

A *udit*

R *eport*



CONTROLS FOR THE ELECTRONIC DATA INTERCHANGE AT
THE DEFENSE FINANCE AND ACCOUNTING SERVICE
COLUMBUS

Report No. D-2001-095

April 6, 2001

Office of the Inspector General
Department of Defense

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 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 ³ I)	Assistant Secretary of Defense for Command, Control, Communications and Intelligence
CCR	Central Contractor Registry
DEBX	Defense Electronic Business Exchange
DFAS	Defense Finance and Accounting Service
DISA	Defense Information Systems Agency
DITSCAP	DoD Information Technology Security Certification and Accreditation Process
EDI	Electronic Data Interchange
JECPO	Joint Electronic Commerce Program Office
MOCAS	Mechanization of Contract Administration Services
SAMMS	Standard Automated Materiel Management System



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

April 6, 2001

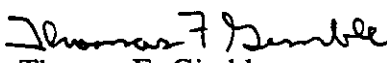
MEMORANDUM FOR ASSISTANT SECRETARY OF DEFENSE (COMMAND,
CONTROL, COMMUNICATIONS, AND
INTELLIGENCE)
DIRECTOR, DEFENSE FINANCE AND ACCOUNTING
SERVICE
DIRECTOR, DEFENSE INFORMATION SYSTEMS
AGENCY
DIRECTOR, JOINT ELECTRONIC COMMERCE
PROGRAM OFFICE

SUBJECT: Audit Report on Controls for the Electronic Data Interchange at the
Defense Finance and Accounting Service Columbus
(Report No. D-2001-095)

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 Joint Electronic Commerce Program Office conformed to the requirements of DoD Directive 7650.3; however, additional comments are needed on Recommendations 3 and 4. For Recommendation 3, the comments should address the verbal agreement made by the Defense Finance and Accounting Office and the Joint Electronic Commerce Program Office regarding the Defense Finance and Accounting Service trading partner agreements. For Recommendation 4, the comments should include an explanation concerning the impact that the remaining five security findings will have on the security of the Electronic Data Interchange as well as the anticipated closing date for the remaining five security findings. Therefore, we request additional comments to the final report by June 6, 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.


Thomas F. Gimble
Acting
Deputy Assistant Inspector General
for Auditing

Office of the Inspector General, DoD

Report No. D-2001-095

(Project No. D2000FG-0057.01)

April 6, 2001

Controls for the Electronic Data Interchange at the Defense Finance and Accounting Service Columbus

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. In 1998, the Joint Electronic Commerce Program Office assumed a lead role in the Electronic Data Interchange as part of the DoD Paper-Free Contracting Initiative. The Electronic Data Interchange sends and receives contract payment information from computer to computer in a standard format, thus allowing documents to be received, validated, accepted, and immediately processed. Electronic Data Interchange was designed to reduce the amount of paper used and stored by DoD contracting personnel, reduce the contract payment cycle time, and facilitate the sharing of information among Government and commercial communities. In essence, Electronic Data Interchange should eliminate the need to use paper documentation to enter contract data in contract pay systems and financial data in accounting systems. Defense Finance and Accounting Service Columbus personnel rely on the information accessed from the Electronic Data Interchange to make an average of 1.2 million payments (344,000 for Mechanization of Contract Administration Services System and 922,000 for Standard Automated Materiel Management System) yearly totaling approximately \$40 billion.

The Director, Defense Finance and Accounting Service Columbus, requested that we review the Electronic Document Access System and the Electronic Data Interchange to determine whether sufficient safeguards were in place to verify the accuracy of electronically transmitted contractual data. We issued a report on the Electronic Document Access System that recommended that the security responsibilities and Defense Finance and Accounting Service security and training requirements for the Electronic Document Access System be defined, and that an end-to-end assessment of system security be completed.

Objectives. The audit objective was to determine whether the security of the Electronic Data Interchange was adequate. The audit included reviews of selected security controls, compliance with the Chief Financial Officers Act requirements, and the management control program as it related to the overall objective. The report discusses the Defense Finance and Accounting Service implementation of the Electronic Data Interchange as it applies to the Defense Finance and Accounting Service Columbus general controls.

Results. The Joint Electronic Commerce Program Office security controls over Electronic Data Interchange were not sufficient to provide reasonable assurance that the Defense Finance and Accounting Service Columbus contract payments were accurate. Specifically, the Defense Information Systems Agency performed security test and evaluations on the Electronic Data Interchange in 1999 and 2000 that resulted in

31 findings, which remain open. Further, the security test and evaluations were based on security agreements that did not include input from the Defense Finance and Accounting Service. Unless corrective actions are taken, data transmitted through the Electronic Data Interchange could be subject to undetected alteration and misuse. The lack of a complete security agreement and a security test and evaluation based on that agreement increased the risk of data inaccuracy because security controls were not sufficient. See the Finding section of the report for details on the audit and Appendix A for details of the review on the management control program.

Summary of Recommendations. We recommend that the Director, Joint Electronic Commerce Program Office, coordinate with the Defense Finance and Accounting Service and the Defense Information Systems Agency to update the security agreement for Electronic Data Interchange to incorporate security requirements and the assessment of the risks associated with using Electronic Data Interchange. We also recommend that the Director, Joint Electronic Commerce Program Office, perform an independent Electronic Data Interchange security test and evaluation, based on an updated security agreement, incorporate the security requirements outlined in the security agreement in the Defense Finance and Accounting Service trading partner agreements for the data originating sites, and initiate corrective action to close the 31 open security test and evaluation findings.

Management Comments. The Joint Electronic Commerce Program Office concurred with coordinating with the Defense Finance and Accounting Service and the Defense Information Systems Agency to update the security agreement for the Electronic Data Interchange, performing an independent Electronic Data Interchange security test and evaluation based on the updated security agreement, and incorporating the security requirements outlined in the security agreement in the Defense Finance and Accounting Service trading partner agreement. However, the Joint Electronic Commerce Program Office partially concurred with closing 31 open security test and evaluation findings, stating that the 31 findings are outdated because they are the result of a security test and evaluation done in 1999. A new security test and evaluation was conducted October 2 through 6, 2000. 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 the Joint Electronic Commerce Program Office were responsive. However, comments regarding the 31 open security findings stated that another security test and evaluation was conducted in October 2000 which resulted in 21 security findings. Of the 21 security findings, 5 are expected to remain open. We request that the Joint Electronic Commerce Program Office explain the impact that the remaining five security findings will have on the security of the Electronic Data Interchange as well as provide an anticipated closing date for the remaining five security findings. We also request that the Joint Electronic Commerce Program Office provide written comments that address the verbal agreement made by the Defense Finance and Accounting Office and the Joint Electronic Commerce Program Office regarding the Defense Finance and Accounting Service trading partner agreements. Therefore, we request additional comments to the final report by June 6, 2001.

Table of Contents

Executive Summary	i
--------------------------	---

Introduction

Background	1
Objective	4

Finding

Adequacy of Security Controls Over the Use of Electronic Data Interchange	5
---	---

Appendixes

A. Audit Process	12
Scope	12
Methodology	13
Management Control Program Review	13
B. Prior Coverage	15
C. Report Distribution	16

Management Comments

Defense Information Systems Agency	19
------------------------------------	----

Background

The Director, Defense Finance and Accounting Service (DFAS) Columbus, requested that we review the use of Electronic Document Access and Electronic Data Interchange (EDI) to determine whether sufficient safeguards are in place to verify the accuracy of electronically transmitted contractual data. We issued the draft report, “General Controls Over the Electronic Document Access System” on August 25, 2000. The report stated that the security responsibilities and DFAS security and training requirements for the Electronic Document Access System have not been defined, and an end-to-end assessment of system security has not been completed.

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

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). JECPO acts as a primary entity under the policy direction of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD [C³I]) to integrate electronic commerce in DoD.

Electronic Data Interchange Responsibility. From 1993 to 1998, the Defense Information Systems Agency (DISA) managed EDI and made it available for use at DFAS Columbus. On November 24, 1998, ASD (C³I) selected JECPO to implement DoD electronic commerce. Also in 1998, EDI management was passed to JECPO as part of the paper-free contracting initiative. As managers of electronic commerce, JECPO is responsible for developing security standards for the certification and accreditation of EDI.

DoD System Certification and Accreditation Process. DoD Manual 5200.40, “DoD Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual,” December 1999, (the accreditation process), establishes standards for certifying and accrediting the security of DoD systems throughout their life cycle. The certification supports the accreditation process that determines whether a system is designed and implemented to 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 a security test and evaluation.

System Security Authorization Agreement. The security agreement is a formal binding agreement among the designated approving authority, the certification authority, information technology system representatives, and the program manager. For EDI, the Program Manager, Information Assurance Program Management Office, DISA is the designated approving authority. The DISA Deputy Director for ASD (C³I) Program Integration is the certification

authority; DFAS is the user representative; and JECPO is the program manager. 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 consists of 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.

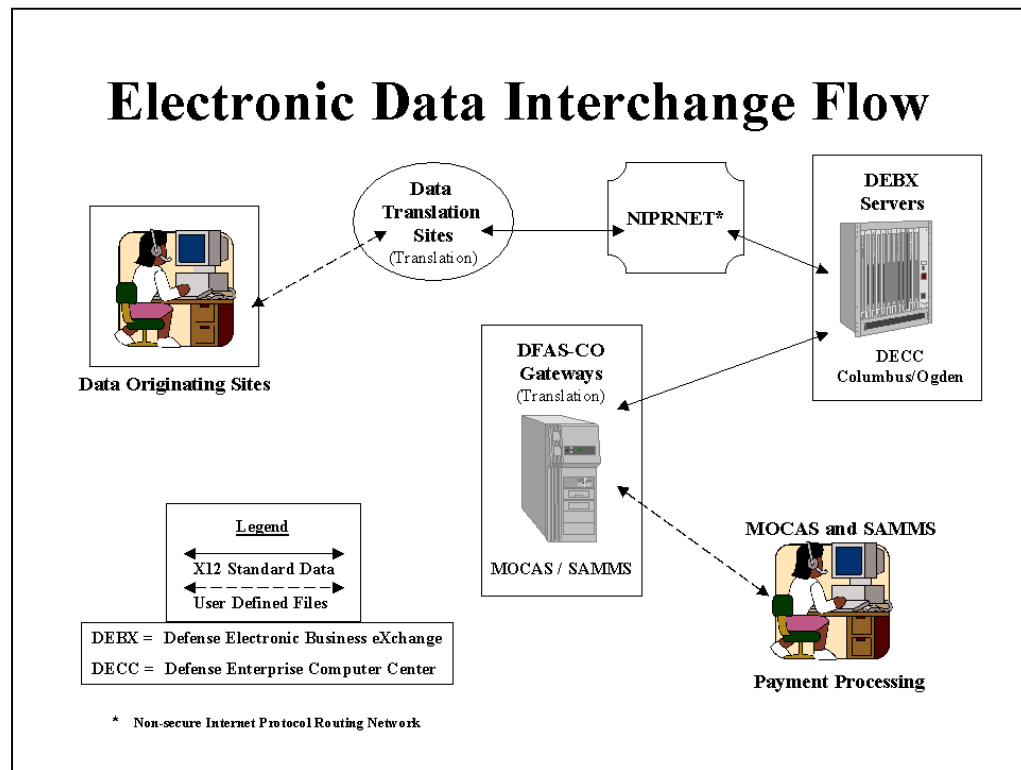
Security Test and Evaluation. The DITSCAP requires a security test and evaluation to be performed in order to evaluate implementation of system security. This security test and evaluation will verify that automated security features affecting confidentiality, integrity, and availability have been implemented according to the security agreement, are performing properly, and provide the required security features. The performance of a security test and evaluation may be a joint effort among the users, systems administrator, and program management. In the case of EDI, the security test and evaluation should consist of DFAS, DISA, JECPO, and data originating sites. The results of the initial security test and evaluation are included in the security agreement that is provided to the designated approving authority for certification and accreditation.

Benefits of Electronic Data Interchange. EDI is the electronic exchange of information between two business concerns (trading partners), in a specific predetermined format. Traditionally, the focus of EDI activity has been on the replacement of paper business forms, such as purchase orders and invoices, with electronic forms. EDI was designed to reduce the amount of paper used and stored by DoD contracting personnel, reduce the contract payment cycle time, and facilitate the sharing of information among Government and commercial communities. In essence, EDI should eliminate the need to use paper documents to enter contract data in contract pay systems and financial data in accounting systems.

DFAS Use of Electronic Data Interchange. DFAS uses EDI to submit information to its contract payment systems.¹ DFAS Columbus personnel rely on the information accessed from EDI to make an average of 1.2 million payments (344,000 for Mechanization of Contract Administration Services [MOCAS] and 922,000 for Standard Automated Materiel Management System [SAMMS]) yearly totaling approximately \$40 billion. Based on the analysis performed on information provided by DFAS, 48 percent of the contract invoices received by MOCAS and SAMMS were paid using EDI.

¹MOCAS and SAMMS are DFAS payment processing systems.

Electronic Data Interchange Flow. The following figure describes the EDI process and the flow of data through EDI.



In order to make a contract payment from MOCAS or SAMMS, DFAS receives images of contracts and receiving reports² from DoD sites, as well as images of invoices from contractors through EDI. EDI translates the data into the American National Standards Institute Accredited Standard Committee X12 format (the X12 format).³ Once the data have been translated into the X12 format, they are forwarded through the Non-secure Internet Protocol Routing Network to the DoD unclassified data communication network into the Defense Business Exchange (DEBX) located in Columbus, Ohio. The DEBX then forwards the data into the DFAS Columbus Gateway, which translates the data from the standard X12 format into files for use by MOCAS and SAMMS payment processing systems.

²The receiving reports confirm to DFAS that the item or service on a contractor's invoice has been received or rendered satisfactorily.

³DoD accepts X12 as the standard format for electronic business transactions.

Objective

The audit objective was to determine whether security for EDI was adequate. The audit included reviews of selected security controls, compliance with the Chief Financial Officers' Act requirements, and the management control program as it related to the overall objective. This report discusses JECPO and DFAS Columbus implementation of controls over EDI. Refer to Appendix A for a discussion of the management control program and Appendix B for prior audit coverage.

Adequacy of Security Controls Over the Use of Electronic Data Interchange

Security controls over the use of Electronic Data Interchange at the Defense Finance and Accounting Service Columbus were not sufficient to provide reasonable assurance that contract payments were accurate. The Defense Information Systems Agency performed security test and evaluations on the Electronic Data Interchange in 1999 and 2000 that resulted in 31 findings, which remain open. Further, the security test and evaluations were based on security agreements that did not include input from the Defense Finance and Accounting Service. The lack of security controls occurred because the Joint Electronic Commerce Program Office and the Defense Finance and Accounting Service have not addressed security over the Electronic Data Interchange to include performing an assessment to identify the risks associated with the use of the Electronic Data Interchange or effectively testing controls over the Electronic Data Interchange process. As a result, data obtained through Electronic Data Interchange may be subject to undetected alteration and misuse. Additionally, the lack of a security agreement and a valid security test and evaluation increased the risk of data inaccuracy and that implemented security may not have operated as intended.

Guidance and Responsibility for Information Systems

Electronic Commerce Responsibilities. In Defense Reform Initiative Directive No. 43, the ASD (C³I) designated JECPO as the DoD-wide organization to oversee implementation of electronic commerce initiatives. DFAS and DISA also play a prominent role in EDI use. DFAS uses EDI to provide data for contract payment processing. DISA provides the infrastructure upon which EDI operates.

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

EDI Guide. DFAS Columbus issued the Electronic Data Interchange Guide on November 4, 1999. The guide contains information pertaining to all current DFAS Columbus EDI transactions. It explains the EDI registration process, format used, and participation requirements (including the trading partner agreements that explain the responsibility of each participant). However, the trading partner agreements do not discuss security.

Establishing EDI Security Controls

Security controls over the use of EDI at DFAS Columbus were not sufficient to provide reasonable assurance that contract payments were accurate. Documentation needed to support the completion of a risk assessment is inadequate. The DITSCAP provides the guidance to assess the risks of operating a system and to determine whether a system can be accredited and certified for use. Specifically, the DITSCAP mandates that information systems managers prepare a system security authorization agreement to document how the system will operate and the risks of operating the system. The risks documented in the security agreement are validated through a security test and evaluation. As a result of a successful security test and evaluation, the system can be certified and accredited for use. If the system does not pass the security test and evaluation the designated approving authority can require that changes be made to the system or grant a 1-year interim authority to operate. The DISA-designated approving authority can issue the interim authority to operate when the benefits of using the system are greater than the security risks discovered in the security test and evaluation. JECPO did not follow this process.

1998 EDI Security Agreement. In 1998, DISA began preparing an EDI security agreement. Also, in 1998, JECPO assumed management of EDI. JECPO, however, did not complete the EDI security agreement because according to the JECPO Deputy Director, controls over paperless transactions should be no greater than the controls over paper transactions. Therefore, JECPO personnel assumed that a completed security agreement was not necessary. Because the security agreement establishes and documents the operating risks of a system, without a complete security agreement, the EDI operating risks were unknown.

In September 1999, DISA performed a security test and evaluation on EDI based on an incomplete security agreement. The DITSCAP requires that the DISA-designated approving authority review the security agreement which includes the results from the assessments and evaluations performed on the system, prior to granting authority to operate or an interim authority to operate. However, the DISA-designated approving authority issued an interim authority to operate in September 1999 although the security test and evaluation was based on an incomplete security agreement. The DISA-designated approving authority later extended the interim authority to operate through October 31, 2000. The DISA-designated approving authority did not follow the certification and accreditation process outlined in the DITSCAP. Although the security test and evaluation was based on an incomplete security agreement, the security test

and evaluation disclosed 21 security findings, which concentrated on important parts of the EDI flow, the DEBX, and the Central Contractor Registry (CCR).⁴

For example;

- the DEBX and the CCR security policy have been in draft since 1996;
- the DEBX and the CCR are operating without full implementation of security safeguards necessary to protect against sabotage, tampering, fraud, misappropriation, misuse, or release to unauthorized persons; and
- several files with superuser and group privileges⁵ on the DEBX and the CCR are listed.

The security agreement for EDI is still in draft and the expected completion date was early January 2001. Additionally, a security test and evaluation based on the new security agreement was completed on October 4, 2000. The security test and evaluation disclosed 10 additional security findings. JECPO personnel stated that they will attempt to correct 8 of the 10 additional findings identified in the security test and evaluation results. Two of the findings disclosed in the security test and evaluation that JECPO personnel expect to correct specifically relate to issues discussed in this report. For example:

- although a System Security Authorization Agreement is in draft, it requires final coordination and signatures of agreement; and
- Memorandums of Agreement, Memorandums of Understanding, and Levels of Agreement have not been established with any of the interfaces to include DFAS and DISA.

As a result of this information, the DISA-designated approving authority granted another extension on the EDI interim authority to operate which now expires on April 30, 2001.

Assessing EDI Security Controls

Security controls at DFAS Columbus were not reliable because JECPO and DFAS have not addressed security over EDI to include performing an assessment to identify the risks associated with the use of EDI or effectively testing EDI controls. JECPO and DFAS had not coordinated an effort to

⁴In order to conduct business with the Federal Government at DFAS Columbus, all contractors must be registered with the DISA Central Contractor Registry, regardless of whether the business is conducted through EDI or on paper.

⁵Superusers have all privileges at all times. Group privilege is a set of users in a system that are given the same access rights to the system.

complete security agreements and assess risks, validate risk assessment through test and evaluation, and account for security requirements in trading partner agreements.

Establishing a Security Agreement and Assessing Risk. The DITSCAP requires that the parties involved in a system's operation work together to establish a security agreement that assesses the risk of using the system. However, JECPO, DFAS, and DISA personnel did not work together to verify that the use of electronic commerce initiatives in DoD was secure.

In August 1998, DISA prepared a draft security agreement for EDI. Further, JECPO began updating the security agreement which had an expected completion date of September 2000. However, JECPO personnel stated that the security agreement did not contain DFAS input. This is a significant oversight because DFAS relies upon correct EDI information to make contract payments. DFAS personnel need to know whether controls to validate that accurate contract payments have been assessed by DoD. To mitigate this risk, JECPO, DFAS, and DISA should develop a working group or team to oversee the preparation of an EDI security agreement.

Validating the Security Agreement through Test and Evaluation. The DITSCAP mandates that the security agreement and any subsequent certification and accreditation be validated through security test and evaluation. In September 1999, DISA performed a security test and evaluation as a result of the draft security agreement developed in August 1998. However, because the security test and evaluation was not based upon a completed security agreement that included DFAS input it is unlikely that the security test and evaluation sufficiently validated the risks of operating EDI at DFAS Columbus.

Further, according to JECPO officials, the 21 findings identified in the September 1999 security test and evaluation will remain open because JECPO officials believed that EDI only automated a paper intensive process and, therefore, needed no additional security. As a result, JECPO has not taken action to correct deficiencies identified through the security test and evaluation and may not have tested for other weaknesses because the security agreement was incomplete.

JECPO conducted an EDI security test and evaluation as a result of the new security agreement. However, JECPO did not address the 21 open findings and did not include DFAS Columbus in the preparation of the new security agreement and the security test and evaluation. Thus, the new security test and evaluation will likely not validate EDI security at DFAS Columbus. JECPO needs to update the security agreement to include DFAS Columbus concerns. JECPO should require DFAS to participate in the EDI security test and evaluation to determine whether the risks are acceptable.

Accounting for DFAS Trading Partner Agreements. The DITSCAP states that the security agreement will be the single document to address the security of a system. However, in order to make contract payments using EDI, DFAS enters into trading partner agreements with contractors and other DoD personnel (data originating sites). Using EDI, contractors send invoices and the DoD sites send receiving reports or other contract payment documentation. DFAS establishes trading partner agreements with each site that submits data through

EDI to DFAS Columbus. Trading partner agreements state that the data originating sites will maintain a certain level of security, but the trading partner agreements are silent on the definition of “certain level of security,” and what security requirements should be maintained. However, once an agreement is signed, no testing is performed by JECPO, DFAS, or the trading partner to verify compliance with the agreement to provide security. Further, the DFAS trading partner agreements need only be established and completed once, and then are valid for all current and future EDI transactions.

JECPO and DFAS have no assurance that security measures have been taken by the originating sites or that data provided to DFAS by those locations are accurate and unaltered. JECPO should require that the trading partner agreements include the security requirements contained in the EDI security agreement and are validated through the EDI security test and evaluation process. This will verify that EDI data are protected in accordance with the DITSCAP requirements.

Status of EDI Security Controls

The controls over EDI use at DFAS Columbus did not provide reasonable assurance that the system was adequately protected. As such, the EDI security weaknesses increased the risk for undetected alteration or misuse. The lack of a complete security agreement and a valid security test and evaluation increased the risk of data inaccuracy. There is also a risk that implemented security procedures may not have operated as intended as evidenced by the 31 open security test and evaluation findings. Therefore, JECPO should correct all the open security test and evaluation findings.

Management Actions

During the audit, we informed JECPO, DFAS, and DISA personnel that the DITSCAP process should be followed for EDI. Subsequently, JECPO started to prepare another draft EDI security agreement, which was completed on January 1, 2001. The DISA designated approving authority granted an extension on EDI interim authority to operate which now expires on April 30, 2001, as a result of a security test and evaluation that was completed on October 4, 2000. The decision to follow the DITSCAP process is acceptable; however, DFAS, which uses EDI to make payments again was not part of the process. Therefore, the input of all affected stakeholders required by the DITSCAP has not been met. DFAS input is necessary to validate that the risks of making \$40 billion in contract payments are tolerable.

Summary

Managers can not attest to the reliability of EDI data until a security agreement has been accomplished with all the necessary participants, the security test and evaluation findings have been assessed, and security policies are contained in trading partner agreements. JECPO should establish an electronic commerce workgroup or team to verify that necessary security requirements are obtained

from DFAS, DISA, and data origination sites. The EDI security agreements and trading partner agreements should be validated through the security test and evaluation and the trading partner agreements should reflect the security requirements outlined in the security agreement.

Recommendations, Management Comments, and Audit Response

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

- 1. Update the security agreement for Electronic Data Interchange to incorporate security requirements and the assessment of the risks associated with using the Electronic Data Interchange to include input and participation from the Defense Finance and Accounting Service and the Defense Information Systems Agency.**

JECPO Comments. JECPO concurred and stated that a security agreement for the Defense Electronic Business Exchange, in accordance with the Defense Information Technology Security Certification and Accreditation Process, has been finalized and agreement was obtained from all principals involved.

- 2. Perform an independent Electronic Data Interchange security test and evaluation, based on an updated security agreement to include Electronic Data Interchange users, the Defense Finance and Accounting Service, and the Defense Information Systems Agency.**

JECPO Comments. JECPO concurred and stated that on October 2 through 6, 2000, an independent security test and evaluation was performed to validate all security requirements as documented in the security agreement. The findings resulting from the security test and evaluation are being addressed and appropriate corrective actions are being implemented.

- 3. Incorporate the security requirements outlined in the security agreement in the Defense Finance and Accounting Service trading partner agreements for the data originating sites.**

JECPO Comments. JECPO concurred and stated that as part of the Electronic Commerce Interoperability Process, Value Added Networks, and direct connect vendors, to include DFAS trading partners, must agree to abide by the terms and conditions when they submit their Client Application Questionnaire.

Audit Response. The formal comments from JECPO were partially responsive because the Electronic Commerce Interoperability Process was not a sufficient means to provide trading partners with the appropriate security requirements. Subsequent to the JECPO written comments, DFAS and JECPO personnel agreed that DFAS would incorporate the security agreement requirements in the trading partner agreements. Therefore, we request that the Joint Electronic Commerce

Program Office provide written comments that address the verbal agreement made by the Defense Finance and Accounting Office and the Joint Electronic Commerce Program Office regarding the Defense Finance and Accounting Service trading partner agreements.

4. Initiate corrective action to close the 31 open security test and evaluation findings.

JECPO Comments. JECPO partially concurred and stated that the 31 findings referenced in the report are outdated because they are the result of a security test and evaluation conducted in 1999. Since the test in 1999, a new security test and evaluation was conducted October 2 through 6, 2000. The security test and evaluation in 2000 resulted in 21 security findings. As of February 2001, 12 findings are closed, 9 findings are open, and 5 of the 9 findings will remain open.

Audit Response. Comments from JECPO are responsive. However, we request that JECPO explain the impact that the remaining five security findings will have on the security of EDI. Additionally, we request that JECPO provide an anticipated closing date for the remaining five security findings.

Appendix A. Audit Process

Scope

Work Performed. We performed the audit at DFAS Arlington, DFAS Columbus, and the Joint Electronic Commerce Program Office. We reviewed how DFAS implemented controls for an entity-wide security program and access controls for EDI. 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 centers to determine how they implemented security over EDA and EDI. We also performed a walk-through of the EDA and EDI process as it relates to MOCAS and SAMMS.

We reviewed how DFAS Columbus implemented the entity-wide security plan and general security controls (access controls). We obtained and reviewed the security readiness reviews performed by DISA Field Security Operations. The reviews identified weaknesses and planned corrective actions for operating software that supports EDI.

Limitations of Audit Scope. The audit was limited to the review of the general controls. As a result of our assessment of the general controls, we determined that a review of the application controls should not be conducted at this time.

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. As of December 2000, the Act does not provide 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 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-02)**
- **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 Management Technology Area. Objective:** Ensure that DoD vital information resources are secure and protected. **Goal:** Assess information assurance posture of DoD operational systems. (IMT-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 in accordance with 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 EDI. Specifically, we reviewed the implementation of DoD policies and procedures governing EDI. 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 could not ensure that the security for EDA and EDI is adequate. All recommendations in this report, if implemented, will provide adequate controls for ensuring that the security for EDI is adequate.

A copy of this report will be provided to the senior official responsible for management controls in ASD(C³I), DFAS Arlington, and DFAS Columbus.

Adequacy of Management's Self-Evaluation. DFAS Columbus officials did not identify EDI 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), “DoD 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. D-2001-029, “General Controls Over the Electronic Document Access System,” December 27, 2000

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, 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, 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

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
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 Information Systems Agency Comments



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

IN REPLY
REFER TO: Inspector General (IG)

5 March 2001

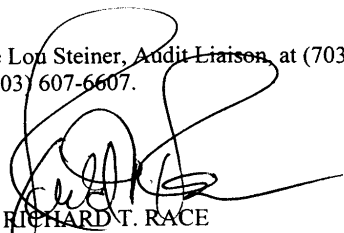
MEMORANDUM FOR INSPECTOR GENERAL, DEPARTMENT OF DEFENSE
(ATTN: ACQUISITION, TECHNOLOGY AND LOGISTICS)

SUBJECT: Response to DoD IG Draft Report, "Controls for the Electronic Data Interchange at the Defense Finance and Accounting Service Columbus," January 5, 2001 (Project D2000FG-0057.01)

1. The attached enclosure provides comments from the Defense Information Systems Agency, Joint Electronic Commerce Program Office on Recommendations 1-4 contained in the above referenced DoD IG Draft Report.

2. If you have any questions, please call Ms. Teddie Lou Steiner, Audit Liaison, at (703) 607-6316 or Jason Bakker, Assistant Audit Liaison, at (703) 607-6607.

For the Director:


RICHARD T. RACE
Inspector General

Enclosure a/s

Quality Information for a Strong Defense



IN REPLY
REFER TO

JOINT ELECTRONIC COMMERCE PROGRAM OFFICE
8725 JOHN J. KINGMAN ROAD, SUITE 1742
FORT BELVOIR, VA 22060-6205

MAR 01 2001

MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL

SUBJECT: Response to the Department of Defense Inspector General (DoD IG) Draft Report on Controls for the Electronic Data Interchange (EDI) at Defense Finance and Accounting Service (DFAS) Columbus (project D2000FG-0057.01, formerly Project No. 0FG-5106)

We have reviewed the subject audit report. Comments are provided in two parts: (1) general comments on the overall report, and (2) specific comments pertaining to the four DoD IG recommendations.

General Comments. Overall, the document makes reference to a number of issues that have been either been resolved or are in the process of being addressed with the appropriate party. The report appears to reflect a misunderstanding of the Electronic Data Interchange (EDI) environment. The Joint Electronic Commerce Program Office does not *accredit* EDI; but rather through the Defense Electronic Business Exchange (DEBX), it *processes* EDI. The DEBX, part of the EC infrastructure network, serves as a single interface between Government and commercial trading partners for conducting electronic commerce/electronic data interchange. The report also seems to imply that all EDI data is identical in its importance and, therefore, an overarching approach is applicable to all data. The JECPO believes that each user requirement must be examined separately, and the controls for one environment may be significantly different from controls used for another requirement. The DEBX infrastructure is strongly protected across the entire end-to-end process, and the JECPO does employ a well-defined and structured process for evaluating, documenting, and satisfying user requirements.

Specific Comments. The following specifically addresses the recommendations in the draft audit report:

1. DoD IG Recommendation: Director, JECPO coordinate with DFAS and Defense Information Systems Agency (DISA) to update the security agreement for EDI to incorporate security requirements and the assessment of the risks associated with using EDI.

JECPO Position: Concur with Recommendation #1.

JECPO Comment: In accordance with the Defense Information Technology Security Certification and Accreditation Process, a System Security Authorization

MAR 01 2001

Agreement (SSAA) for DEBX has been prepared (Attachment A). This document has been finalized and concurrence by all principals completed. (On Feb 15, 2001 DFAS concurred with the format, content, and certification activities within the DEBX SSAA.)

2. DoD IG Recommendation: Director, JECPO perform an independent EDI security test & evaluation based on an updated security agreement consisting of EDI users, the DFAS and the DISA.

JECPO Position: Concur with Recommendation #2.

JECPO Comment: On October 2-6, 2000, an independent Security Test and Evaluation (ST&E) was performed to validate all security requirements as documented in the SSAA. The ST&E was conducted at DEBX processing sites located at Defense Enterprise Computing Center-Columbus, OH (DECC-C) and Defense Enterprise Computing Center-Ogden, UT (DECC-O). The findings, resulting from the ST&E, are being addressed and appropriate corrective actions are being implemented. (Attachment B) There were no Category I findings at either location.

3. DoD IG Recommendation: Director, JECPO incorporate the security requirements outlined in the security agreement in the DFAS trading partner agreement for the data originating sites.

JECPO Position: Concur with Recommendation #3.

JECPO Comment: As a part of the Electronic Commerce Interoperability Process (ECIP), Value Added Networks (VANs) and direct connect vendors, to include DFAS trading partners, must agree to abide by the terms and conditions when they submit their Client Application Questionnaire. The ECIP is designed to provide procedures, including security requirements, for connecting to the DEBX.

4. DoD IG Recommendation: Director, JECPO close the 31 open security test and evaluation findings.

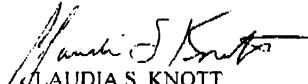
JECPO Position: Partially Concur with Recommendation #4.

JECPO Comment: The 31 findings referenced in the report are outdated because they are the result of a security test and evaluation done in 1999 on the Electronic Commerce Processing Node (now DEBX) and Central Contractor Registry Interface at three operational sites. Since the test in 1999, the DEBX baseline has been upgraded and a new ST&E was conducted 2-6 October 2000 at DECC-C and at DECC-O. The ST&E in 2000 resulted in 21 security findings (10 findings

MAR 01 2001

at DECC-C and 11 findings at DECC-O). As of February 2001, twelve are closed, nine are open; and five (of the nine) will remain open. The five findings that are open are required to perform major functions of DEBX. The remaining four are categorized as "Procedure, Paperwork or Policy" and are expected to be closed 4QTR01. Countermeasures and mitigating factors have been addressed/implemented for all of the open findings. (Attachment B)

Attachments


CLAUDIA S. KNOTT
Executive Director
JECPO/eBusiness
Information Operations

Copy to:
DASD (Deputy CIO)
DLA (J6)
DISA (D2)
DLA IG
DISA IG

Audit Team Members

The Finance and Accounting Directorate, Office of the Assistant Inspector General for Auditing, DoD prepared this report. Personnel of 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
Lisa C. Rose-Pressley
Stephen G. Wynne