

~~FOR OFFICIAL USE ONLY~~

September 17, 2002



Information System Security

Defense Information Systems
Agency Defense Enterprise
Computing Center St. Louis
Information Security Program
(D-2002-148)

~~SPECIAL WARNING~~

~~This document contains information exempt from mandatory disclosure under the Freedom of Information Act.~~

~~This report contains certain unclassified information relating to the organization and function of the Defense Information Systems Agency Defense Enterprise Computing Center St. Louis that may be protected by 5 U.S.C. 522 (b)(2). Safeguards must be taken to prevent publication or improper disclosure of all information in the report.~~

Department of Defense
Office of the Inspector General

Quality

Integrity

Accountability

~~FOR OFFICIAL USE ONLY~~

Additional Copies

To obtain additional copies of this report, visit the Web site of the Inspector General of the Department of Defense 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 Future Audits

To suggest ideas for or to request future 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 of the 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

| | |
|---------|---|
| C & A | Certification and Accreditation |
| DECC | Defense Enterprise Computing Center |
| DFAS | Defense Finance and Accounting Service |
| DISA | Defense Information Systems Agency |
| DITSCAP | DoD Information Technology Security Certification and Accreditation Process |
| IG DoD | Inspector General of the Department of Defense |
| OMB | Office of Management and Budget |
| SSAA | System Security Authorization Agreement |



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

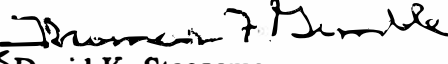
September 17, 2002

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE
(COMPTROLLER)/CHIEF FINANCIAL OFFICER
ASSISTANT SECRETARY OF DEFENSE (COMMAND,
CONTROL, COMMUNICATIONS, AND
INTELLIGENCE)
DIRECTOR, DEFENSE FINANCE AND ACCOUNTING
SERVICE
DIRECTOR, DEFENSE INFORMATION SYSTEMS
AGENCY

SUBJECT: Report on the Defense Information Systems Agency Defense Enterprise
Computing Center St. Louis Information Security Program
(Report No. D-2002-148)

We are providing this report for information and use. No written response to this report was required, and none was received. Therefore, we are publishing this report in final form.

We appreciate the courtesies extended to the staff. Questions should be directed to (b) (6) at (703) 604-(b) (6) (DSN 664-(b) (6)) or (b) (6) at (703) 604-(b) (6) (DSN 664-(b) (6)). See Appendix C for the report distribution. The team members are listed inside the back cover.


for David K. Steensma
Deputy Assistant Inspector General
for Auditing

~~Special Warning~~

~~This document contains information exempt from mandatory disclosure under the Freedom of Information Act.~~

~~This report contains certain unclassified information relating to the organization and function of the Defense Information Systems Agency Defense Enterprise Computing Center St. Louis that may be protected by 5 U.S.C. 552 (b) (2). Safeguards must be taken to prevent publication or improper disclosure of all information in this report.~~

~~FOR OFFICIAL USE ONLY~~

Office of the Inspector General of the Department of Defense

Report No. D-2002-148

September 17, 2002

(Project No. D2002FG-0058.007)

Defense Information Systems Agency Defense Enterprise Computing Center St. Louis Information Security Program

Executive Summary

Who Should Read This Report and Why? Defense Information Systems Agency (DISA) Defense Enterprise Computing Center St. Louis (DECC St. Louis) information security officials and anyone responsible for developing, implementing, and maintaining an information security program should read this report. This report discusses how the DECC St. Louis completed the certification and accreditation process and developed an information security program for its facility.

Background. DECC St. Louis is 1 of 18 consolidated information systems processing sites that houses, operates, and administers a diverse group of applications in support of the U.S. Transportation Command, the Army, the Marine Corps, and the Defense Finance and Accounting Service operations. Also, DECC St. Louis provides information technology services to the Defense Logistics Agency and the DISA Defense Information Technology Contracting Office. DECC St. Louis reports to the DISA Principal Director for Computing Services. DECC St. Louis uses mainframe and server-based platforms to house customer-designed applications used to process classified, unclassified but sensitive, and personnel (Privacy Act) information to support operations for its DoD customers. Specifically, DECC St. Louis provides support for DoD combat support activities such as logistics, supply, payroll, personnel, health, and transportation.

Results. DECC St. Louis developed an information security program and completed the certification and accreditation process for its facility. DECC St. Louis incorporated its information security program into the system security authorization agreement for its facility. The system security authorization agreement for DECC St. Louis included a current security plan, contingency plan, and risk assessment and management plan. In addition, DECC St. Louis implemented logical access and physical security controls. As a result, DECC St. Louis minimized the possibility that the operations of its DoD customers would be disrupted by information security risks to the mainframes, mid-tier systems, and networks at its facility.

Management Comments. We provided a draft of this report on August 12, 2002. No written response to this report was required, and none was received. Therefore, we are publishing this report in final form.

~~FOR OFFICIAL USE ONLY~~

Table of Contents

| | |
|--|----|
| Executive Summary | i |
| Background | 1 |
| Objectives | 2 |
| Findings | |
| Defense Information Systems Agency Defense Enterprise Computing Center St. Louis Information Security Program | 3 |
| Appendixes | |
| A. Scope and Methodology | |
| Scope | 10 |
| Methodology | 10 |
| B. Prior Coverage | 12 |
| C. Report Distribution | 13 |

Background

Accountability. Section 1061, title X, subtitle G, of the National Defense Authorization Act of Fiscal Year 2001 (Public Law 106-398) amends chapter 35 of title 44, United States Code to state in section 3535:

(a)(1) Each year each agency shall have performed an independent evaluation of the information security program and practices of that agency.

(2) Each evaluation by an agency under this section shall include--

(A) testing of the effectiveness of information security control techniques for an appropriate subset of the agency's information systems; and

(B) an assessment (made on the basis of the results of the testing) of the compliance with--

(i) the requirements of this subchapter; and

(ii) related information security policies, procedures, standards, and guidelines.

(3) The Inspector General or the independent evaluator performing an evaluation under this section may use an audit, evaluation, or report relating to programs or practices of the applicable agency.

(b)(1)(A) Subject to subparagraph (B), for agencies with Inspectors General appointed under the Inspector General Act of 1978 (5 U.S.C. [United States Code] App.) or any other law, the annual evaluation required under this section or, in the case of systems described under subparagraphs (A) and (B) of section 3532(b)(2), an audit of the annual evaluation required under this section, shall be performed by the Inspector General or by an independent evaluator, as determined by the Inspector General of the agency.

Defense Enterprise Computing Center St. Louis Responsibilities. Defense Enterprise Computing Center (DECC) St. Louis is 1 of 18 consolidated information systems processing sites including 5 DECCs and 13 DECC Detachments and is under the control of the Defense Information Systems Agency (DISA) Directorate for Computing Services. DECC St. Louis houses, operates, and administers a diverse group of applications in support of DoD combat support activities such as logistics, supply, payroll, personnel, health, and transportation. In addition, DECC St. Louis performs processing services for its DoD customers, including job classification, priority, and scheduling; workload balancing; equipment analysis and ordering; requirement analysis; output product distribution; and facilities planning. DECC St. Louis also

provides optional support services to its DoD customers including network management, communications, local area network, information assurance, and system administration and monitoring.

In addition, DECC St. Louis must ensure the confidentiality, integrity, and availability of the data entrusted to them for processing and storage. DECC St. Louis is responsible for ensuring that its security mechanisms are present and operational. DECC St. Louis is further responsible for the certification and accreditation of its hardware, operating system software, and communications systems. The DECC St. Louis customers are responsible for the certification and accreditation of their software applications operating on the platforms at DECC St. Louis.

Magnitude of DECC St. Louis Operations. DECC St. Louis supports DoD customers located worldwide. DECC St. Louis primary customers include the U.S. Transportation Command, the Army, the Marine Corps, and the Defense Finance and Accounting Service (DFAS). DECC St. Louis also provides information technology services to the Defense Logistics Agency and the DISA Defense Information Technology Contracting Office. DECC St. Louis processes data that supports the command and control software applications for the U.S. Transportation Command. The command and control mission for the U.S. Transportation Command would be jeopardized without effective support from DECC St. Louis. Additionally, DECC St. Louis processes all Marine Corps logistics, finance, and manpower applications. Further, DECC St. Louis processes all Army logistics and post, camp, and station infrastructure applications. Neither the Army nor the Marine Corps could mobilize or sustain operations without effective support from DECC St. Louis. DECC St. Louis also processes all data for DFAS applications that directly support the Army and Marine Corps functions. DFAS would be crippled without effective support from DECC St. Louis.

How DECC St. Louis Acquires Customers. DECC St. Louis is a fee-for-service operation. The DECC St. Louis customers are obligated to pay DECC St. Louis for the information technology services delivered in the Service-level agreement. The Service-level agreement describes the terms and conditions of the information technology services that the DECC St. Louis will provide to its customers. DECC St. Louis reviews the Service-level agreement annually, or as required by the customer.

Objectives

The audit objective was to assess the implementation of the Government Information Security Reform requirements of the Floyd D. Spence National Defense Authorization Act by DFAS and DECC St. Louis. See Appendix A for a discussion of the audit scope and methodology. See Appendix B for prior coverage related to the audit objective.

Defense Information Systems Agency Defense Enterprise Computing Center St. Louis Information Security Program

DECC St. Louis had developed an effective information security program for its facility. Specifically, the DECC St. Louis facility incorporated its information security program into a system security authorization agreement (SSAA). The program included:

- a security plan,
- a contingency plan, and
- a risk assessment and management plan.

In addition, DECC St. Louis had implemented logical access and physical security controls.

DECC St. Louis established an effective information security program because it complied with the information security policies and completed the certification and accreditation (C & A) process.

As a result, the DECC St. Louis facility minimized the possibility that the operations of the U. S. Transportation Command, the Army, the Marine Corps, and DFAS would be disrupted by information security risks to the mainframes, mid-tier systems, and networks at its facility.

Information Security Policy

Office of Management and Budget Guidance. Office of Management and Budget (OMB) Circular A-130, Revised, "Management of Federal Information Resources," November 30, 2000, prescribes policies and standards for protecting Government information. DoD must ensure that risks and the potential for loss are understood and continually assessed. DoD must also take steps to minimize risk and ensure that controls are implemented and remain effective over time.

DoD Directive 5200.28. DoD Directive 5200.28, "Security Requirements for Automated Information Systems," March 21, 1988, applies to all automated information systems, including stand-alone systems, communications systems, and computer systems of all sizes. The Directive specifically states that an automated information system accreditation should be accomplished and supported by a certification plan, a risk analysis of the automated information system in its operational environment, an evaluation of the security safeguards, and a certification report. It also states that the Designated Approving Authority should approve the documents supporting each accreditation.

DoD Instruction 5200.40. DoD Instruction 5200.40, “DoD Information Technology Security Certification and Accreditation Process (DITSCAP),” December 30, 1997, implements a standard approach for protecting and securing DoD information systems. The Instruction also provides procedures for accomplishing the C & A process established in DoD Directive 5200.28. The DITSCAP is applicable during all life-cycle phases to any DoD system that collects, stores, transmits, or processes unclassified or classified information. The DITSCAP procedures identify four life-cycle phases consisting of definition, verification, validation, and post accreditation. In addition, the DITSCAP delineates the responsibilities of the Designated Approving Authority, information systems security officer, program manager, and certification authority as essential to the DITSCAP process.

DoD Manual 8510.1. DoD Manual 8510.1-M, “DoD Information Technology Security Certification and Accreditation (DITSCAP) Application Manual,” July 31, 2000, is a stand-alone reference manual. This Manual supports the DITSCAP by providing a detailed approach to the activities that must be done in order to complete the C & A process. The Manual also provides the minimum requirements needed for a complete SSAA.

System Security Authorization Agreement

DECC St. Louis developed an information security program and incorporated the information security program into the SSAA for its facility. OMB Circular No. A-130 requires Federal agencies to implement and maintain an information security program to ensure that adequate security is provided for all agency information collected, processed, transmitted, stored, or disseminated in general support systems and major applications. OMB Circular No. A-130 further requires Federal agencies to complete a security plan for general support systems and major applications. DoD Directive 5200.28 requires that DoD Components and Defense agencies complete and test the contingency plan for an information system to ensure that the security controls function reliably and that adequate back-up functions are maintained continuously during interrupted service.

DoD Manual 8510.1 requires that the DoD Components and Defense agencies complete the following tasks during their C & A process:

- to complete a contingency plan and risk management review during the validation phase of the C & A process for their information systems;
- to assess the vulnerabilities against the documented threat, the ease of exploitation, the potential rewards, and the probability of occurrence during their risk management review for information systems;
- to evaluate the operational procedures and safeguards and their ability to offset risks in order to determine their effectiveness for information systems;

-
- to document the results of the contingency plan evaluation and the risk management review in the SSAA for information systems; and
 - to use the SSAA to fulfill the requirements of the security plan.

Security Plan. DECC St. Louis completed a facility security plan on January 20, 2001. Officials at DECC St. Louis stated that the security plan was updated when the C & A package was submitted to the designated approving authority in January 2002. The security plan for DECC St. Louis provided an overview of the security requirements of the facility and described the controls and procedures in place that met the identified security requirements. Officials at DECC St. Louis stated that the DISA Field Security Operations conducted a security readiness review of DECC St. Louis to monitor its security requirements and procedures. DISA Field Security Operations ensured that DECC St. Louis implemented the new security requirements based upon the results of the security readiness review.

OMB Circular A-130 requires Federal agencies to complete a security plan. The security plan includes responsibilities and expected behavior of all individuals with access to the system, consequences when the behavior is not consistent with the expected behavior included in the security plan, and training requirements for individuals with access to the system. The security plan for DECC St. Louis identified the responsibilities of and the training requirements for information security officials such as the security manager, information system security manager, and the information system security officer.

Contingency Plan. DECC St. Louis completed a Business Continuity Plan for its facility. The Business Continuity Plan acts as the contingency plan for the DECC St. Louis facility. Officials at DECC St. Louis stated that its Business Continuity Plan was updated on March 4, 2002. The Business Continuity Plan for DECC St. Louis documented emergency response and back-up and recovery procedures for the facility. DoD Directive 5200.28 requires that the contingency plan for an information system be tested. In August 2001, DECC St. Louis and one of its customers, the Army Aviation and Missile Command located at Redstone Arsenal, Huntsville, Alabama, conducted a test of the continuity of the operations plan for seven Army Aviation and Missile Command applications. In addition, DISA Computing Services Operations-Denver/Assured Computing (DISA Computing Services Operations) reviewed and graded the DECC St. Louis Business Continuity Plan in January 2002 to ensure that the plan conformed to the template specified by DISA Computing Services Operations. This review was the first review for DECC St. Louis using the new Business Continuity Plan format. DECC St. Louis scored an average of 74 percent success rate during the DISA Computing Services Operations review. During the prior year review, DECC St. Louis scored 98 percent success rate using the old Business Continuity Plan format. Officials at DECC St. Louis stated that the 24 percent difference in the score resulted from DECC St. Louis and DISA Computing Services Operations adapting to the new requirements in the Business Continuity Plan format.

Risk Assessment and Management Plan. DISA Field Security Operations completed a risk assessment for DECC St. Louis in January 2001. DoD Manual 8510.1 requires that a risk management review be completed, which includes an assessment of the threats and vulnerabilities for an information system. DISA Field Security Operations completed a threat assessment and a vulnerability assessment during the risk assessment. DISA Field Security Operations documented the results of the threat and vulnerability assessments in the DECC St. Louis SSAA. DISA Field Security Operations identified threats to the DECC St. Louis. OMB Circular A-130 requires that DoD take steps to minimize risk and ensure that controls are implemented and remain effective over time. The DISA Field Security Operations identified risks to DECC St. Louis and also identified the security improvements and risk mitigation controls that were implemented at the facility to manage the residual risks.

In addition, DoD Manual 8510.1 requires that a cost benefit analysis be completed to identify the appropriate countermeasures to mitigate the risks to an information system. The DISA Field Security Operations did not complete a cost versus risk analysis for DECC St. Louis. Officials at DECC St. Louis stated that a cost versus risk analysis was not completed for its facility because no countermeasures were identified for DECC St. Louis that required a funding decision. OMB Circular A-130 requires that DoD continually assess risks. The Circular does not establish when or how often a Component should perform a risk assessment. Therefore, officials at DECC St. Louis believed that the facility satisfied the OMB requirement because the DECC St. Louis performs risk assessments as part of the C & A process for the facility, which occurs every three years.

Implementation of Logical Access and Physical Security Controls

DECC St. Louis had implemented logical access and physical security controls at its facility. DoD Directive 5200.28 requires that the DoD Components and Defense agencies implement safeguards for information systems to detect and prevent unauthorized disclosure, destruction, or modification of data. DoD Directive 5200.28 further requires that the DoD Components and Defense agencies implement physical security controls to protect the hardware, software, and documentation for an information system, and all classified and sensitive unclassified data handled by the information system.

Logical Access Controls. DECC St. Louis had implemented logical access controls to protect its mainframe and mid-tier systems from adverse information security risks. For example, DECC St. Louis used security software packages to detect and prevent unauthorized access to its network and to the software applications operating on the DECC St. Louis mainframes. In addition, DECC St. Louis had established a decentralized information security administration structure. DECC St. Louis employed six full-time information system security officers to oversee the mainframes. DECC St. Louis required the information system security officers at its facility to monitor the activities of individuals with access to the software applications operating on the mainframes. If the information system security officers at DECC St. Louis detected a security

violation, the information system security officers were required to follow the standard operating procedures for reporting security violations established in the "DISA Western Hemisphere Handbook," December 1, 2000.

DECC St. Louis required its Army, Marine Corps, and DFAS customers to appoint security administrators at their field locations to monitor the activities of individuals with access to the software applications operating on the DECC St. Louis mainframes. The security administrators were responsible for assigning and deactivating access to the software applications. The information system security officers at DECC St. Louis were responsible for assigning and deactivating access to the software applications for the Army, Marine Corps, and DFAS security administrators.

Both Government civilian and contractor personnel occupied the information systems security officer positions at DECC St. Louis. The information system security officer positions are designated as Automatic Data Processing-I¹ and are critical-sensitive. The information system security officers at DECC St. Louis had access to the security software packages, which controlled entry to the software applications operating on its mainframes. In addition, the DECC St. Louis information system security officers had access to the development and production portions of the software applications operating on its mainframes. However, the information systems security officers did not develop, maintain, or upgrade the software applications operating on the DECC St. Louis mainframes. DoD Regulation 5200.2, "DoD Personnel Security Program," January 1987, requires DoD military, civilian, consultants, and contractor personnel occupying information systems positions designated as Automatic Data Processing-I, II², and III³ to undergo a security investigation. DECC St. Louis required its information systems security officers to undergo a background investigation and to hold at least a secret clearance before the Headquarters, DISA Security Office authorized them to perform duties designated Automatic Data Processing-I.

Physical Security Controls. DECC St. Louis had implemented physical security controls to protect its systems and facility. For example, access to the facility was controlled by security guards, personnel identification badges, and alarmed entry and exit door devices. DECC St. Louis also maintained audit trails of personnel accessing its facility and controlled the number of visitors to its facility by requiring pre-scheduled visits. Visitors to the facility were

¹ Automatic Data Processing-I position is designated critical-sensitive. The incumbent is responsible for the direction, planning, and design of a computer system, including the hardware and software. In addition, the incumbent can access a system during operation or maintenance in such a way as to cause grave damage or realize a significant personal gain. Automatic Data Processing-I positions require the highest security and education standards for the incumbent.

² Automatic Data Processing-II position is a non-critical sensitive position in which the incumbent has a degree of access to a system that creates a significant potential for damage or personal gain but less than that in an Automatic Data Processing-I position.

³ Automatic Data Processing-III position is a non-sensitive position that involves all other Federal computer activities not designated as Automatic Data Processing-I and II.

required to have an escort at all times. Officials at DECC St. Louis stated that the DISA Field Security Operations performs annual security readiness reviews of the access and physical security controls. DISA Field Security Operations performed the last security readiness review of DECC St. Louis in February 2001.

Certification and Accreditation Process

DECC St. Louis had an effective information security program because they had complied with the information security policies. DECC St. Louis performed a level-three⁴ certification analysis for its facility, which included:

- a detailed analysis of its information systems and networks,
- an information system security analysis,
- a vulnerability assessment,
- a risk assessment analysis,
- a system security architecture study,
- an operations security review, and
- a network penetration test.

In January 2002, the DISA Chief Information Officer, who acts as the Designated Approving Authority for DISA, granted the DECC St. Louis facility a site accreditation. Officials at DECC St. Louis stated that the site accreditation was based upon the classification of the information processed at the facility. Officials at DECC St. Louis further stated that the site accreditation granted by the DISA Chief Information Officer allowed DECC St. Louis to operate any system at or below the secret classification level. DECC St. Louis processed classified, unclassified but sensitive, and personnel (Privacy Act) information. The DECC St. Louis site accreditation did not include the software applications provided by its customers. The Service-level agreement between DECC St. Louis and its customers specifically stated that the DECC St. Louis customers were responsible for the certification and accreditation of their information systems, while the DECC St. Louis was responsible for the C & A of the hardware, operating systems, and communications systems at its facility.

⁴ A level-three certification analysis is a detailed analysis on the business functions, security requirements, mission criticality, software, computer infrastructure, data processed, and types of users for an information system to determine the degree of confidentiality, integrity, availability, and data necessary to protect the system.

Impact of Information Security Program on Business Operations

DECC St. Louis minimized the possibility that the U.S. Transportation Command, the Army, the Marine Corps, and DFAS operations would be disrupted by information security risks to its mainframe, mid-tier systems, and networks. DECC St. Louis completed a detailed analysis of the information systems and networks at its facility during the C & A process. DECC St. Louis identified risks to the mainframes, mid-tier systems, and networks at its facility that would affect the availability, integrity, and confidentiality of its systems. If the DECC St. Louis had not established an information security program and completed the C & A process, DECC St. Louis would not have been aware of the information security risks to its mainframes, mid-tier systems, and networks. For example, the DISA Field Security Operations determined that unauthorized access to the local area network at DECC St. Louis could interfere with the ability of its facility to continue operations. The U.S. Transportation Command, the Army, the Marine Corps, and DFAS relies on DECC St. Louis to support their missions and the DoD warfighter. Loss of operations at DECC St. Louis could jeopardize the command and control mission of the U.S. Transportation Command. In addition, neither the Army nor the Marine Corps could mobilize or sustain operations without effective support from DECC St. Louis. A loss of operations at DECC St. Louis would also cripple DFAS operations. DECC St. Louis minimized the risk to its local area network through the implementation of logical access controls such as user identification and passwords.

Summary

DECC St. Louis had developed an information security program at their facility. The facility needed to have an information security program that would ensure continued operations even under the most stressed conditions because a loss of operations at DECC St. Louis could prevent the DoD customers and warfighters from accomplishing their missions. Furthermore, DECC St. Louis evaluated the adequacy of its information security program during its C & A process and identified risks that could affect the availability, confidentiality, and integrity of its information systems. DECC St. Louis had implemented security improvements and risk mitigation controls to manage the identified risks. In addition, DECC St. Louis established a contingency plan documenting the emergency response and back-up and recovery procedures. Finally, DECC St. Louis implemented logical access and physical security controls to safeguard the mainframes, mid-tier systems, and the software applications operating on mainframes at that facility from unauthorized disclosure, destruction, or modification.

Appendix A. Scope and Methodology

Scope

Work Performed. The overall audit objective was to assess implementation of the Government Information Security Reform requirements of the Floyd D. Spence National Defense Authorization Act by DFAS. However, we also conducted audit fieldwork at DECC St. Louis because several of the systems included in our audit operate on mainframes located at the DECC St. Louis. We interviewed personnel at the DECC St. Louis such as the Chief of the Security Division, the Information Systems Security Manager, the Information System Security Officers, the Continuity of Operations Coordinator, the Chief of the Financial Management Division, and the Chief of the Customer Support and Marketing Division.

We evaluated the DECC St. Louis information security program, which included, the C & A process, logical access controls, risk assessment and management plan, security plan, physical security controls, and contingency/disaster recovery plans. We reviewed the DECC St. Louis SSAA dated November 2001, which included the risk analysis dated January 20, 2001, security plan dated January 20, 2001, and Business Continuity Plan dated March 4, 2002. We reviewed the DECC St. Louis C & A statements dated January 11, 2002, and analyzed the DECC St. Louis Physical Security Review dated February 2001. In addition, we reviewed samples of audit logs, the statement of work for DECC St. Louis On-Site Contractor Technical Support dated February 6, 2002, and security investigations for contractor personnel occupying critical-sensitive information systems positions.

Limitations to Scope. We did not review the management control program related to the overall audit objective because DoD recognized information assurance as a systemic control weakness in its FY 2000 Statement of Assurance.⁵

General Accounting Office High-Risk Area. The General Accounting Office has identified several high-risk areas in DoD. This report provides coverage of the Information Security high-risk area.

Methodology

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

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

⁵ FY 2000 was the last Statement of Assurance issued by the Department of Defense.

Audit Dates and Standards. We performed this audit from March 2002 through July 2002 in accordance with generally accepted government auditing standards.

Contacts During the Audit. We visited or contacted individuals and organizations within DoD.

Appendix B. Prior Coverage

Inspector General of the Department of Defense (IG DoD)

IG DoD Report No. D-2002-134, "Implementation of Government Information Security Reform by the Defense Finance and Accounting Service Nonappropriated Fund Information Standard System," July 24, 2002

IG DoD Report No. D-2002-132, "Implementation of Government Information Security Reform by the Defense Finance and Accounting Service for the Civilian Personnel Resource Reporting Systems," July 23, 2002

IG DoD Report No. D-2002-015, "Summary of Security Control Audits of DoD Financial and Accounting Systems," November 7, 2001

IG DoD Report No. D-2001-184, "FY 2001 DoD Information Security Status for Government Information Security Reform," September 19, 2001

IG DoD Report No. D-2001-183, "Implementation of DoD Information Security Policy for Processing Accomplished at Defense Enterprise Computing Centers," September 19, 2001

IG DoD Report No. D-2001-182, "Information Assurance Challenges—A Summary of Results Reported April 1, 2000, Through August 22, 2001," September 19, 2001

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)

Department of the Army

Assistant Secretary of the Army (Financial Management and Comptroller)
Auditor General, Department of the Army
U. S. Army Audit Agency

Department of the Navy

Naval Inspector General
Auditor General, Department of the Navy
Naval Audit Service

Department of the Air Force

Auditor General, Department of the Air Force

Unified Command

Commander, U.S. Transportation Command

Other Defense Organizations

Director, Defense Finance and Accounting Service
Director, Defense Information Systems Agency
Principal Director for Computing Services
Inspector General, Defense Information Systems Agency

Non-Defense Federal Organizations

Office of Management and Budget
Office of Information and Regulatory Affairs

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member

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

Team Members

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

(b) (6)
[Redacted]