Audit Report

OFFICE OF THE INSPECTOR GENERAL

COMPUTER SECURITY FOR THE FEDERAL ACQUISITION COMPUTER NETWORK

Report No. 96-214 August 22, 1996

19991123 069

Department of Defense

DTIC QUALITY INSPECTED 4

DISTRIBUTION STATEMENT A
Approved for Public Release
Distribution Unlimited

AQI00-02-0509

Additional Information and Copies

To obtain additional copies of this audit report, contact the Secondary Reports Distribution Unit of the Analysis, Planning, and Technical Support Directorate at (703) 604-8937 (DSN 664-8937) or FAX (703) 604-8932.

Suggestions for Audits

To suggest ideas for or to request future audits, contact the Planning and Coordination Branch of the Analysis, Planning, and Technical Support Directorate at (703) 604-8939 (DSN 664-8939) or FAX (703) 604-8932. Ideas and requests can also be mailed to:

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

Defense Hotline

To report fraud, waste, or abuse, contact the Defense Hotline by calling (800) 424-9098; by sending an electronic message to Hotline@DODIG.OSD.MIL; or by writing to the Defense Hotline, The Pentagon, Washington, D.C. 20301-1900. The identify of each writer and caller is fully protected.

Acronyms

ADP	Automatic Data Processing
DISA	Defense Information Systems Agency
EC	Electronic Commerce
EDI	Electronic Data Interchange
FACNET	Federal Acquisition Computer Network
FAR	Federal Acquisition Regulation

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

August 22, 1996

MEMORANDUM FOR DEPUTY UNDER SECRETARY OF DEFENSE
(ACQUISITION REFORM)
DIRECTOR, DEFENSE INFORMATION SYSTEMS
AGENCY

SUBJECT: Audit Report on Computer Security for the Federal Acquisition Computer Network (Report No. 96-214)

We are providing this audit report for your information and use. Management comments on a draft of this report were considered in preparing the final report.

Management comments on the draft report conformed to the requirements in DoD Directive 7650.3. Therefore no additional comments are required. As a result of management comments requesting redirection of recommendations, we redirected Recommendations A.2. and A.3. to the Deputy Under Secretary of Defense (Acquisition Reform). The recommendations pertain to approval of a security plan for the Federal Acquisitions Computer Network and to limiting use of that network until a digital signature capability for it is obtained. Therefore, we request that the Deputy Under Secretary of Defense (Acquisition Reform) comment on the recommendations by October 23, 1996.

We appreciate the courtesies extended to the audit staff. Questions on the audit should be directed to Ms. Kimberly A. Caprio, Audit Program Director, at (703) 604-9248 (DSN 664-9248) (electronic mail KCaprio@DODIG.OSD.MIL) or Mr. Kent E. Shaw, Audit Project Manager, at (703) 604-9228 (DSN 664-9228) (electronic mail KShaw@DODIG.OSD.MIL). See Appendix G for the report distribution. The audit team members are listed inside the back cover.

Robert J. Lieberman

Robert J. Lieberman
Assistant Inspector General
for Auditing

Office of the Inspector General, DoD

Report No. 96-214 **August 22, 1996**
(Project No. 5CA-3003)

Computer Security for the Federal Acquisition Computer Network

Executive Summary

Introduction. Presidential memorandum, "Streamlining Procurement Through Electronic Commerce," October 26, 1993, promotes the simplification and streamlining of the procurement process for small purchases by enabling the electronic exchange of procurement information between the private sector and the Government. Further, the memorandum advocates providing greater access to Federal procurement opportunities, ensuring simplified access for potential suppliers, and using nationally accepted data formats. Congress fully endorsed the electronic commerce initiative when it passed the Federal Acquisition Streamlining Act of 1994 (the Act). The Act requires implementation of the development of the Federal Acquisition Computer Network (FACNET) and electronic generation and transmission of procurement transactions between the Government and its contractors. The Act required that the FACNET system be implemented Government-wide by January 2000.

The use of electronic transactions rather than paper-based transactions introduces new security risks. An electronic system must:

o be able to reliably carry transactions from their source to their destination,

o provide for recovery from major and minor disasters without jeopardizing the ability of the Government to purchase needed items in a timely manner,

o provide sufficient audit trails to prove that transactions were delivered as intended, and

o provide sufficient protection from disclosure of information that the Government or its contractors consider sensitive.

Additionally, because transactions sent electronically cannot be signed in the traditional sense, alternative methods of transaction authorization must be in place. FACNET processes 15,000 to 20,000 transactions per day. During June 1996, DoD made 2,629 contract awards using FACNET. The dollar value of those awards was not available. An overview of the FACNET infrastructure is provided in Part I.

Audit Objectives. The audit objective was to evaluate procedures for data security, continuity of operations, transaction audit trails, personnel security, and compliance

with security requirements for small purchases made through the FACNET electronic commerce and electronic data interchange program. We also examined the management control program as it relates to the primary audit objective.

Audit Results. The Defense Information Systems Agency had not obtained capabilities for digital signatures or encryption for procurement transactions sent over FACNET. As a result, FACNET transactions could suffer undetected alterations, may not satisfy legal requirements, and may be subject to compromise (Finding A). The Defense Information Systems Agency had not established data backup procedures or developed the required continuity of operations plans for FACNET. As a result, the ability of FACNET to recover operations following a disaster is not assured (Finding B). The Defense Information Systems Agency Electronic Commerce and Electronic Data Interchange Program Management Office had not provided adequate controlled access protection for FACNET. As a result, FACNET is not protected from fraud and criminal threats (Finding C). The management control program could be improved because we identified material weakness applicable to the computer security for FACNET primary audit objective (Appendix A).

Summary of Recommendations. We recommend that the Deputy Under Secretary of Defense (Acquisition Reform) approve a plan and establish milestones for implementing digital signatures and data encryptions for the FACNET system and limit use of FACNET transactions that require signatures until the Defense Information Systems Agency obtains digital signature capabilities. We recommend that the Director, Defense Information Systems Agency develop backup procedures for FACNET gateways that include storage of critical data at an off-site location; and develop continuity-of-operations plans for the gateways. We recommend that the Defense Information Systems Agency Electronic Commerce and Electronic Data Interchange Program Management Office enhance network security by implementing a firewall protection mechanism and by ensuring that FACNET complies with controlled access protection requirements.

Management Comments. The Director, Defense Information Systems Agency, concurred with the draft report recommendations. The Director stated that the Defense Information Systems Agency either has implemented or plans to implement corrective actions. However, the Defense Information Systems Agency requested redirection of two recommendations to the Deputy Under Secretary of Defense (Acquisition Reform), because the Deputy Under Secretary of Defense (Acquisition Reform) should make the determination whether digital signatures and encryption are the proper technical solution. See Part I for a discussion of management comments. See Part III for the complete text of management comments.

Audit Response. The actions proposed by the Defense Information Systems Agency are fully responsive and meet the intent of our recommendations. As a result of the Defense Information Systems Agency request, we redirected Recommendations A.2. and A.3. to the Deputy Under Secretary of Defense (Acquisition Reform). We request that the Deputy Under Secretary of Defense (Acquisition Reform) submit comments on those recommendations by October 23, 1996.

Table of Contents

Executive Summary i

Part I - Audit Results

Audit Background 2
Audit Objectives 4
Finding A. Data Security 5
Finding B. Data Backup and Continuity of Operations 11
Finding C. Controlled Access Protection 15

Part II - Additional Information

Appendix A. Scope and Methodology
Scope 20
Management Control Program 21
Appendix B. Summary of Prior Audits and Other Reviews 22
Appendix C. Other Matters of Interest 25
Appendix D. Glossary 27
Appendix E. Electronic Data Interchange Transactions That Require Digital Signatures and Encryption Capabilities 29
Appendix F. Organizations Visited or Contacted 30
Appendix G. Report Distribution 31

Part III - Management Comments

Defense Information Systems Agency Comments 34

Part I - Audit Results

Audit Background

Electronic Commerce/Electronic Data Interchange in DoD. Electronic Data Interchange (EDI) is computer-to-computer exchange of business data in a standardized format. The prime function of EDI is to help businesses exchange data quickly and without error. Electronic Commerce (EC) is the integration of EDI, electronic mail, electronic bulletin boards, electronic funds transfer, and internal automated processing into a comprehensive system supporting all business functions.

In May 1988, the Deputy Secretary of Defense directed the DoD Components to make maximum use of EDI for the paperless processing of all business-related transactions. The American National Standards Institute X12 uniform standards were to be used as the standards for the EDI program. During September 1993, the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), responsible for implementing EC/EDI in DoD, designated the Defense Information Systems Agency (DISA) as the EC/EDI executive agent responsible for developing EC/EDI technology.

Presidential memorandum, "Streamlining Procurement Through Electronic Commerce," October 26, 1993, promoted the simplification and streamlining of the procurement process for small purchases by enabling the electronic exchange of procurement information between the private sector and the entire Government. Further, the memorandum advocated providing greater access to Federal procurement opportunities, ensuring simplified access for potential suppliers, and using nationally accepted data formats. Subsequently, Congress passed the Federal Acquisition Streamlining Act of 1994. The Act directed establishment of the Federal Acquisition Computer Network (FACNET) Government-wide by January 2000.

FACNET Infrastructure. Figure 1 shows the FACNET infrastructure. The FACNET infrastructure is the system of interconnected communications and computer systems supporting the exchange of EDI transactions between Government organizations and their contractors or trading partners. The infrastructure for the existing FACNET consists of 283 DoD procuring offices that are each connected to one of the seven gateways, two network entry points, value-added networks, and trading partners on FACNET. Appendix D defines terms that are commonly used in electronic commerce.

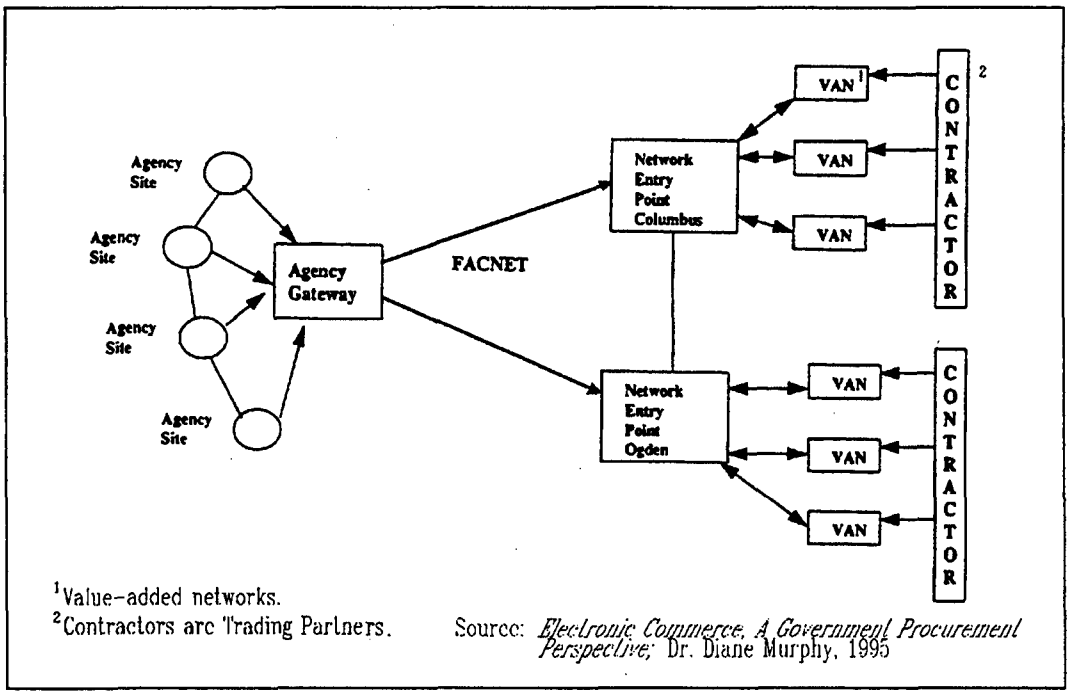

Figure 1. DoD FACNET Architecture.

Gateway. A gateway includes both hardware and software that provide EDI translation services, archiving, security, and environment management for converting nonstandard business application systems data into standard EDI format to Government procurement organizations. The DoD gateways are located at Mechanicsburg, Pennsylvania; Jacksonville, Florida; San Diego, California; Puget Sound, Washington; Montgomery, Alabama; Columbus, Ohio; and Ogden, Utah.

Network Entry Point. The gateways are connected to network entry points. A network entry point is a collection of hardware and software systems that provides communications connectivity between value-added networks and the gateways to support exchange of EDI transactions between Government procurement organizations and trading partners. Two network entry points are in Columbus, Ohio, and Ogden, Utah. A backup facility to the network entry points was recently installed in Slidell, Louisiana. DISA uses the backup facility for software development and testing for FACNET.

Value-Added Network. A value-added network is a commercial entity that provides connections to the FACNET and technical support to its customers. Frequently, the value-added network provides a help desk and troubleshooting for EDI problems, assists with the configuration and upgrades to software, and provides training to its customers on how to use the EDI

system effectively. The Government has 26 certified value-added networks. Government contractors can connect to FACNET by subscribing to services provided by any of the value-added networks. None of the operation costs incurred by the value-added network are charged to the Government.

FACNET Security Implications. Using FACNET eliminates many of the paper documents normally required for a procurement. As a result, original hard copy evidence of obligation or commitment by the Government, its bidder or contractors, or its other data exchange partners may not be available. Instead, electronic records must be used. EDI data become electronic records as they are prepared for transmission and when they are received.

Security must be established to assure that EDI data, as electronic records, are authentic and properly authorized, are reliably carried from their source to their destination, can be recovered from major and minor disasters, and are completely and accurately retained with audit trails for purposes of accountability. In addition, EDI data, while being communicated or stored as records, must be protected from loss, modification, or unauthorized disclosure.

Audit Objectives

The primary audit objective was to evaluate procedures for data security, continuity of operations, transaction audit trails, personnel security, and compliance with network security requirements for small purchases made through the FACNET EC/EDI program. We also examined the management control program as it applied to the primary audit objective. See Appendix A for a discussion of the scope, methodology, and management control program. Appendix B summarizes prior coverage related to the audit objectives. During the audit, we identified problems with personnel security ratings at gateways and network entry points and with DISA transactions through FACNET. Appendix C provides details on those areas.

Finding A. Data Security

DISA has not obtained capabilities for digital signatures or encryption for procurement transactions sent over FACNET. Although representatives of DISA, in conjunction with the National Security Agency, have developed implementing guidance for the use of digital signatures and encryption, DISA has not yet approved the guidance for implementation, and none of the transactions sent over FACNET are digitally signed or encrypted. DISA management had a long-term goal of providing an encryption capability, but had not developed any short-term goals for providing such protection. DISA management did not believe that digital signatures were required for small purchases. Without digital signatures, altered FACNET transactions cannot be readily detected. Additionally, without digital signatures, certain procurement transactions that are being sent over FACNET may not satisfy legal requirements of the Federal Acquisition Regulation and United States Code, title 31, section 1501 (31 U.S.C. 1501). Without encryption, sensitive contractor information such as proposals, bids, and personnel data are subject to compromise.

Digital Signatures and Encryption

Historically, many jurisdictions have adopted "statutes of frauds," for various transactions. A statute of frauds is a law requiring contracts to be in writing and signed to be enforceable. While the Comptroller General has noted that no Federal statute of frauds exists, 31 U.S.C. 1501(a)(1) specifies the provision for recording a valid obligation against the Government. That provision requires a binding agreement, in writing, and executed within the availability of the funding to be used. Because the transactions are paperless, EDI requires alternative procedures to authenticate a transaction. A new technology, called a digital signature, has been developed to serve the same purpose as a handwritten signature. A digital signature is a series of binary digits appended to a digital document. But unlike a handwritten signature, the digital signature is unique to the document being signed. Specifically, the digital signature is unforgeable, proves authenticity, is not reusable, precludes document alteration, cannot be repudiated, and has the same legal status as a handwritten signature.

Encryption is a technique involving scrambling of data in such a manner that the data are unintelligible to anyone other than the intended receiver. The encryption process involves using an encryption algorithm that transforms the data bits into a stream of digits that seems random. Performing the transformation requires a secret key or password. The receiver uses this key to decrypt and recover the original message.

Requirements for Signatures on Procurement Transactions

Federal Acquisition Regulation (FAR) part 4, "Administrative Matters," requires the contracting officer and the contractor to sign a contract. Recent changes were made to the FAR to facilitate implementation of EDI. Additionally, 31 U.S.C. 1501, "Documentary evidence requirement for Government obligations," requires a binding agreement, in writing, and executed within the availability of the funding to be used.

FAR Requirements. Federal Acquisition Circular No. 90-29, "Federal Acquisition Regulation; Introduction of Miscellaneous Amendments," July 3, 1995, was issued to implement changes to the FAR for electronic contracting, simplified acquisition procedures, and FACNET. Although FAR section 4.101, "Contracting Officer's Signature," still requires the contracting officer to sign a written contract, the circular broadens the FAR section 2.101 definition of "in writing" or "written" to include electronically transmitted and stored information. The definition of "signature" or "signed" was changed to mean the discrete, verifiable symbol of an individual that, when affixed to a writing with the knowledge and consent of the individual, indicates a present intention to authenticate the writing.

31 U.S.C. 1501 Requirements. The 31 U.S.C. 1501 states that an amount can be recorded as an obligation when the amount is supported by documentary evidence of a written binding agreement between an agency and another person for a purpose authorized by law. To record a contract as an obligation, a bid must be in writing, acceptance of the bid must be communicated to the bidder in the same manner as the bid was made, and a contract must incorporate the terms and conditions of the bid without qualifications.[1]

[1] 35 Comptroller General 319 (1955).

Transactions That Need Digital Signatures and Encryption Capabilities

DISA has not obtained digital signatures or encryption capabilities. A series of transactions sent over FACNET requires digital signatures and encryption. Appendix E lists the EDI procurement transactions that we believe require a digital signature and the transactions that may be regarded by a trading partner as sensitive and require an encryption capability. For example, the American National Standards Institute 843, "Response to Request for Quotation," should be digitally signed to authenticate the bid and satisfy legal requirements, and it should be encrypted to prevent disclosure to the trading partner's competitors. Our determinations of those transactions that need to use digital signatures were based on whether the current forms that the EDI transactions replace required signatures. Use of encryption for sensitive information should, we believe, be at the option of the trading partner, but the capability for encryption should be offered. If required by the trading partner, DoD must obtain the capability as well.

Acceptance of Digital Signatures for Electronically Generated Documents

The Comptroller General issued decision B-245714, 71 Comptroller General 109, December 13, 1991, which concluded that contracts formed using EDI technologies may constitute valid obligations so long as the technology used provides the same degree of assurance and certainty as traditional "paper and ink" methods of contract formation.

Before using FACNET, or any other method of EDI, the agency head should ensure that the EDI system is capable of ensuring authentication and confidentiality commensurate with the risk and magnitude of the harm from loss, misuse, or unauthorized access to or modification of the information. As mentioned above, and discussed in the Comptroller decision, recording a valid obligation of the Government requires a binding written agreement. Contracts must contain an offer, acceptance, and expression of an intent to enter upon a binding agreement. Typically, the signatures of the parties provide the evidence of that intent.

FACNET managers have generally taken the position that because FACNET is being used for small purchases under the simplified acquisition threshold, under FAR part 13, "Simplified Acquisition Procedures," those acquisitions may be transacted orally. To the extent that oral procedures are authorized, a good

argument can be made that no signature would be required on corresponding electronic procedures. FAR sections 13.106 through 13.108 discuss the authorized procedures and the effects of the different methods. Purchase orders under FAR section 13.501(g) are normally to be signed by the contracting officer in accordance with FAR section 4.101. However, under certain circumstances, unsigned electronic purchase orders are specifically allowed (see FAR section 13.506). FAR section 13.503 specifies situations for requiring written acceptance of purchase orders by the contractor, but seemingly also allows proceeding without such a written acceptance in some cases.

We believe that the best practice is to require a written, signed confirmation of any transaction intended to bind the parties and obligate the expenditure of appropriated funds. That confirmation may be electronic as discussed by the Comptroller General, but to protect the interest of the parties and to form a valid obligation under 31 U.S.C. 1501, the transaction should have a confirmation.

Data Encryption

In addition to digital signatures, information sent over FACNET between DoD and its trading partners needs to be encrypted to protect sensitive data, such as bids, trade secrets, personnel data, proprietary data, and other contractor sensitive information. Encryption would protect such data from disclosure as they flow through the network. Contracting officers are required by FAR part 3 to protect such information.

The American National Standards Institute established a standard[2] for data authentication and encryption. The standard is intended to verify the identity of the sender to the recipient of the transaction, verify the data integrity, provide confidentiality of the business data, and detect insertions, modification, deletion, or impersonation.

[2]American National Standards Institute standard X12.58, "Security Structures."

Implementation of Digital Signature and Encryption Capabilities

During December 1994, DISA network security experts, working with representatives from the National Security Agency, developed a comprehensive security plan for the EDI program. However, as of March 1996, DISA has not approved the plan. The plan requires the use of digital signatures and encryption for the FACNET program.

We discussed with DISA management the need for digital signatures. DISA management did not believe that such capabilities were required for small purchases or purchase orders because in the past, many transactions, specifically purchase orders, were concluded orally, over the telephone. Normally, however, an oral agreement should be confirmed by a signed, written document, when recording a valid obligation as is contemplated by 31 U.S.C. 1501. While that signature and writing may be in an electronic form, according to the Comptroller General decision cited earlier, we believe that the best course is to require some authentication or signature to provide evidence that the Government and contractor are bound by an agreement. DISA management told us that they intended to provide an encryption capability to FACNET, but only after the Fortezza security card had been fully implemented. The Fortezza card is a DoD initiative to use electronic smart cards to authenticate access to DoD computer systems and to provide an encryption capability.

We believe that the Fortezza cards would satisfy existing requirements for encryption and digital signatures, but full implementation of the Fortezza cards could take a long time to complete. In the interim, DISA should approve its existing security plan, or a plan similar to it, for the EDI program and implement short-term solutions, such as software encryption, to satisfy existing requirements for digital signature and encryption. Until DISA obtains a digital signature capability, DISA should limit FACNET use to transactions that do not require a signature.

Without digital signatures, altered FACNET transactions cannot be readily detected. Additionally, without digital signatures, certain procurement transactions that are being sent over FACNET may not satisfy legal requirements of the FAR and 31 U.S.C. 1501. Without encryption, sensitive contractor information such as proposals, bids, and personnel data are subject to compromise.

Recommendations and Management Comments

Redirected Recommendations. As a result of management comments requesting redirection of recommendations, we redirected Recommendations A.2. and A.3. to the Deputy Under Secretary of Defense (Acquisition Reform). DISA stated that the Deputy Under Secretary of Defense (Acquisition Reform) should make the determination whether digital signature is the proper technical solution.

A.1. We recommend that the Director, Defense Information Systems Agency approve a security plan, with milestones, that would provide digital signature and encryption capabilities to the Federal Acquisition Computer Network.

DISA Comments. DISA concurred, stating that it established the EDI Security Working Group for the purpose of addressing EDI Security Policy and development of the security implementation plan consistent with DoD guidelines.

A.2. We recommend that the Deputy Under Secretary of Defense (Acquisition Reform) limit the use of Federal Acquisition Computer Network to those transactions that do not require a signature under 31 U.S.C. 1501 or Federal Acquisition Regulation section 4.101 until the Defense Information Systems Agency obtains a digital signature capability.

Management Comments. We request that the Deputy Under Secretary of Defense (Acquisition Reform) provide comments on the recommendation. No additional DISA comments on this recommendation are required.

A.3. We recommend that the Deputy Under Secretary of Defense (Acquisition Reform) obtain a software encryption and digital signature capability for the Federal Acquisition Computer Network until DoD fully implements the Fortezza card.

Management Comments. We request that the Deputy Under Secretary of Defense (Acquisition Reform) provide comments on the recommendation. No additional DISA comments on this recommendation are required.

Finding B. Data Backup and Continuity of Operations

DISA did not establish uniform procedures for data backup at its seven gateways, did not store data off-site, and did not have a continuity-of-operations plan for its gateways. DISA had not established data backup procedures or a continuity-of-operations plan because DISA had placed a higher priority on operational issues. Without adequate backup procedures, the ability of FACNET to recover operations following a disaster is not assured. Without appropriate continuity-of-operations plans, including backup gateway facilities, segments of FACNET may become inoperable, and organizations that rely on an inoperable gateway are unable to perform EDI. Additionally, such records need to be retained long enough to satisfy minimum retention periods specified in the FAR and by the National Archives and Records Administration.

Data Backup and Continuity of Operations

The Office of Management and Budget and the DoD have issued guidelines on requirements for data backup and continuity of operations. Office of Management and Budget Circular No. A-130, "Management for Federal Information Resources," December 24, 1985, states that agencies shall ensure that information is protected commensurate with the risk and magnitude of harm that would result from loss. In addition, the Circular requires that agencies establish policies and assign responsibilities to ensure that appropriate continuity of operations are developed and maintained. The intent of such plans is to assure that essential functions can still be performed in the event that information technology is interrupted.

DoD Directive 5200.28, "Security Requirements for Automated Information Systems," March 21, 1988, states that unclassified information shall be safeguarded against tampering, loss, and destruction, and shall be available when needed. Furthermore, FAR section 4.805, "Storage, Handling, and Disposal of Contract Files," states that agencies shall prescribe procedures for handling, storing, and disposing of contract files, and the data storage and retrieval procedures shall protect the original data from alteration. With regard to simplified acquisition procedures that are applicable to FACNET transactions, the FAR states that the retention period for unsuccessful offers or quotations for contracts using simplified acquisition procedures is 1 year after date of award or until final payment, whichever is later. The FAR further states that if the contracting officer determines that files have future value to the Government, retention is as long as advisable.

The National Archives and Records Administration (National Archives), however, has more stringent record retention periods than the FAR. The National Archives General Records Schedule 3, "Procurement, Supply, and Grant Records," August 1995, does not authorize destruction of contract, requisition, and purchase order records for transactions of more than $25,000 until 6 years and 3 months after final payment and 3 years after final payment for transactions below $25,000.

Data Backup

DISA did not establish uniform procedures or retention cycles for backing up FACNET data at the seven DoD gateways. As a result, DoD sites we reviewed had varying retention cycles and backup procedures. For example, the gateway in Mechanicsburg, Pennsylvania, performs a tape backup only once every 2 weeks. Conversely, the gateway in Columbus, Ohio, performs a tape backup on a daily basis but purges the data after one week. Although no firm criteria exist for frequency of backups, tape backups should be conducted at least daily, to allow prompt recovery should an error occur and to avoid extensive loss of contractor data. The data should be retained for 1 year in accordance with the FAR requirements. Without adequate backup procedures, the ability of FACNET to recover operations following a disaster is not assured.

Off-Site Storage

Backup data were not stored off-site at any of the gateways that we visited and were not in compliance with DoD Directive 5200.28. Backup data were generally kept adjacent to the computers. When data are not stored off-site, any damage to the computer room area potentially will damage the backup data as well as the original.

Continuity of Operations

The seven FACNET gateways do not have appropriate backup facilities for the continuity-of-operations in the case of system failure. A backup facility is another facility, that is, another gateway, that could assume the workload of an

inoperative gateway. Without a backup facility, an inoperative gateway results in an inability to perform EDI by those organizations that rely on that gateway. For example, a recent hardware problem caused the gateway at Gunter Air Force Base to not process transactions for 2 days; 22 Air Force procurement offices were unable to process EC/EDI transactions during that period. A backup facility would enable continuity of operation in the event of system failure. Management at each of the gateways needs to establish memorandums of agreements and data connections to other gateways that can support them in the event of downtime at the gateway or to develop alternative means to ensure that EC/EDI transactions are minimally affected by inoperative gateways.

Network Entry Points

The two network entry points at Ogden, Utah, and Columbus, Ohio, had adequate protection from disaster because all EDI transactions were being simultaneously transmitted to both sites and because a backup network entry point facility had been established at Slidell, Louisiana.

Recommendations and Management Comments

B. We recommend that the Director, Defense Information Systems Agency:

1. Develop uniform backup procedures at the Federal Acquisition Computer Network gateways to maintain continuity of operations following a disaster or if the Federal Acquisition Computer Network becomes inoperative. Those backup procedures should include retention cycles that will satisfy minimum retention periods specified in the Federal Acquisition Regulation and by the National Archives and Records Administration and that are of sufficient frequency to ensure recovery with minimum loss of data.

DISA Comments. DISA concurred, stating that it had developed standardized backup procedures. DISA would test those new procedures beginning June 17, 1996.[3]

[3]We confirmed that DISA performed the tests as planned, and DISA told us that the tests were successful. DISA is now preparing a report on the test.

2. Store all backup data for the Federal Acquisition Computer Network in a secure location off site from the computer facility.

DISA Comments. DISA concurred, stating that it has procedures in place to store all backup data for EDI infrastructure in a secure location off site from the computer facility.

3. Establish backup facilities and procedures for each of the Federal Acquisition Computer Network gateways to ensure that DoD procuring offices and their trading partners are able to continue processing electronic commerce/electronic data interchange transactions during gateway failures.

DISA Comments. DISA concurred, stating that it is establishing a backup facility at Slidell, Louisiana, however, until the facility is fully operational, DISA will use the operational support facility in Sterling, Virginia, to support backup requirements.

Finding C. Controlled Access Protection

The DISA EC/EDI Program Management Office did not implement the required controlled access protection for FACNET. Access protection was not implemented because the Military Departments and certain Federal agencies requested the Program Management Office not to accept or implement the security recommendations made by the DISA Center for Information Systems Security and the National Security Agency. Also, DISA did not implement additional measures for protection, such as firewalls. As a result, FACNET is not adequately protected from fraud and criminal threats.

Controlled Access Protection Policy

DoD Directive 5200.28, "Security Requirements for Automated Information Systems," March 21, 1988. The Directive states that an automated information system must have Class C2 protection if the system processes sensitive, unclassified information. Class C2 is controlled access protection to prevent unauthorized users from reading and modifying the sensitive information in the network. Controlled access protection can be accomplished by providing identification and authentication, discretionary access control, audit, and object reuse.

Identification and authentication of users are to ensure that the user is authorized to access the system and that the user is who the user claims to be. Discretionary access control limits users' access to system resources according to the access level that they are authorized to accomplish their work. Auditing tracks user accesses, tracks problems that arise, and makes tools available for detecting when unauthorized accesses are attempted or succeed. Object reuse is essentially the clearing of either computer or disk memory between tasks to reduce the potential that subsequent lower access tasks or users do not gain inadvertent access to higher access information by reusing the same memory or disk space.

National Institute of Science and Technology Special Publication 800-10, "Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls," December 1994. The publication states that a firewall can provide additional controlled access protection in the network. The main purpose of a firewall is to control access to or from a protected network by forcing connections to pass through the firewall where they can be examined and evaluated for unwanted access. In principle, a firewall can be thought of as a

device to limit traffic into and out of the network. For example, some firewalls allow only electronic mail traffic through them, thereby protecting the network against attacks from other Internet utility software.

Implementation Of Controlled Access Protection

The DISA EC/EDI Program Management Office did not implement security measures in FACNET to prevent unauthorized users from reading or modifying the sensitive information. Specifically, the DISA EC/EDI Program Management Office did not implement controlled access protection, which includes identification and authentication, discretionary access control, auditing, and object reuse. Without controlled access protection, FACNET data are not protected from unauthorized users reading or modifying the data. DISA must establish controlled access protection for FACNET to assure that EDI data are protected from unauthorized reading and modification.

Compliance With Controlled Access Protection Requirements

The DISA EC/EDI Program Management Office has neither accepted nor implemented the recommended security requirements. DISA EC/EDI program management officials stated that procurement functional users from the Military Departments and the Federal agencies requested the DISA EC/EDI Program Management Office not to accept or implement a recommended solution because it will delay FACNET implementation. The DISA EC/EDI Program Management Office agreed with this request because it viewed the Military Departments and Federal agencies as its customers and wished to satisfy its customer's wishes.

FACNET transactions, even if unclassified, are considered sensitive because they contain trade-secret data, sensitive financial data, or other proprietary data the dissemination of which must be restricted.

In December 1993, the DISA EC/EDI Program Management Office tasked the DISA Center for Information Systems Security and the National Security Agency to provide security requirements for EC/EDI for DoD small procurements. In May 1995, the DISA Center for Information Systems Security and the National Security Agency provided the DISA EC/EDI Program Management Office with two reports on the functional and technical solutions

for FACNET security requirements. The reports identified available technology to implement EC/EDI security requirements, including Class C2 controlled access protection.

FACNET Exposure to Other Networks

FACNET data are transmitted through a series of other networks including the Military Network, the Air Force Internet Network, the Naval Network, or the Defense Data Network, all of which are connected to the Internet. The Internet is a network of computer networks that provides interactive sessions between computers. In recent years, the Internet has suffered from severe security problems. During 1995, the Internet received 900 million hacker attacks. Networks that ignore those problems face significant risk that they will be attacked by hackers and that they may provide hackers with a staging ground for attacks on other networks.

Because the Military Network, the Air Force Internet Network, Naval Network, and the Defense Data Network are connected to the Internet, FACNET transactions sent through those Government networks are vulnerable to unauthorized access. Therefore, firewalls are needed as an additional layer of protection and can be used to compensate for other weaknesses inherent when communicating through the Internet by evaluating incoming messages, limiting traffic, and protecting FACNET from potential attack.

DISA has made efforts to identify the vulnerability of DoD automated systems networks. In December 1995, the automated systems security incident support team from DISA reported that it conducted 48 vulnerability analysis assessment program tests on various DoD systems. The team concluded that 86 percent of DoD unclassified computers were easily penetrated; 98 percent of penetrations were undetected; and 95 percent of detected penetrations were unreported. A recent audit report by the General Accounting Office[4] confirmed that DoD automated systems networks are vulnerable to attack. See Appendix B for details on that report. DISA did not test FACNET, but DISA acknowledges the vulnerability of its system in general.

[4]Report No. GAO/AIMD-96-84, "Information Security Computer Attacks at Department of Defense Pose Increasing Risks," May 22, 1996.

Recommendations and Management Comments

C. We recommend that the Director, Defense Information Systems Agency:

1. Implement the Class C2 controlled access protection for the Federal Acquisition Computer Network.

DISA Comments. DISA concurred, stating that it has implemented the required controlled access protection. DISA is updating its Security Certification and Accreditations.

2. Install firewall protection for the Federal Acquisition Computer Network.

DISA Comments. DISA concurred, stating that it established a firewall protection capability at the Megacenter in Ogden, Utah. DISA also implemented an alternate security solution at the Megacenter in Columbus, Ohio, which included a transmission control protocol/Internet protocol wrapper and restricted send-mail shell. Also, a firewall at the Megacenter in Columbus is scheduled to be implemented as part of the upgrade to the EDI infrastructure.

Part II - Additional Information

Appendix A. Scope and Methodology

Scope

Audit Work Performed. We examined selected security controls for FACNET at the two network entry points and three of the seven gateways. Security controls we reviewed included the security of the EDI procurement transactions, contingency plans for operation following a disaster, the ability of FACNET to track transactions and provide visibility to the receipt status of the transactions to its users, the adequacy of personnel security, and the adequacy of FACNET network security. For data security, we assessed the need for digital signatures and encryption for EDI procurement transactions. For contingency planning, we determined whether the network entry points and gateways had developed the contingency plans and risk analysis required by DoD Directive 5200.28 and had an adequate retention period for procurement transactions to enable recovery. For personnel security, we determined whether key personnel had the required position sensitivity ratings and background checks. On network security, we interviewed computer security experts and reviewed security requirements promulgated by the National Institute of Science and Technology and American National Standards Institute X.12.58, "Security Structures." Appendix F lists those organizations contacted during the audit.

We limited our review of EDI security to the network entry points and the DoD gateways for FACNET. Accordingly, our review did not include an assessment of security at the value-added networks, trading partners, or any of the DoD procurement offices. Our review did not assess security of the EDI program operated by the Defense Logistics Agency separately of FACNET. Additionally, we did not review security of FACNET gateways operated by other Federal agencies.

Audit Period, Standards, and Locations. We performed this program audit from September 1995 through March 1996. The audit was made in accordance with auditing standards issued by the Comptroller General of the United States as implemented by the Inspector General, DoD. We included tests of management controls we considered necessary. We did not use statistical sampling procedures or computer-processed data to perform this audit.

Management Control Program

DoD Directive 5010.38, "Internal Management Control Program," April 14, 1987, requires DoD organizations to implement a comprehensive system of management controls that provides reasonable assurance that programs are operating as intended and to evaluate the adequacy of the controls.

Scope of the Review of Management Controls. We reviewed the adequacy of DISA management controls over FACNET security as they pertain to security of data, backup of data, contingency planning, and network security. We also reviewed the results of any self-evaluation of those management controls.

Adequacy of Management Controls. We identified a material management control weakness, as defined by DoD Directive 5010.38, relating to computer security for FACNET. DISA management controls over FACNET security were not adequate to ensure that FACNET transactions were authentic, met legal requirements, and adequately protect sensitive information from disclosure; that the FACNET system could recover operations following a disaster; and that network access controls were adequate. Recommendations A.1., A.2., A.3., B.1., B.2., B.3., C.1., and C.2., if implemented, will establish the needed controls. A copy of the report will be provided to the senior official responsible for management controls for DISA.

Adequacy of Management's Self-Evaluation. DISA officials identified EC/EDI as an assessable unit in a self-evaluation performed in August 1995 and assigned EC/EDI a medium level of risk. Because we did not review the entire EC/EDI area, we are unable to determine the appropriate level of risk. However, computer security for FACNET should be covered under that assessable unit. As part of the review of the EC/EDI area, DISA should have conducted an evaluation of the management controls applicable to computer security for FACNET. Because DISA did not conduct an evaluation of the management controls applicable to computer security for FACNET, DISA did not identify or report the management control weaknesses identified by the audit.

Appendix B. Summary of Prior Audits and Other Reviews

We identified two General Accounting Office and one Naval Audit Service audit that dealt with security issues at FACNET sites. Additionally, the Inspector General, DoD, has issued three reports specifically about FACNET. The Inspector General, DoD, also issued a report on controls over operating system and security software supporting the Defense Finance and Accounting Service which identified DISA personnel security weaknesses.

General Accounting Office

General Accounting Office Report GAO/AIMD-96-84, "Information Security Computer Attacks at Department of Defense Pose Increasing Risks," May 22, 1996, reported that computer attacks are increasing, the attacks are a multimillion dollar nuisance to DoD, and there is mounting evidence that attacks on DoD computer systems pose a serious threat to national security. The report recommends that the Secretary of Defense ensure that sufficient priority, resources, and top-management attention are committed to establishing a more effective information systems security program. The report also recommends that the Secretary of Defense assign clear responsibility and accountability throughout the DoD for the successful implementation of the security program. DoD officials generally agreed with the findings, conclusions, and recommendations.

General Accounting Office Report GAO/T-NSIAD/AIMD-95-190, "Implementation of the Federal Acquisition Streamlining Act of 1994," July 20, 1995, states that Government-wide standards for protecting the security of sensitive procurement information were not yet defined. The report contains no recommendations.

The Inspector General, DoD

Report No. 96-172, "Audit of Certification Management of Value-Added Networks," was issued on June 21, 1996. The overall audit objective was to determine the adequacy of the value-added network certification process and of the management and oversight of value-added networks. The report

recommends that DISA issue policy requiring enforcement of compliance with FAR section 9.104, "Contractor Qualifications," to include establishing a system for evaluating business qualifications, such as a weighted procedure or point system; issue policy for monitoring value-added networks for compliance with the value-added network license agreement; and expedite the completion and issuance of the new value-added network license agreement. The report recommends that DISA issue policy requiring enforcement of compliance with the FAR section 9.104, "Contractor Qualifications," to include establishing a system for evaluating business qualifications such as a weighted procedure for point system; issue policy of monitoring Value-Added Networks for compliance with Value-Added Network License Agreement; and expedite the completion and issuance of the new Value-Added Network License Agreement. DISA partially concurred with the draft report recommendations.

Report No. 96-129, "Audit of DoD Implementation of Electronic Commerce in Contracting for Small Purchases," was issued on May 24, 1996. The review identified a series of issues involved in the implementation of electronic commerce within DoD. The issues include: realization of the "single face to industry" concept, adequacy of the transmission of data by the DoD FACNET infrastructure, implementation of security controls, level of vendor participation, adequacy of management controls for FACNET transactions, and adequate development of FACNET implementation plans. This report contains no findings or recommendations.

Report No. 96-057, "Audit of DoD Use of Electronic Bulletin Boards in Contracting," was issued on January 8, 1996. The report states that the use of bulletin boards by DoD procurement offices to conduct small purchase transactions was not a major impediment to FACNET implementation. Bulletin boards served as an interim solution that enabled procurement offices to conduct electronic commerce until FACNET becomes fully operational. Procurement officials were not investing significant resources to establish new bulletin boards or to upgrade existing capabilities, and they were committed to phasing out the use of bulletin boards when FACNET becomes fully operational. The report contains no findings or recommendations.

Report No. 94-065, "Audit of Controls over Operating System and Security Software Supporting the Defense Finance and Accounting Service" was issued on March 24, 1994. The report stated that DISA personnel security sensitivity ratings were at levels lower than required by DoD Regulation 5200.2-R, "DoD Personnel Security Program, C3I." DISA management concurred with the recommendation and initiated corrective action. The report identified other security weaknesses in operating systems and security system, but these problems did not relate to FACNET.

Naval Audit Service

Report No. 059-95, "Selected General Controls at Defense Megacenter Mechanicsburg, PA," September 26, 1995, concludes that selected general controls at Defense Megacenter Mechanicsburg did not always operate effectively and efficiently. Guidance on managing minicomputer systems was lacking, backup diesel generators were not reliable, and the Defense Megacenter had not properly designated criticality of automatic data processing personnel. Additionally, DISA could put $1.1 million to better use by restructuring hardware maintenance contracts, eliminating second and third shift guard services, and canceling leases on excess software. The report recommends that DISA improve effectiveness and efficiency by consolidating hardware maintenance contracts and improving physical security and the management of system software and hardware. DISA concurred with recommendations to improve physical security access controls and to establish guidance or direction to improve physical security and Service-level agreement control weaknesses. DISA also agreed that about $490,000 in Defense Business Operations Funds could be put to better use by consolidating maintenance contracts and canceling leases for unused system software products. DISA did not agree with the recommendation to eliminate second and third shift guard protection.

Appendix C. Other Matters of Interest

FACNET technical personnel at the gateways and network entry points lacked the required personnel security ratings. Also, DISA had difficulty tracking transactions through FACNET. Findings in prior Inspector General, DoD, audit reports on personnel security for automatic data processing (ADP) were directed to DISA, and DISA is taking corrective action on those findings; therefore, this report makes no additional recommendations. Because problems with ability to track transactions through FACNET are covered in more detail in our audit of EC/EDI trouble tickets, we are not making recommendations on that problem in this report.

Personnel Security. Key DISA technical personnel who work at FACNET gateways and network entry points did not have the sensitivity levels and security background checks required for those positions. Security requirements for personnel in ADP positions are established by DoD Directive 5200.2-R, "Personnel Security Program Regulations." Appendix K of that regulation establishes three security categories for computer and computer-related positions. The three categories are ADP-I, ADP-II, and ADP-III. The following are the criteria for assigning ADP personnel sensitivity levels, which depend on the degree of access to an automated information systems operations that an employee has.

o ADP-I (Critical-Sensitive Positions) are those positions in which the incumbent is responsible for the planning, direction, and implementation of a computer security program; has major responsibility for the direction, planning, and design of a computer system, including the hardware and software; or can access a system during the operation or maintenance with a relatively high risk for causing grave damage or for realizing a significant personal gain.

o ADP-II (Noncritical-Sensitive Positions) are those positions in which the incumbent is responsible for the direction, planning, design, operation, or maintenance of a computer system, and whose work is technically reviewed by a higher authority of the ADP category to ensure the integrity of the system.

o ADP-III (Nonsensitive Positions) are all other positions involved in computer activities.

DoD Directive 5200.2-R requires that those positions with sensitivity level ADP-I have favorable single scope background investigations. Compliance with

DoD Directive 5200.2-R had been reported in a prior audit report on DISA[1], and DISA has initiated but not completed corrective action on that finding.

Ability to Track Transactions Through FACNET. The existing FACNET system does not provide a reliable means to track transactions as they flow through the system. DISA technical staff generally must use manual research methods and UNIX-based file search utilities to research reports of lost or late transactions. UNIX is a computer operating system developed by Bell Laboratory that can be run on a variety of hardware architectures.

[1]Report No. 94-065, "Controls Over Operating System and Security Software Supporting the Defense Finance and Accounting Service," March 24, 1994.

Appendix D. Glossary

Digital Signature. Transformation of a message using cryptography so that a person having the initial message and signer's public key can accurately determine whether the transformation was created using the private key that corresponds to the signer's public key, and whether the initial message has been altered since the transformation was made.

Electronic Commerce. End-to-end, paperless business environment that integrates electronic transfer and automated business systems.

Electronic Data Interchange. Electronic data interchange, exchange of information without human intervention, using a standardized format.

Encryption. The process of transforming plaintext into ciphertext or enciphered data to prevent disclosure of the information.

FACNET. Federal Acquisition Computer Network. The development of FACNET was a requirement of the Federal Streamlining Act of 1994.

Firewall. A type of router that is placed between a network and the Internet to filter incoming and outgoing traffic to enhance network security.

Gateway. A device, for hardware or software, that converts one network's message protocol to the format used by another network. Used to connect the Government's procurement offices to the network.

Internet. The inter-working of existing corporate and Government networks using commonly used telecommunications standards; a collection of networks and gateways that uses the Transport Control Protocol/ Internet Protocol suite of protocols.

Modem. An acronym for modulator/demodulator. A hardware device that allows computers to communicate by telephone line.

Network Entry Point. FACNET computers used to connect the gateways to the value-added networks. FACNET network entry points are used to control the flow and routing of procurement transactions through the network. The two FACNET network entry points are located in Ogden, Utah, and Columbus, Ohio.

TCP/IP (Transmission Control Protocol over Internet Protocol). A collection of communication protocols used by most Internet applications.

Trading Partner. The sending and receiving parties in EDI transactions.

Value-added Network. A commercial communications network that supplies communication services, usually in the form of store and forward capability, to multiple users for transmitting information. Also provides application services (that is, electronic-mail) and related administrative services.

Appendix E. Electronic Data Interchange Transactions That Require Digital Signatures and Encryption Capabilities

American National Standards Institute X12 Transaction Type	Replaces Form	Digital Signature Required	Encryption Capability Needed
810 - Invoice	SF 1443 (Contractor's Request for Progress Payments)	Yes	No
824 - Application Advise		No	No
832 - Price Sales Catalog		No	No
836 - Contract Award Summary		No	No
838 - Trading Partner Profile		Yes	No
838 - Trading Partner Profile	SF 129 (Solicitation Mailing Application)	Yes	No
840 - Request for Quote	SF 18 and SF 33 (Request for Quote)	Yes	No
843 - Response to Request for Quote	SF 33 (Solicitation, Offer, and Award)	Yes	Yes
850 - Purchase Order, Delivery Order	DD 1155 (Purchase Order)	Yes	Yes
850 - Purchase Simple Contracts	SF 26 (Award/Contract)	Yes	Yes
855 - Purchase Order Acknowledgment		No	No
860 - Purchase Order Change	SF 30 (Amendment Of Solicitation/ Modification Contract)	Yes	No
864 - Text Message		No	No
865 - Purchase Order Change Acknowledgment		No	No
869 - Order Status Report		No	No
870 - Order Status Report		No	No
997 - Functional Acknowledgment		No	No

Appendix F. Organizations Visited or Contacted

Office of the Secretary of Defense

Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), Washington, DC
Deputy Under Secretary of Defense (Acquisition Reform)
Director, DoD Electronic Commerce

Defense Organizations

Defense Information Systems Agency, Arlington, VA
Defense Information Systems Agency, Western Hemisphere, Fort Ritchie, MD
Defense Megacenter, Columbus, OH
Defense Megacenter, Mechanicsburg, PA
Defense Megacenter, Ogden, UT
Headquarters, Defense Logistics Agency, Alexandria, VA
Defense Logistics Agency Software Design Center, Columbus, OH
National Security Agency, Fort Meade, MD

Air Force

Bolling Air Force Base, Washington, DC
Maxwell Air Force Base-Gunter Annex, Montgomery, AL

Non-Defense Federal Organizations

General Accounting Office, Washington, DC
National Institute of Standards and Technology, Gaithersburg, MD

Appendix G. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense for Acquisition and Technology
  Deputy Under Secretary of Defense (Acquisition Reform)
  Director, Defense Logistics Studies Information Exchange
Under Secretary of Defense (Comptroller)
  Deputy Chief Financial Officer
  Deputy Comptroller (Program/Budget)
Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
Assistant to the Secretary of Defense (Public Affairs)

Department of the Army

Assistant Secretary of the Army (Financial Management and Comptroller)
Auditor General, Department of the Army

Department of the Navy

Assistant Secretary of the Navy (Financial Management and Comptroller)
Auditor General, Department of the Navy

Department of the Air Force

Assistant Secretary of the Air Force (Financial Management and Comptroller)
Auditor General, Department of the Air Force

Other Defense Organizations

Director, Defense Contract Audit Agency
Director, Defense Information Systems Agency
Director, Defense Logistics Agency
Director, National Security Agency
  Inspector General, National Security Agency
Inspector General, Defense Intelligence Agency

Non-Defense Federal Organizations

Federal Electronic Commerce Acquisition Program Management Office
Office of Federal Procurement Policy, Office of Management and Budget,
Technical Information Center, National Security and International Affairs Division, General Accounting Office

Chairman and ranking minority member of each of the following congressional committees and subcommittees:

- Senate Committee on Appropriations
- Senate Subcommittee on Defense, Committee on Appropriations
- Senate Committee on Armed Services
- Senate Subcommittee on Acquisition and Technology, Committee on Armed Services
- Senate Committee on Governmental Affairs
- House Committee on Appropriations
- House Subcommittee on National Security, Committee on Appropriations
- House Subcommittee on Military Procurement, Committee on National Security
- House Committee on Government Reform and Oversight
- House Subcommittee on National Security, International Affairs, and Criminal Justice, Committee on Government Reform and Oversight
- House Committee on National Security

Part III - Management Comments

Defense Information Systems Agency Comments

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

IN REPLY REFER TO Inspector General

17 Jun 96

MEMORANDUM FOR INSPECTOR GENERAL, DEPARTMENT OF DEFENSE
ATTN: DIRECTOR, CONTRACT MANAGEMENT DIRECTORATE

SUBJECT: Draft Audit Report on Computer Security for the Federal Acquisition Computer Network (Project No. 5CA-3003)

Reference: DODIG Draft Audit Report, subject as above, 27 Mar 96

1. We reviewed subject report and concur in part with the findings and recommendations. We feel that recommendations A.2 and A.3 should be readdressed to DUSD (Acquisition Reform) because they have responsibility for enforcing digital signature and promulgating security policy.

2. Our management comments are enclosed which discuss corrective actions to be taken or actions already completed. My point of contact is Ms. Sandra J. Sinkavitch. If you require additional information, Ms. Sinkavitch may be reached on (703) 607-6316.

Philip D. Lavrete
for RICHARD T. RACE
Inspector General

Enclosure a/s

Quality Information for a Strong Defense

MANAGEMENT COMMENTS TO THE DOD INSPECTOR GENERAL DRAFT REPORT ON COMPUTER SECURITY FOR THE FEDERAL ACQUISITION COMPUTER NETWORK
PROJECT NO. 5CA-3003

RECOMMENDATION A.1: Approve a security plan, with milestones, that would provide digital signature and encryption capabilities to the Federal Acquisition Computer Network.

RESPONSE: Concur. DISA established the EDI Security Working Group for the purpose of addressing EDI Security Policy and development of the Security Implementation Plan following the guidelines of the DoD Directive 5000.2-R. The Security Implementation Plan consists of an Interim short-term solutions and the long-term plan with established milestones. This issue is also being addressed with the Federal Civilian Agencies to ensure adequate protection is provided to the entire Electronic Commerce/ Electronic Data Interchange environment.

RECOMMENDATION A.2: Limit the use of Federal Acquisition Computer Network to those transactions that do not require a signature under 31 U.S.C. 1501 or Federal Acquisition Regulation Section 4.101 until the Defense Information Systems Agency obtains a digital signature capability.

RECOMMENDATION A.3: Obtain a software encryption and digital signature capability for the Federal Acquisition Computer Network until DoD fully implements the Fortezza card.

RESPONSE A.2 and A.3: Defer to DUSD(AR).

The Principal Staff Assistant for Electronic Commerce in DOD is the DUSD(AR). Digital signature falls under DUSD(AR) responsibility and we defer to their judgement on this matter. DUSD(AR) should make the determination if digital signature is the correct and proper technical solution.

If it is determined that DOD should implement digital signature, given today's legal constraints, this would mean a tremendous cost and effort on behalf of the Functional User. The Functional User's Automated Information System(AIS) must acquire

the ability to do digital signature. Being that the digital signature must be applied after translation of the Functional User's AIS User Defined File (UDF) format to American National Institute (ANSI) X12 format (Functional User's AIS must perform the duties of the EDI Gateway). The AIS must incorporate the use of ANSI X12 address-routing to and from the NEP, which is currently the duty of the EDI Gateway. The AIS must also upgrade its backup and archiving procedures, in addition to the other services being performed by an EDI Gateway.

Under this approach the EDI Infrastructure would only be a transport mechanism, this will negatively affect the implementation of the future evolutions of the EDI Infrastructure. The problem with this approach is, it makes the assumption that all Functional User AIS's will do translation and the other functions of the EDI Gateway, this is false.

RECOMMENDATION B.1: Develop uniform backup procedures at the Federal Acquisition Computer Network gateways to maintain continuity of operations following a disaster or should the Federal Acquisition Computer Network become inoperative. Those backup procedures should include retention cycles that will satisfy minimum retention periods specified in the Federal Acquisition Regulations and by the National Archives and Records Administration' and of sufficient frequency to ensure recovery with minimum loss of data.

RESPONSE: Concur. DISA has begun the process to eliminate EDI gateways by evolving the EDI Infrastructure, therefore it is not cost effective to develop additional COOP procedures at this time. Under the new operational environment, standardized backup procedures are developed and will begin being testing 17 June 96.

RECOMMENDATION B.2: Store all backup data for the Federal Acquisition Computer Network in a secure location off site from the computer facility.

RESPONSE: Concur. DISA currently has procedures in place to store all backup data for EDI Infrastructure in a secure

location off site from the computer facility. Both NEPs transmit, via File Transfer Protocol (FTP), their data to one another, where the data is achieved and stored. Recommend closure.

RECOMMENDATION B.3: Establish backup facilities and procedures for each of the Federal Acquisition Computer Network gateways to ensure that DoD procuring offices and their trading partners are able to continue processing electronic commerce/electronic data interchange transactions during gateway failures.

RESPONSE: Concur. As mentioned in response B.1., DISA is in the process of collapsing the EDI gateway functionality into the Electronic Commerce Processing Node (ECPN). DOD procuring offices will communicate with their trading partners, via VANs, directly through the ECPN. DISA is currently establishing a COOP facility at Slidell, however, until the facility is fully operational, DISA will use the DISA Operational Support Facility (OSF) in Sterling, VA, to support COOP requirements.

RECOMMENDATION C.1: Implement the Class C2 controlled access protection for the Federal Acquisition Computer Network.

RESPONSE: Concur. ISA has implemented the required controlled access protection (Class C2), (Identification and Authentication, discretionary access control, audit, and object reuse). DISA is also working with the functional community to collect their security requirements which will be used to build the future phases of the EDI Infrastucture. DISA is currently updating its Security Certifications and Accreditations.

RECOMMENDATION C.2: Install firewall protection for the Federal Acquisition Computer Network.

RESPONSE: Concur. DISA established a firewall protection capability at the Ogden facility. However, DISA implemented an alternate security solution at Columbus. This solution includes a TCP/IP Wrapper, and Restricted Send-Mail Shell. A firewall is scheduled to be implemented as part of the upgrade to the EDI Infrastructure.

Audit Team Members

This report was prepared by the Contract Management Directorate, Office of the Assistant Inspector General for Auditing, DoD.

Paul J. Granetto
Kimberley A. Caprio
Kent E. Shaw
Young J. Jin
Johnetta R. Colbert
Robert E. Beets
William C. Coker
Awanda A. Grimes
Nancy C. Cipolla

INTERNET DOCUMENT INFORMATION FORM

A . Report Title: Computer Security for the Federal Acquisition Computer Network

B. DATE Report Downloaded From the Internet: 11/23/99

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

D. Currently Applicable Classification Level: Unclassified

E. Distribution Statement A: Approved for Public Release

F. The foregoing information was compiled and provided by:
DTIC-OCA, Initials: __VM__ **Preparation Date 11/23/99**

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