and used by DFAS Columbus were accurate. This lack of sufficient security controls for EDA occurred because:

- security responsibilities are not defined;
- an end-to-end assessment of security has not been completed,
- DFAS security and training requirements are not defined, and
- DFAS Columbus security staff lacked adequate resources.

As a result, risk existed that data maintained in EDA could be altered or misused. Further, auditors would remain unable to rely on EDA system controls, so verification of the transactions would remain labor intensive and administratively burdensome.

Guidance and Responsibility for Securing EDA

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 heads of DoD Components shall ensure that periodic independent reviews of the security and protection of their automated information system are accomplished to ensure compliance with stated security goals.

DoD System Certification and Accreditation Manual. DoD Manual 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP) Application Document," December 1999, (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 non-technical security features of an information technology system and other safeguards. The certification supports the accreditation process that determines whether a particular design and implementation meet 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. Before a system can be certified and accredited, the accreditation process requires the completion of a System Security Authorization Agreement (security agreement) and the system test and evaluation.

System Security Authorization Agreement. The security agreement is a formal binding agreement between the organizations responsible for operating and securing the system. The agreement is between the designated approving authority, the certification authority, information technology system representatives, and the program manager. For EDA, these are the DFAS Chief Information Officer, the Defense Information Systems Agency (DISA), and JECPO, respectively. The security agreement specifies the level of security required when the system development begins or when changes to a system are made. The security agreement is designed to fulfill the requirements for a security plan and to meet all the needs for certification and accreditation support documentation. The security agreement includes such items as the system mission, threats to the system, target environment, target architecture, security requirements, and applicable data access policies, and resources. Using the security agreement, the decision approving authority determines the accreditation based on the security safeguards, risk, corrective actions, and compliance with the security agreement.

System Test and Evaluation. The objective of the system test and evaluation is to evaluate implementation of system security to ensure that automated security features affecting confidentiality, integrity, and availability have been implemented according to the security agreement, are performing properly, and provide the required security features. The performance of a system test and evaluation may be a joint effort between the users, systems administration, and program management. In the case of EDA, the system test and evaluation may include DFAS, DISA, and JECPO. The results of the system test and evaluation are included in the security agreement.

DISA Security Readiness Reviews. DISA Field Security Operations personnel perform security readiness reviews on DISA facilities to identify security and infrastructure deficiencies and to generate reports on the discrepancies. According to the "Security Readiness Review Process Guide," July 30, 1999, organizations should be made aware of the results of the security readiness review process and vulnerability assessment scans conducted at their site because they represent the major part of their certification and accreditation security posture. Since certification tasks include a review and analysis of all prior security readiness review results to determine the security posture of the site and its information systems or technology, it is in the best interest of the site to correct identified security vulnerabilities as quickly as possible.

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 the same process and procedures as those described in the DITSCAP.

EDA Security Responsibilities. The Under Secretary of Defense (Comptroller) issued "Business Rules for Electronic Document Access," as a working draft on June 24, 1999, and stated that they were effective immediately. According to

the business rules, EDA security is the responsibility of all organizations involved in the process including JECPO, DFAS, DISA, the users, and data originating sites. Participation by all parties is critical to ensure that security is planned and managed as an end-to-end process. We commend the Director, DFAS Columbus, for acknowledging a potential security weakness and requesting Inspector General, DoD, assistance for an in-depth look at EDA security.

Security of EDA

Reliance on EDA. DFAS Columbus personnel rely on the information accessed from EDA to make more than 82,000 contract payments each month, and contracting officials throughout DoD rely on EDA data to monitor contracts, contract modifications, Government bills of lading, and vouchers. In addition, to provide opinions on DoD annual financial statements compiled by DFAS, auditors must assess the reliability of information contained in EDA. If they are unable to rely on the information contained in EDA, they must significantly increase their sample size to test the integrity of the financial information at DFAS Columbus. For example, the Air Force Audit Agency required DFAS to produce 11,000 documents to verify the reliability of electronic data. Therefore, the data maintained within EDA must be accurate and secure to preclude unauthorized access and manipulation of data.

Adequacy of Security Efforts of EDA Data Used by DFAS Columbus. As users and participants in the EDA process, DFAS, JECPO, and DISA, as well as the originators of EDA data, have a responsibility to ensure the accuracy and reliability of the information, and thus the security controls over EDA input, access, and use. As such, they need to demonstrate reasonable assurance that EDA data are accurate to users, and that security controls are in place and periodically tested to provide an acceptable level of assurance.

Our review of EDA controls at DFAS Columbus, revealed that the controls were not sufficient to provide reasonable assurance that data transmitted using EDA were accurate. We identified examples of access control weaknesses and other security vulnerabilities that reduced system reliability. In addition, the Air Force Audit Agency identified weaknesses during the audit of the Air Force FY 1999 financial statements that precluded their reliance on the security of EDA data.

Access Control Issues. At DFAS Columbus, the information security manager is responsible for implementing all security measures, and each division is assigned a terminal area security officer who is responsible for requesting access for EDA from the Ogden computer center. The terminal area security officer reports to the information security manager at DFAS Columbus.

The information security manager at DFAS Columbus has not implemented the concept of least privilege for access to EDA.[1] An access control list based on least privilege can limit the damage that may result if the concept of least privilege is ignored. An access control list specifies for each named system or file, a list of named individuals with their respective level of access to that system or file.

The terminal area security officer within each division at DFAS Columbus maintains a list of personnel who have access to EDA. The list, however, is not based upon least privilege, security levels, or type of position held at DFAS Columbus. Rather, access to EDA was granted based on a supervisor's determination that an employee needed access regardless of whether the individual had access to other systems that could be incompatible. The supervisors at DFAS Columbus have not been provided the criteria they needed to properly determine the level of access to EDA. Although the information security manager is responsible for implementing security controls, the Director, DFAS Columbus is responsible for providing the access criteria.

We identified one DFAS Columbus employee who had sufficient access to manipulate data and erase the audit trail because of access to EDA, the Electronic Document Management System, the Electronic Data Interchange system,[2] and the Mechanization of Contract Administration Services (MOCAS). This employee could change the Master Address File within the MOCAS system which allows access to change contractor and government entity codes and addresses, incorporate invoices, and have payments made by changing significant parts of contracts within the MOCAS system. Coupled with access to EDA, this person could access contracts, copy them, change relevant data, and incorporate that data into the MOCAS system so that payments could be made directly to that individual. We discussed this scenario with DFAS Columbus management who agreed that access profiles are necessary to determine whether other employees could have this capability. The information security manager was unaware of the employee's access levels. DFAS Arlington officials maintain that the same risk exists with paper contracts received through the mail system; however, safeguards must be in place to ensure that EDA does not make it easier to alter or misuse data.

Although DFAS Columbus is working on establishing access control lists based on least privilege, they could not tell us whether there were other personnel who had the same type of access or state whether that type of access occurred only once. At present, the information security manager can not quantify the potential security risk.

---

[1] DoD Directive 5200.28 defines the concept of least privilege as that of each user is granted the most restrictive set of privileges needed for the performance of their position.

[2] DFAS Columbus Site personnel are investigating the extent of this employee's access to the Electronic Data Interchange system because DFAS personnel should only have view access.

Security Vulnerabilities. The information security manager at DFAS Columbus was not aware of any security readiness reviews conducted on the EDA servers at the Columbus computer center. A security readiness review assesses the operating system and computer for vulnerabilities that would allow an intruder to perform malicious acts and destroy the audit trail. As part of its responsibility to oversee security of DoD systems, DISA periodically conducts security readiness reviews of systems to determine the reliability of the system and its data. In June 1999, DISA performed a security readiness review on the EDA servers at the Columbus computer center and reported 34 findings. Although the Columbus computer center has resolved the findings, the information security manager was unaware that the security readiness review was completed or that findings had existed. The information security manager should coordinate with DISA personnel to evaluate the security readiness reviews on the EDA servers and the subsequent results because the findings may impact the security of the system.

Air Force Audit Agency Validation of EDA Data. In performing audit work in support of the Air Force FY 1999 financial statements, the Air Force Audit Agency had to assess the accuracy of EDA and other data that support the financial statements. At DFAS Columbus, they were unable to rely on the EDA data, and therefore had to do more work to validate amounts identified in EDA documents. The Air Force Audit Agency expended an additional 1.3 man-years of resources to validate the transactions; however, DFAS estimated that they used an additional 10 to 12 man-years to satisfy the Air Force Audit Agency request. According to the Air Force Audit Agency, about 30 percent of the EDA contracts reviewed did not contain signatures, which also resulted in additional work for Air Force Audit Agency and DFAS personnel.

The Director, DFAS Columbus, stated that DFAS does not know why there were no signatures on some of documents received. Further, the Director stated that DFAS assumes the documents entered into EDA are valid and accurate.

The Air Force Audit Agency contacted contracting officers to substantiate the documents maintained in EDA. Although all the EDA contracts proved to be valid, the Air Force Audit Agency stated that since the contracts are web-accessed, possible fraud could be generated by either a contracting officer or other personnel with access to the EDA and other DFAS systems. Currently, procurement and administrative contracting officers are inputting contracting documents into EDA. The Air Force Audit Agency stated that an individual with contracting officer access privileges could submit a contract without signatures and obtain a payment. Also, the Air Force Audit Agency stated that DFAS Columbus personnel use EDA contracting documents to enter data into the MOCAS system to make automatic payments without human intervention. Because of concerns on the validity of the EDA data and its reliability, the Air Force Audit Agency needed to substantiate the data with the signed and dated copies maintained at the contracting offices, consequently using more resources and reducing the benefits of EDA.

EDA Security Responsibilities

EDA security was insufficient because security responsibilities were not well defined, an end-to-end assessment of security was not accomplished, security training was inadequate, and the DFAS Columbus security staff lacked adequate resources.

Security Definition. JECPO and DFAS did not clearly define EDA security. According to JECPO officials, their focus has been on implementing electronic commerce initiatives according to the Deputy Secretary of Defense mandate to move toward paperless contracting by January 2000. Therefore, security was not a priority while EDA was being implemented. JECPO officials stated that security over EDA transactions should not be any greater than the same transactions using paper documentation; however, no documented assessment of the risks of digitizing contractual documents was available. JECPO and DFAS officials also concluded that DISA was responsible for implementing security for EDA because EDA ran on DISA computers. However, DISA officials stated that they had no authority to mandate security controls for organizations outside direct DISA control and that they would only implement security that is specifically requested by the user site. Therefore, JECPO and DFAS did not adequately assume responsibility for EDA security requirements and a comprehensive security plan was not developed and finalized. For example, the DoD Electronic Document Access Security Plan, working draft, dated July 15, 1996, does not address how security would be implemented for each of the principals: JECPO, DFAS, DISA, and the document authors. The plan was not finalized although JECPO estimates there are 15,000 EDA users. The lack of EDA security can be partially attributed to the lack of security in the ASD(C^3I) Electronic Business/Electronic Commerce Strategic Plan. Although the strategic plan provides a blueprint for DoD electronic business, the ASD(C^3I) needs to revise the plan to include security requirements to provide guidance for JECPO, which reports to the ASD(C^3I).

End-to-End Assessment of EDA Security. DFAS Arlington had taken steps to partially address EDA end-to-end security by initiating Memorandums of Understanding in October 1997 with EDA data originating sites. The agreements with DFAS and the data originating sites describe the terms in which the document provider would no longer supply paper copies of contracting documents to DFAS Columbus. However, DFAS does not review the Memorandums of Understanding once they are established because DFAS does not have the authority to mandate end-to-end security requirements for electronic business.

The Memorandum of Understanding states that it is the responsibility of the data originating sites to ensure the validity of the documents entered into EDA. Further, the Memorandum of Understanding indicates that in order to implement EDA and turn off the use of paper between the requesting organization and DFAS, documents released to EDA must be approved,

authentic and legal, readable, and identical to the signed paper copy. The Memorandum of Understanding is silent on signature requirements, and DFAS assumes that the data originating sites would not enter invalid contracts into EDA.

JECPO, through the ASD(C^3I), has the authority to implement end-to-end security requirements for EDA. Therefore, JECPO, rather than DFAS,[3] should incorporate security requirements in the Memorandum of Understanding, and also establish the review requirements for the EDA data originating sites and users. In addition, to ensure the security of the system from the data originating sites through the Defense Electronic Business Exchange or the Defense Automated Printing Service to the users of EDA data, an assessment of EDA security should be made to address the end-to-end process. Such an end-to-end assessment would be consistent with the accreditation process and should include the System Security Authorization Agreement and the System Test and Evaluation.

System Security Authorization Agreement. The accreditation process establishes a standard, integrated approach to protecting and securing a system. The DITSCAP describes the security agreement as the vehicle that defines the implementation of information technology security requirements. A security agreement describes the system from definition through system test and evaluation, risk assessments, system rules of behavior, contingency planning, accreditation documentation and accreditation statements, and security responsibilities. Thus, a security agreement should provide a comprehensive end-to-end assessment of EDA.

Because the system is implemented by JECPO, used by DFAS and contracting offices, and operated by DISA, it is essential that a security agreement be developed to coordinate EDA security requirements among these organizations. Although the designation of responsibilities for security over EDA is undefined, JECPO, as the DoD-wide integrator of electronic commerce initiatives, should initiate the development of the security agreement for the EDA system. The development of the security agreement should include coordination with the DFAS and DISA to incorporate all relevant elements as outlined in the DITSCAP accreditation process manual. The security agreement should be developed which specifies security responsibilities for JECPO, DFAS, DISA, and the data originating sites.

EDA system certification and accreditation can not be achieved without the development of the security agreement. However, the DFAS Chief Information Officer issued an Interim Approval to Operate on October 22, 1999, through October 23, 2000, based on a verbal presentation. The DFAS Chief Information Officer extended the Interim Approval to Operate on

[3] As part of the System Security Authorization Agreement with DFAS and other EDA users, JECPO may delegate authority to DFAS or other activities to oversee enforcement of the Memorandum of Understanding depending upon resource constraints. However, JECPO must determine that the Memorandum addresses EDA data security.

October 24, 2000, for 180 days so that JECPO could have time to finalize Memorandums of Understanding with interfacing systems and finalize the draft System Security Authorization Agreement.

According to the DITSCAP, an interim approval to operate is a temporary approval that may be issued for no more than a one-year period after the security agreement and system test and evaluation are developed and tested. The DFAS Chief Information Officer granted the approval of the EDA interim approval to operate acknowledging that EDA security needs improvement, but the benefits of operating the system outweigh the risks. Although the DFAS Chief Information Officer provided the approval to operate, JECPO has the responsibility for integrating electronic commerce in DoD. As such, JECPO should develop the security agreement for EDA in coordination with DFAS and DISA to incorporate all relevant elements as described in the DITSCAP, prior to expiration of the 180 days extension, when the extended interim authority to operate expires. The development of the security agreement is essential for ensuring that security requirements are addressed and that joint responsibility for security is delegated as appropriate.

System Test and Evaluation. According to the DITSCAP, once a security agreement has been established, a system test and evaluation should be performed prior to certification to assess the security infrastructure and to determine whether security features have been implemented according to the security agreement. Specifically, the system test and evaluation validates identification and authentication, audit trail capabilities within the system, and the rules that define how the network connection is implemented. According to the DITSCAP, the system test and evaluation should include test procedures on technical hardware and software security requirements to test the correct implementation of the security policy. Also, security functional testing must evaluate the system to determine whether installation procedures were correctly implemented.

The lack of an evaluation may result in the improper integration and operation of all security features affecting confidentiality, integrity, and availability of the system. Although the responsibility for EDA security is not clear, JECPO as the DoD organization responsible for electronic commerce implementation should initiate planning for testing and evaluating the EDA system.

The system test and evaluation process should document the procedures necessary to measure security at DISA, DFAS, and data origination sites because neither DFAS nor DISA has the authority to enforce security outside their own agencies. The system test and evaluation should determine whether security controls are working as intended and that all parties are following the controls described in the security agreement.

DFAS Training and Security Requirements. DFAS Columbus is a user of EDA and must ensure the adequacy of EDA security. Information security

training is essential to meeting the security requirements within any organization because of the rapid movement into the electronic commerce arena. Information system security managers and security staff are the focal point in any organization for information system security.

Security Training. The Director, DFAS Columbus, had not ensured that the information security manager received the necessary security training. According to DFAS Regulation 8000.1-R, the DFAS Directors supervise security personnel and manage DFAS security policy for systems under their control and within the sites. The information security manager is an essential element to the overall security at DFAS Columbus. However, the information security manager stated that training on information management, security controls, physical and access controls had not been received. The only training for the information security manager included attendance at security conferences with no in-depth detailed training on information management and security controls. The Director, DFAS Columbus, should require the information security manager to attend training on information management and information security controls, planning and administration of the security program, access control, network security measures, electronic commerce security issues, and physical protection of the computing facilities.

DFAS Chief Information Officer Information Assurance Training. On June 29, 1998, the ASD(C^3I) requested that the Under Secretary of Defense for Personnel and Readiness identify a common set of information assurance training and certification requirements for military and civilian occupation specialties. The memorandum directs that DoD Components shall demonstrate full compliance through the development and implementation of certification plans and procedures for all DoD employees who use DoD computer systems or perform the duties of system administrators and maintainers. In Inspector General, DoD, Report No. 99-107, "Computer Security for the Defense Civilian Pay System," March 16, 1999, we recommended that DFAS revise DFAS Regulation 8000.1-R to outline specific training requirements for each security position commensurate with assigned functional responsibilities. DFAS concurred with the recommendation.

The DFAS Chief Information Officer had not developed the training curriculum for security officers (information security manager, information system security officers, and terminal area security officers) as required by the ASD(C^3I). The DFAS Chief Information Officer acknowledged that they are revising the training requirements that were due out in August 2000, including requirements for each type of security officer. Because of increased reliance on automation and the need for proper controls and access, it is critical for those responsible for security to be knowledgeable of the systems security requirements and potential vulnerabilities. Once trained, these personnel should be better able to identify and oversee security requirements for DFAS Columbus systems and processes. The DFAS Chief Information Officer needs to complete the development of a training curriculum to qualify information security managers for their positions.

DFAS Columbus Security Efforts for EDA. In addition to not having available a training curriculum, DFAS Columbus also lacked sufficient staff to adequately perform the security functions described in DFAS Regulation 8000.1-R or to review the DFAS Columbus information systems, including EDA.

Security Resources. The Director, DFAS Columbus, did not ensure that the information security manager had the personnel resources to enforce applicable security policies. The information security manager was formally assigned in February 2000 after serving as an alternate since 1998. The information security manager and an alternate are responsible for all information security at DFAS Columbus. However, the alternate does not actively participate in specific system security because of responsibilities with the DFAS Columbus network. Each system at DFAS Columbus was to have an information system security officer to help address security concerns for particular systems. According to the DFAS Columbus information security manager, the information system security officers have not been appointed. The information security manager must have the resources to protect DFAS Columbus information systems. The Director, DFAS Columbus, should also assess and provide the resources the information security manager needs to perform the functions outlined in DFAS Regulation 8000.1-R.

Security Reviews. According to DFAS, because of limited staff, the information security manager had not developed an overall plan to review systems, to review security readiness review results, or coordinate remedies with DISA. For the same reason, the information security manager had been unable to conduct periodic independent reviews of system adequacy. For EDA and other systems, the information security manager had not developed access control lists (profiles) to preclude employees from having access greater than needed. As a result, employees that changed jobs may have retained access privileges to systems they no longer needed access to. This could result in an employee gaining sufficient access to potentially commit fraud or to perform malicious acts without detection.

To improve security at DFAS, the Director, DFAS Columbus, needs to require the information security manager to document and execute a plan to implement and enforce all applicable security policies and safeguards. The information security manager should also develop access profiles for all personnel having access to the EDA and other DFAS Columbus systems.

Summary

The general controls for the EDA system at DFAS Columbus did not provide reasonable assurance that the system was adequately protected. As such, the EDA security weaknesses allowed the risk of undetected fraud or misuse. The lack of a security agreement or a system test and evaluation increases the risk of data inaccuracy and that implemented security may not be operating as intended. JECPO oversight needs to be expanded to include the development of the

security agreement for the EDA system and the conduct of a system test and evaluation to reduce risk. An EDA system test and evaluation should be developed and testing accomplished to provide assurance that the EDA system is protected and operating as intended.

There was not a reasonable basis to rely upon DFAS Columbus controls to prevent fraud or misuse because the lack of resources and training for the information security manager position. Also, the lack of knowledge by the information security manager of system vulnerabilities increases the risk of intrusion.

Additionally, DFAS estimated that 10 to 12 man-years were necessary to gather the documentation needed by the Air Force Audit Agency for reviewing electronic transactions to support their FY 1999 financial statement audits. Because of the limited reliability of DFAS Columbus security for their electronic transactions, the Air Force Audit Agency required DFAS Columbus to provide more than 11,000 paper documents to support the sampled electronic transactions, which eliminated the EDA benefits of reducing the reliance on paper. Until controls are improved, auditors may need to continue to request paper copies for electronic transactions being audited.

Efforts Taken by JECPO, DFAS and DISA. JECPO, DFAS, and DISA have initiated some security measures for EDA use at DFAS Columbus.

JECPO Efforts. As of October 2000, JECPO acknowledged responsibility for end-to-end security of EDA and has initiated actions to address such. Specifically, JECPO with the support of DFAS, is developing the security agreement and the system test and evaluation and is updating EDA documentation as necessary. Based on comments from a draft of this report, JECPO stated that a system test and evaluation was conducted the week of September 11, 2000, at the Defense Enterprise Computing Center at Ogden, Utah, and Columbus, Ohio. Final report recommendations from the system test and evaluation will be reviewed and appropriate corrective actions will be implemented. In addition, JECPO is in the process of developing and coordinating Memorandums of Agreement with each of the EDA user organizations.

DFAS Efforts. DFAS acknowledged the need to work with JECPO and DISA to improve EDA security. DFAS also acknowledged the need to improve security at DFAS Columbus to provide training to its security personnel. In addition, DFAS has initiated Memorandums of Understanding to establish a working agreement between DFAS and the data originating sites to authorize their use of EDA and to permit their discontinuing submission of paper documents to DFAS Columbus. In the Memorandums of Understanding, DFAS states that the users must comply with DFAS EDA business rules. The business rules require that internal controls at the contract writing organization are sufficient to ensure that only valid, awarded contracts are placed on EDA, no pen and ink changes are made to the contracts once they are converted to EDA, and the procurement office retains the official signed contract. Further, the

Memorandums of Understanding place responsibility for ensuring the accuracy and validity of documents in EDA on the providers of the contract information.

DISA Efforts. In addition, as a good first step, DISA computer centers in Columbus and Ogden have implemented secure locations by installing Enforcer software for the EDA document servers for intrusion detection, and all EDA connections to the computer centers are through a firewall. DISA Field Security Operations personnel recommended the intrusion detection software.

Recommendations, Management Comments, and Audit Response

1. We recommend that the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence revise the Electronic Business/Electronic Commerce Strategic Plan to address specific security responsibilities and requirements.

ASD(C^3I) Comments. The ASD(C^3I) concurred.

Audit Response. Comments from the ASD(C^3I) are responsive. We request that the ASD(C^3I) specify when the revision to the Electronic Business/ Electronic Commerce Strategic Plan will be accomplished in comments on the final report.

2. We recommend that the Director, Joint Electronic Commerce Program Office:

a. Develop the System Security Authorization Agreement to provide end-to-end security for the Electronic Document Access system in coordination with the Defense Finance and Accounting Service and the Defense Information Systems Agency to incorporate all relevant elements as outlined in the DoD Information Technology Security Certification and Accreditation Process manual before October 22, 2000.

JECPO Comments. Comments from JECPO were included in comments from DISA. JECPO concurred and has prepared a draft System Security Authorization Agreement that was completed and delivered to DFAS and DISA on September 7, 2000, for coordination. JECPO is in the process of finalizing the agreement.

Audit Response. JECPO comments are responsive. We request that JECPO provide a completion date for the finalized agreement in comments to the final report.

b. Develop and execute the Electronic Document Access system test and evaluation to include all Electronic Document Access system users, the Defense Finance and Accounting Service, and the Defense Information Systems Agency.

JECPO Comments. JECPO concurred and stated that an EDA security test and evaluation was completed in September 2000 at DECC Ogden and DECC Columbus using the draft System Security Authorization Agreement, September 7, 2000, and DITSCAP guidance. JECPO comments also stated that final recommendations would be reviewed and appropriate corrective actions would be implemented.

Audit Response. The JECPO comments are responsive. We request that JECPO provide a completion date for when the review would be performed and corrective actions would be implemented in comments to the final report.

c. Incorporate security requirements and review guidelines within the Memorandums of Understanding with Electronic Document Access document providers and users.

JECPO Comments. JECPO concurred and is in the process of drafting and coordinating the memorandums with each of the feeder and interfacing systems with EDA. JECPO anticipates the revised Memorandums of Understanding to be signed during first quarter FY 2001. Also, the signed Memorandums of Understanding will be made a part of the System Security Authorization Agreement, system test and evaluation, and EDA security documentation package.

3. We recommend that the Chief Information Officer, Defense Finance and Accounting Service, complete a security training curriculum for the information security manager, the information system security officer, and the terminal area security officer in accordance with the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, June 29, 1998, memorandum on Information Assurance training.

DFAS Comments. DFAS concurred and stated that training is being provided agency-wide including security personnel at DFAS Columbus and will be completed by March 2001.

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

a. Require the information security manager to document and execute a plan to implement and enforce all applicable security policies and safeguards over the systems located at the Defense Finance and Accounting Service Columbus.

DFAS Comments. DFAS concurred and stated that the Information Security Manager has prepared a draft of the Information Security Plan that outlines goals, objectives, specific actions, roles, and responsibilities of DFAS information security managers. The final version of the Information Security Plan is expected to be completed by December 31, 2000, with implementation in January 2001.

b. Develop access profiles for all personnel having access to the Electronic Document Access.

DFAS Comments. DFAS nonconcurred and stated that Contract Pay Services personnel do not have the capability to alter or change EDA documents, but can only browse and print documents. DFAS maintains that the contract writing organizations control the content of converted EDA documents. In addition, DFAS stated that the Terminal Area Security Officers maintain access to systems on a spreadsheet for each person and are reviewed to ensure that there are no internal control violations. Further, DFAS Columbus stated that they will request a listing of all contract pay services personnel that have access to EDA for comparison with existing MOCAS access tables and profiles. The comparison will ascertain whether there are inconsistencies between the functional requirements of the personnel and their granted access. The DFAS comments indicate that if inconsistencies are found, corrective action will be taken to restrict the query access to only the EDA documents needed to accomplish assigned duties.

Audit Response. DFAS comments are responsive. Although DFAS nonconcurred with the recommendation, the development of a listing to compare existing MOCAS tables and profiles with access to EDA meets the intent of the recommendation.

c. Require the information security manager to attend training on information management and information security controls, planning and administration of the security program, access control, network security measures, electronic commerce security issues, and physical protection of the computing facilities.

DFAS Comments. DFAS concurred and stated that the Information Security Manager has attended over 450 hours in formal training. DFAS agreed that a course curriculum specifically geared to information security management is desired and the expected completion date for the information security training is March 2001.

d. Assess the resource needs of the information security manager and redirect or request additional resources, as necessary, to perform the functions described in the Defense Finance and Accounting Service Regulation 8000.1-R, "Information Management Corporate Policy," May 21, 1999.

DFAS Comments. DFAS concurred and stated that the Information Security Manager is part of the establishment of the Technical Services Organization that will be completed in June 2001.

Appendix A. Audit Process

Scope

Work Performed. Personnel at DFAS Columbus rely on the information accessed from EDA to make more than 82,000 contract payments each month. We performed the audit at DFAS Arlington, DFAS Columbus, and the Joint Electronic Commerce Program Office from December 1999 through July 2000. We reviewed how DFAS implemented controls for an entity-wide security program and access controls for the EDA system. We interviewed the DFAS Columbus information security manager, the DFAS Columbus terminal area security officers, and the DISA security representatives at the Columbus and Ogden Defense Enterprise Computer Centers to determine how they implemented security over EDA. We also performed a walkthrough of the EDA process as it relates to the Mechanization of Contract Administration Services and the Standard Automated Materiel Management System. We reviewed the security readiness reviews performed by DISA Field Security Operations on the Columbus computer center EDA operating software. The reviews identified weaknesses and planned corrective actions for operating software that supports EDA.

Limitations to Audit Scope. The audit was limited to the review of the general controls for the EDA 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. Subsequent reports on the Electronic Document Interchange and Electronic Document Management systems will be 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. Currently, DoD has not established a corporate-level goal for information assurance, although the General Accounting Office lists it as a high-risk area. This report pertains to achievement of the following goal, subordinate performance goal, and performance measures:

- **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.

- **FY 2001 Subordinate Performance Goal 2.5:** Improve DoD financial and information management. **(01-Dod-2.5)**

- **FY 2001 Performance Measure 2.5.1:** Reduce the number of noncompliant accounting and finance systems. **(01-DoD-2.5.1)**

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 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 area.

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 December 1999 through July 2000 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 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 EDA. Specifically, we reviewed the implementation of DoD policies and procedures governing EDA. 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 EDA. 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 ASD(C^3I); DFAS Arlington; and DFAS Columbus.

Adequacy of Management's Self-Evaluation. DFAS Columbus officials did not identify EDA as an assessable unit and, therefore, did not identify or report the material management control weaknesses identified by the audit.

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

Inspector General, DoD, Report No. 99-107, "Computer Security for the Defense Civilian Pay System," March 16, 1999

Inspector General, DoD, Report No. 99-103, "DoD Efforts to Implement Year 2000 Compliance for Electronic Data Interchange," March 5, 1999
Inspector General, DoD, Report No. 96-214, "Computer Security for the Federal Acquisition Computer Network," August 22, 1996

Air Force

Air Force Audit Agency, Project No. DW000005, "Accounting for Selected Assets and Liabilities (Fund Balance with Treasury), Fiscal Year 1998 Air Force Consolidated Financial Statements, Defense Finance and Accounting Service - Columbus Center, Columbus OH," December 8, 1999

Air Force Audit Agency, Project No. DW000003, "Accounting for Revenues and Other Financing Sources (Disbursements), Fiscal Year 1998 Air Force Consolidated Financial Statements, Defense Finance and Accounting Service - Columbus Center, Columbus OH," November 22, 1999

Air Force Audit Agency, Project No. 97064011, "Electronic Data Interchange Procurement Transactions," December 24, 1998

Appendix C. Report Distribution

Office of the Secretary of Defense

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

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 Contract Management Agency
Director, Defense Finance and Accounting Service
  Director, Defense Finance and Accounting Service Columbus
Director, Defense Information Systems Agency
Director, Defense Logistics Agency

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 Management, Information, and Technology, Committee on Government Reform
House Subcommittee on National Security, Veterans Affairs, and International Relations, Committee on Government Reform

Assistant Secretary of Defense for Command, Control, Communications, and Intelligence Comments

COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000
October 24, 2000

MEMORANDUM FOR INSPECTOR GENERAL, DoD
(Attn: DIRECTOR, FINANCE AND ACCOUNTING)

SUBJECT: Audit Report on General Controls Over the Electronic Document Access System (Project No. D2000FG-0057)

My office reviewed the subject report. I concur with the recommendation to revise the Electronic Business/Electronic Commerce Strategic Plan to address specific security responsibilities and requirements. We are in the process of updating the subject plan to ensure proper oversite of current regulatory implementation.

for Paul R. Brubaker
Deputy Assistant Secretary of Defense
(Deputy CIO)

Defense Information Systems Agency Comments

DEFENSE INFORMATION SYSTEMS AGENCY
701 S. COURTHOUSE ROAD
ARLINGTON, VIRGINIA 22204-2199

IN REPLY REFER TO: Inspector General (IG)

23 October 2000

MEMORANDUM FOR INSPECTOR GENERAL, DEPARTMENT OF DEFENSE
(ATTN: FINANCE AND ACCOUNTING DIRECTORATE)

SUBJECT: Response to DoD IG Draft Report, General Controls Over the Electronic Document Access System (Project D2000FG-0057, formerly Project 0FG-5106)

1. The Joint Electronic Commerce Program Office was requested to provide comments to recommendations 2.a, 2.b. and 2c of the subject report. These are included as Enclosure 1. In addition the DISA Field Security Office is providing general comments on the portion of the report applicable to the three EDAS servers located within the Defense Enterprise Computing Center (DECC) Columbus environment. These comments are at Enclosure 2.

2. If you have any questions, please ~~call~~ Jason Bakker, at (703) 607-6607.

RICHARD T. RACE
Inspector General

Enclosures a/s

Quality Information for a Strong Defense

B. Develop and execute the Electronic Document Access system test and evaluation to include all Electronic Document Access system users, the Defense Finance and Accounting Service, and the Defense Information Systems Agency.

Comments: Director, JECPO concurs with the recommendation to develop and execute the EDA ST&E. An EDA ST&E was conducted the week of 11 Sep 00 at DECC Ogden and Columbus in accordance with the guidelines described in the EDA SSAA and in accordance with Defense Information Technology Security Certification & Accreditation Process (DITSCAP) requirements. Final report recommendations from the ST&E will be reviewed and appropriate corrective action(s) will be implemented. The ST&E findings along with corrective actions to be taken will be briefed to the Delegated Approving Authority (DAA) requesting an Authorization to Operate (ATO) for the EDA system be given.

C. Incorporate security requirements and review guidelines within the Memorandums of Understanding with Electronic Document Access document providers and users.

Comment: Director, JECPO concurs with the recommendation to incorporate security requirements and review guidelines within the MOUs with EDA document providers and users. The JECPO is in the process of drafting and coordinating Memorandums of Agreement (MOAs) with each of the feeder/interfacing systems to EDA. It is anticipated that these MOAs will be signed 1st Qtr FY01. Copies of these signed MOAs will be then made a part of the SSAA, ST&E, and EDA Security documentation package.

Subject: DODIG Draft Audit Report of EDA Suspense: 18 Oct 00

Action Requested: DISA IG Office requests that the JECPO is specifically requested to respond to recommendations 2.a., 2.b., and 2.c located on pages 14 & 15 of report.

- comments should indicate concurrence or nonconcurrence.
- comments should describe actions taken or planned in response to agreed upon recommendations and provide the completion dates of the actions.
- State specific reasons for any nonconcurrence and propose alternative actions, if appropriate.

Page 14, Recommendations:

2. We recommend that the Director, Joint Electronic Commerce Program Office:

   A. Develop the System Security Authorization Agreement to provide end-to-end security for Electronic Document Access system in coordination with the Defense Finance and Accounting Service and the Defense Information Systems Agency to incorporate all relevant elements as outlined in the DoD Information Technology Security Certification and Accreditation Process manual before October 22, 2000.

      Comment: Director, JECPO concurs with the recommendation to develop the SSAA for the EDA system in coordination with DFAS & DISA, and concurs that a review of the end-to-end security requirements of DoD EDA must be accomplished and in coordination with the affected Agencies and Program Offices. JECPO also believes it is the responsibility of each Agency or System Program Office, with an interface to DoD EDA, to implement appropriate security within their areas of control. The JECPO must rely on the integrity of the security evaluation for each interface system and the authority of the applicable DAA to address security issues outside the direct control of this Program Office. The JECPO will conduct a security review of that part of the EDA system within its organizational control, which includes the Defense Enterprise Computer Center at Ogden and at Columbus. The JECPO has prepared a draft SSAA and this was completed and delivered to DFAS & DISA for review and coordination. (Completion Date: 7 Sep 00). The JECPO is in the process of finalizing the SSAA as a result of the System Test & Evaluation, (Estimated Completion Date: 18 Oct 00). The JECPO is also in the process of developing and coordinating Memorandums of Agreement (MOAs) with each of the user organizations of the EDA system along with those EDA feeder/interfacing systems (Defense Automation & Production Service (DAPS), Defense Contract Management Agency (DCMA), Navy and Air Force Interface (NAFI), and Defense Finance & Accounting Service (DFAS).

SUMMARY SHEET

SUSPENSE DATE: 12 October 2000

	TO	ACTION	TYPED NAME	INIT	DATE		TO	ACTION	TYPED NAME	INIT	DATE
1.	WE62	CONCUR	Mr. Haskakis			11.					
2.	D3312	CONCUR	Mr. Harrison			12.					
3.	D331	CONCUR	Mr. Hughes			13.					
4.	D33	Approve	COL Huffman			14.					
5.						15.					
6.						16.					
7.						17.					
8.						18.					
9.						19.					
10.						20.					

ACTION OFFICER	OPR CODE	PHONE NUMBER	SIGNATURE	DATE
Mr. Mike Lee	D3312	(717) 267-9879	/S/	12 Oct 00

SUBJECT DoD IG Draft Report, Audit Report on General Controls Over the Electronic Document Access System (EDAS) (Project No. D2000FG-0057) (formerly Project No. 0FG-5106)

SUMMARY

1. BACKGROUND:

a. The above Draft Report has been provided to HQ DISA, CIO, DISA D2; Joint Electronic Commerce Program Office (JECPO) and to the Director, Defense Finance and Accounting Service (DFAS) as they are the named respondents in the Draft Report. FSO is providing comments as to that portion of the report applicable to the 3 EDAS servers located within the Defense Enterprise Computing Center (DECC) Columbus environment.

b. The only paragraph in the report which mentions DISA Field Security Operations and DECC Columbus is noted in the Guidance and Responsibility for Securing EDA, found on page 5 of the Draft Report. The paragraph is titled, DISA Security Readiness Reviews, wherein it explains the SRR Process Guide and "that Organizations should be made aware of the results of the SRR and vulnerability assessment scans conducted at their site because they comprise a major part of the certification and accreditation security posture." This has been accomplished for EDAS as witnessed by the auditors statement where they cited "In June 1999 DISA performed a security Readiness Review on the EDAS servers at the Columbus computer center (DECC Columbus) and reported 34 findings. Although the Columbus computer center has resolved the findings the information security manager (DFAS Columbus Center ISSM) was unaware that the security readiness review was completed or that the findings had existed." We cannot explain why the DFAS Columbus ISSM was unaware of the findings on the EDAS platform as it is our standard practice to involve the DFAS (SAs and IS staff) in the SRR resolution process. The DECC Columbus IS staff has and will continue to coordinate with the DFAS Columbus Center IS staff on SRRs and closing the findings identified therein.

SUMMARY SHEET *(Continuation)*

SUBJECT DoD IG Draft Report, Audit Report on General Controls Over the Electronic Document Access System (EDAS) (Project No. D2000FG-0057) (formerly Project No. 0FG-5106)

SUMMARY

RECOMMENDATION: Recommend that the Commander, GNOSC, D33 concur with comment as to the DFAS Columbus ISSM being unaware of the EDAS findings, stating; Field Security Operations and the DECC Columbus staff will continue to include the DFAS IS staff in SRR Resolution Meetings and stress their need to keep DFAS Columbus ISSM advised as to the SRR status.

Defense Finance and Accounting Service Comments

DEFENSE FINANCE AND ACCOUNTING SERVICE
1931 JEFFERSON DAVIS HIGHWAY
ARLINGTON, VA 22240-5291
WWW.DFAS.MIL

NOV 15 2000

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

SUBJECT: Audit Report on General Controls Over the Electronic Document Access System (Project No. D2000FG-0057)

The Electronic Document Access (EDA) system is one of DoD's leading crosscutting paperless initiatives. We requested this audit as means to validate DOD's evolving technologies and provide valuable insight for improvement the end-to-end EDA process.

DFAS' comments are provided per the attachment. Specific actions have been identified for those recommendations contained in the report for which DFAS has operational control.

Harry S. Hinton
Acting Director for Finance

Attachment
As stated

DFAS RESPONSE TO IG REPORT ON EDA SECURITY
GENERAL CONTROLS OVER THE ELECTRONIC DOCUMENT
ACCESS SYSTEM
PROJECT # D2000FG-0057

DOD IG Finding Pg. 4.:

Security controls over the EDA system were not sufficient to provide users with reasonable assurance that data transmitted electronically and used by DFAS Columbus Center were accurate. This lack of sufficient security controls for EDA occurred because:

- Security responsibilities were not defined
- An end to end assessment of security has not been completed
- DFAS security and training requirements are not defined and
- The DFAS Columbus Center lacked adequate resources

As a result, program risk increases and data maintained in EDA could be subject to alteration or misuse. Further, auditors performing work in support of DFAS financial statements will continue to have to expend significant resources to support and verify compliance with CFO Act Requirements.

DFAS REPLY:

DFAS agrees with the DoD IG recommendations to fully address security responsibilities and requirements; develop the System Security Authorization Agreement (SSAA); complete security training; and better enable the security manager in Columbus through better training and provision of resources to fully oversee the security responsibilities of the Center. In addition, DFAS acknowledges that security responsibilities were not fully defined or documented. However, DFAS does not agree that data maintained in EDA could be subject to alteration or misuse by users of the system. Strong controls are in place to prevent access and modification of the document. Further, DFAS has sufficient internal controls and resources in place to prevent such an occurrence. Lastly, with regards to the auditor efforts, the Columbus response applies:

"As stated in the draft report, page 8, the Air Force Audit Agency (AFAA) substantiated all contracts reviewed in their FY 1999 Chief Financial Officers (CFO) audit and, therefore, obtained a 100 percent authentication of EDA documents. Consequently, the AFAA reduced their sample selection from 1,200 plus transactions in FY 99, to less than 300 under their current FY 2000 CFO work for both General and Working Capital Fund Audits."

DOD IG Finding Page 7.: "The terminal area security officer within each division at the DFAS Columbus Center maintains a list of personnel who have access to EDA. The list, however, is

not based upon least privilege, security levels, or type of position held at DFAS Columbus Center. Rather, access to EDA was granted based on a supervisor's determination that an employee needed access regardless of whether or the individual had access to other system that could be incompatible....."

DFAS Reply: DFAS employees only have read access to EDA. No DFAS employee has access to EDA that enables him or her to add, delete or alter EDA documents.

DOD IG Finding Page 7.: "The information security manager at DFAS Columbus Center was not aware of any security readiness reviews conducted on the EDA servers at the Columbus computer center. A security readiness review assesses the operating system and computer for vulnerabilities that would allow an intruder to perform malicious acts and destroy the audit trail. As part of its responsibility to oversee security of DOD systems, DISA periodically conducts security readiness reviews of systems to determine the reliability of the system and its data. In June 1999, DISA performed a security readiness review on the EDA servers at the Columbus computer center and reported 34 findings. Although the Columbus computer center has resolved the findings, the information security manager was unaware that the security readiness review was completed or that findings existed."

DFAS Reply: This statement is true in regards to the information security manager interviewed. Our research indicated that the employee was new to the position and was unaware of the June 1999 review. Other DFAS Headquarters and Columbus Center officials were fully aware of the review and findings. Recommend this portion of the report be removed.

DOD IG Finding Page 8.: Last paragraph states that "According to DFAS Headquarters officials, EDA is not supposed to have internal controls....."

DFAS Reply: DFAS takes internal controls serious and believes EDA must have internal controls in place. This was the primary reason for requesting this audit. Recommend removing this statement from the report.

Other comments:

End to End Testing. The System Security Authorization Agreement (SSAA) is a key document in the accreditation process. It is governed by the DoD Information Technology Security Certification and Accreditation Process (DITSCAP). The SSAA describes the DITSCAP plan and outlines the tailoring factors for the specific system to be accredited. It is appropriate for the plan to identify the specific environment to be tested, and to refer to related, associated, or "feeder" systems, which may be tested separately. In fact, it makes sense to test these other systems in their own environment and to refer to or incorporate the test results in the EDA SSAA, rather than to duplicate effort.

DOD IG Recommendations:

1. We recommend the Chief Information Officer, Defense Finance and Accounting Service, complete a security training curriculum for the information security manager, the information system security officer, and the terminal security officer in accordance with the Assistant Secretary of Defense for Command, Control, Communications and Intelligence June 29, 1998 memorandum on Information Assurance training.

   DFAS REPLY:

   - Concur - DFAS Arlington is in the process of completing all required information assurance training addressed in Recommendation 3. The training is being provided agency-wide to include the security personnel at DFAS Columbus and will be completed by March 2001.

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

   a. Require the information security manager to document and execute a plan to implement and enforce all applicable security policies and safeguards over the systems at the Defense Finance and Accounting Service Columbus Center.

      DFAS REPLY:

      - Concur – The information security manager (ISM) has prepared a draft copy of the Information Security Plan (ISP) which outlines the goals, objectives, specific actions, roles, and responsibilities of various DFAS managers and associates. The final version of the ISP will be completed by December 31, 2000 and implemented in January 2001.

   b. Develop access profiles for all personnel having access to Electronic Document Access.

      DFAS REPLY:

      - Nonconcur - Contract Pay Services personnel do not have the capability to alter or change EDA documents. Their access is limited to browse and print capability only. The contract writing organizations are the initiators of contracts and modifications converted for EDA documents and have content control. Accordingly, access profiles as recommended is considered a moot issue in light of the above.

      - Contract Pay Services personnel accesses to the systems are controlled by a Terminal Area Security Office (TASO). Each TASO is responsible for all employees in an assigned organization unit. The system accesses are captured in a spreadsheet for each person and reviewed to ensure no internal control violations.

whether there are inconsistencies between the functional requirements of the two accesses. If inconsistencies are found, corrective action will be taken to restrict the query access to only the EDA documents needed to accomplish assigned duties.

c. Require the information security manager to attend training on information management and information security controls, planning and administration of the security program, access control, network security measures, electronic commerce security issues and physical protection of the computing facilities.

DFAS REPLY:
Concur: The ISM has attended in excess of 450 hours formal training. We concur that course curriculum geared specifically to the discipline of information security management is desired. The estimated completion date of training is NLT March 2001.

d. Assess the resource needs of the information security manager and redirect or request additional resources, as necessary, to perform the functions described in the Defense Finance and Accounting Service Regulation 8000.1-R, "Information Management Corporate Policy", May 21, 1999.

DFAS REPLY:
Concur - The ISM is part of the establishment of the Technical Services Organization which will be completed June 2001.

DOD IG Material Management Control Weakness.
The DOD IG also requested management comment on the material control weakness discussed in Appendix A. It states, "Management controls were not adequate to ensure the accuracy of electronic transactions using EDA".

DFAS REPLY:

- Nonconcur - Access Profiles. Users of EDA vary in their right access to documents (some access vouchers, some access contracts, some access both). EDA access is always "read only". No DFAS user may alter an EDA document. In DFAS Columbus, entitlements processing personnel, disbursing personnel, and others involved in the bill paying process, must have access to MOCAS and EDM, along with EDA and with multiple feeder systems. This multiple access is necessary in order to process payments. While there is separation of duties for the functions that they perform, these individuals do have access to several systems as part of the bill paying process. Internal controls over the MOCAS payment process preclude errors or fraudulent transactions from resulting in erroneous payments. Limiting access as suggested by the auditors would not apply to those individuals who are involved in the payment process, unless it limited their ability to process valid as well as invalid payments.

- Possibility that EDA documents could be altered. The auditors offered no support that EDA documents could be altered. They did report a single individual with improper access to certain MOCAS tables. However, that access did not allow the individual to change EDA.

There is an implication in the report that someone might access EDA and copy a contract, then use that contract to make an improper payment. It should be noted that anyone making a copy of an EDA contract would not be able to store that copy on the EDA server. Thus the copy would be nothing more than a copy of a contract such as is readily available today.

- Need for signatures on EDA documents. The EDA business rules and DFAS/DLA legal opinions do not require signatures on EDA documents. Internal controls are in place to assure that contracts are signed before they are loaded onto EDA. Actual signatures are on file on the official contract copy maintained by the Contracting Officer.

- Accuracy of EDA documents. According to the audit report, the Air Force Audit Agency required DFAS to produce 11,000 documents to verify the reliability of electronic data. The report acknowledges that all EDA contracts reviewed by the Air Force Audit Agency proved to be valid. It is difficult to understand how this report can conclude that EDA data cannot be relied upon when so many documents were validated without a single error. EDA business rules require a 95% accuracy rate. The Auditors validated a 100% accuracy rate.

Audit Team Members

The Finance and Accounting Directorate, Office of the Assistant Inspector General for Auditing, DoD, prepared this report.

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

INTERNET DOCUMENT INFORMATION FORM

A . Report Title: General Controls Over the Electronic Document Access System

B. DATE Report Downloaded From the Internet: 01/04/01

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

D. Currently Applicable Classification Level: Unclassified

E. Distribution Statement A: Approved for Public Release

F. The foregoing information was compiled and provided by:
DTIC-OCA, Initials: __VM__ **Preparation Date 01/04/01**

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