August 30, 2002

# Information System Security

## Government Information Security Reform Act Implementation: Defense Security Assistance Management System
(D-2002-142)

Department of Defense
Office of the Inspector General

*Quality* *Integrity* *Accountability*

**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**

| | |
|---|---|
| ASD($C^3$I) | Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) |
| DECC | Defense Enterprise Computing Center |
| DISA | Defense Information Systems Agency |
| DITSCAP | DoD Information Technology Security Certification and Accreditation Process |
| DSAMS | Defense Security Assistance Management System |
| DSCA | Defense Security Cooperation Agency |
| GISR | Government Information Security Reform |
| SSAA | System Security Authorization Agreement |

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

August 30, 2002

MEMORANDUM FOR ASSISTANT SECRETARY OF DEFENSE (COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE)
DIRECTOR, DEFENSE SECURITY COOPERATION AGENCY

SUBJECT: Report on Government Information Security Reform Act Implementation: Defense Security Assistance Management System (Report No. D-2002-142)

We are providing this report for information and use. This audit was conducted in accordance with the provisions of the Government Information Security Reform Act, title X, subtitle G of the Floyd D. Spence National Defense Authorization Act for FY 2001, October 30, 2000 (Public Law 106-398).

We appreciate the courtesies extended to the audit staff. For additional information on this report, please contact Mr. Tilghman A. Schraden at (703) 604-9186 (DSN 664-9186) (tschraden@dodig.osd.mil) or Ms. Kathryn L. Palmer at (703) 604-8840 (DSN 664-8840) (kpalmer@dodig.osd.mil). See Appendix C for the report distribution. Audit team members are listed inside the back cover.

for David K. Steensma
Deputy Assistant Inspector General
for Auditing

## Office of the Inspector General of the Department of Defense

**Report No. D-2002-142** **August 30, 2002**
(Project No. D2002LD-0100)

# Government Information Security Reform Act Implementation: Defense Security Assistance Management System

## Executive Summary


**Who Should Read This Report and Why?** DoD personnel who are involved in implementing Government Information Security Reform Act (GISRA Act) requirements should read this report. The report discusses our independent assessment of the information security posture of the Defense Security Assistance Management System, a Defense Security Cooperation Agency system.

**Background.** To gather data on assessments of the effectiveness of DoD information assurance policies, procedures, and practices, DoD developed a GISR Act collection matrix for automated information systems. DoD selected a sample of 560 automated information systems from the almost 4,000 automated information systems in DoD. For those 560 systems, DoD reported the aggregate results of the assessments for FY 2001 in "GISR Report FY01: Government Information Security Reform Act, Report of the Department of Defense," October 2001. Of the 560 systems, the Office of the Inspector General of the Department of Defense, the Defense Information Systems Agency Inspector General, and Military Department audit agencies assessed a sample of 115 systems. This report is one in a series of GISR Act audits and is an assessment of the Defense Security Assistance Management System. The Defense Security Assistance Management System is a mission-essential system developed to produce and track security assistance-related contractual documents (sales agreements between governments).

**Results.** In our assessment of the Defense Security Assistance Management System, the Defense Security Cooperation Agency implementation of GISR Act requirements, as reported in the GISR Act collection matrix for FY 2001, was generally accurate as of August 1, 2001, the date of the FY 2001 collection matrix data, with the exception of one response regarding hardware and system software maintenance plans. Additionally, there was an outstanding issue related to personnel security that had been addressed in Inspector General of the Department of Defense Report No. D-2001-141, "Allegations to the Defense Hotline on the Defense Security Assistance Management System," June 19, 2001. We found that contractor employees were continuing development work on Defense Security Assistance Management System software while their security clearances were pending. Although 1 of the 32 responses provided in the collection matrix was inaccurate, we concluded that the Defense Security Cooperation Agency was following the standard DoD process to certify and accredit the system. As a result, the Defense Security Cooperation Agency was making progress toward achieving full information security accreditation for the Defense Security Assistance Management System. For details on the audit results, see the Finding section of the report.

**Management Comments.** We provided a draft of this report on August 1, 2002. No written response to this report was required, and none was received. Therefore, we are publishing this report in final form.

# Table of Contents

**Executive Summary** i

**Background** 1

**Objectives** 3

**Finding**

Defense Security Assistance Management System Information Security 4

**Appendixes**

A. Scope and Methodology 13
Prior Coverage 14
B. Government Information Security Reform Act Collection Matrix Submission 15
C. Report Distribution 23

## Background

**Government Information Security Reform.** On October 30, 2000, the President signed the Floyd D. Spence National Defense Authorization Act for FY 2001 (Public Law 106-398), which includes title X, subtitle G, the "Government Information Security Reform" (GISR Act). Subtitle G directs that the Government ensure effective controls for highly networked Federal information resources; management and oversight of information security risks; and a mechanism for improved information system security oversight and assurance for Federal information security programs. The GISR Act directs each Federal agency (DoD for purposes of this report) to annually evaluate its information security program and practices and, as part of the budget process, submit the results of the evaluation to the Office of Management and Budget. The GISR Act covers both unclassified and national information security systems and creates a comparable security management framework for each. The GISR Act also requires that the agency Inspector General or other independent agent evaluate the agency information security program and practices. Also, the GISR Act requires each agency Inspector General or other independent agency to select and test a subset of systems that will confirm the effectiveness of the information security programs.

**DoD Responsibilities.** The GISR Act directs DoD to annually evaluate its information security program and practices. The DoD uses information technology for thousands of processes that are integral to support and operational functions. Mission-critical, mission-essential, and support-function processes, or applications, reside on computer systems throughout DoD. Applications for the DoD Components include financial accounting; personnel; pay and disbursement; materiel shipping, receiving, and storing; munitions maintenance; and weapon systems-associated applications.

The GISR Act directs that DoD as part of the budget process submit the results of its annual evaluation to the Office of Management and Budget. Office of Management and Budget guidance, memorandum 01-24, "Reporting Instructions for the Government Information Security Reform Act," June 22, 2001, directs the Secretary of Defense to transmit the FY 2001 annual evaluation of information security program and practices to the Office of Management and Budget by October 1, 2001. The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) (ASD[$C^3$I]) formed and chaired an Integrated Process Team to develop and finalize the guidance and methodology for DoD reporting of the GISR Act. The GISR Act Integrated Process Team developed a 32-column spreadsheet--GISR Act collection matrix--to gather data on assessments of the effectiveness of DoD information assurance policies, procedures, and practices. DoD required the FY 2001 GISR Act collection matrix data completion as of August 1, 2001.

**Inspector General Responsibilities.** Office of Management and Budget issued memorandum 01-08, "Guidance on Implementing the Government Information Security Reform Act," in January 2001 to provide implementation instructions for Federal agencies in carrying out the GISR Act. Guidance specific to the duties of each Inspector General as an independent evaluator was also included in that memorandum. The Office of Management and Budget guidance states that each

Inspector General or independent evaluator "should perform an annual evaluation of the agency's security program and practices. This testing includes testing the effectiveness of security controls for an appropriate subset of agency systems." Although the GISR Act applies to all Government information systems, the Office of Management and Budget acknowledged that agencies could not review all of those systems every year. As a result, the independent evaluation should identify and assess a logical representative sampling of systems that can be used to form the basis of a conclusion regarding the effectiveness of an agency's overall security program.

**DoD Systems.** The Office of the Inspector General of the Department of Defense developed a stratified random sample from the population of automated information systems the DoD evaluated and reported for FY 2001 in the "GISR Report FY01: Government Information Security Reform Act, Report of the Department of Defense," October 2001 (DoD GISR Act Report). DoD selected and reported in the DoD GISR Act Report on a sample of 560 automated information systems from the almost 4,000 systems listed in the DoD Information Technology Registry.[1] The Office of the Inspector General of the Department of Defense stratified random sample included 115 systems from the universe sample of 560 systems that were reported on in the DoD GISR Act Report. The audit agencies for the Military Departments and the Defense Information Systems Agency (DISA) Inspector General were to evaluate 91 of the 115 information systems in the sample by August 2, 2002. The Office of the Inspector General of the Department of Defense was to evaluate the remaining 24 systems that support DoD agencies and activities. This report discusses the evaluation of 1 of the 24 DoD-level systems, the Defense Security Assistance Management System (DSAMS).

**DoD Information Security Program.** DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)," December 30, 1997, provides the procedures for certification and accreditation of information technology to include information systems, networks, and sites in DoD. It also assigns responsibilities for oversight and implementation of the certification and accreditation process. DITSCAP is to be used as guidance throughout the certification and accreditation process. DoD Manual 8510.1-M, "Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual," July 2000, provides implementation guidance that standardizes the certification and accreditation process throughout DoD.

[1]The Information Technology Registry was established in response to requirements contained in section 8102(a) of the National Defense Appropriation Act for FY 2001 and section 811(a) of the National Defense Authorization Act for FY 2001. The DoD registry must contain all of the fielded mission-critical and mission-essential systems as well as all the mission-critical and mission-essential systems that are in development.

## Objectives

Our overall audit objective was to assess DSAMS for implementation of the GISR Act requirements of the Floyd D. Spence National Defense Authorization Act for FY 2001. See Appendix A for a discussion of the audit scope and methodology and for prior coverage.

# Defense Security Assistance Management System Information Security

Data reported for DSAMS in support of the implementation of the GISR Act requirements for FY 2001 were generally accurate as of August 1, 2001, with the exception of one response regarding hardware and system software maintenance plans. Additionally, there was an outstanding issue related to personnel security that had been addressed in Inspector General of the Department of Defense Report No. D-2001-141, "Allegations to the Defense Hotline on the Defense Security Assistance Management System," June 19, 2001. We found that contractor employees were continuing development work on DSAMS software while their security clearances were pending. However, the Defense Security Cooperation Agency (DSCA)[2] was following DITSCAP to certify and accredit DSAMS. As a result, DSCA was making progress in achieving full information security accreditation for DSAMS.

## Defense Security Cooperation Agency Mission

DSCA provides direction, supervision, and oversight of security cooperation programs in support of U.S. national security and foreign policy objectives. As part of that mission, DSCA manages foreign military sales requests, approvals, funding, payments, and transfers. DSAMS is the automated information system that supports foreign military sales management for DSCA and the Military Departments.

## System Background

DSAMS is a mission-essential[3] system developed to produce and track security assistance-related contractual documents (sales agreements between governments). By FY 2004, the DSAMS Program Office expects that DSAMS will also handle planning and execution of security assistance training. DSAMS was originally planned to replace 13 legacy systems operating within DSCA, the Defense Finance and Accounting Service, and the Military Departments. The first module of DSAMS was deployed in February 1998 to the Naval Inventory Control Point, Philadelphia, Pennsylvania; the Navy International Programs Office, Arlington, Virginia; and the Naval Education and Training Security Assistance Field Activity, Pensacola, Florida. The Army began use of DSAMS in December 1998, and the Air Force began use in July 1999. The Defense Finance and Accounting Service became actively engaged with the deployment of the second DSAMS module in August 2000. As of March 2002, DSAMS was installed at 67 user sites.

[2]DSCA is the program office for DSAMS and is responsible for the continued development and maintenance of the system.

[3]Mission-essential systems are those systems that are basic and necessary for the accomplishment of an organization's mission.

**System Configuration.** DSAMS uses client and server architecture,[4] and users access DSAMS through a personal computer, software components installed at the user's site, and the Non-Secure Internet Protocol Router Network connection. The DSAMS application and database reside on a server located at the DISA Defense Enterprise Computing Center (DECC), Oklahoma City, Oklahoma, and employs an Oracle database structure.

**System Operations.** DSAMS is an unclassified system but contains sensitive data, such as information about foreign customers' contracts for materiel and services procured from the U.S. Government. DSAMS was originally planned to facilitate a full life-cycle management system for security assistance-related documents.

## Data Collection Matrix

DSCA provided the response for the DSAMS to ASD($C^3$I) as of August 1, 2001, and the data reported were generally accurate. In response to the GISR Act requirement for each Federal agency to annually evaluate and report on its information security program and practices, ASD($C^3$I) developed a GISR Act data collection matrix (the matrix) for DoD. The Assistant Secretary developed the matrix as a management tool to track information assurance trends and outcomes. The matrix consisted of a spreadsheet divided into four sections for data. Section titles included identifying information, accreditation information, assessment criteria information, and operations and assessments interest items.

In response to the information requested in the matrix, DSCA was generally required to answer yes, no, or provide a date for action completed. With the exception of a special section that could be used for augmenting comments, no other explanation was required or expected. A discussion of each section of the matrix, the data that DSCA reported in the matrix for DSAMS, and our analysis of the data follows. Appendix B contains the information for DSAMS that was reported in the matrix that ASD($C^3$I) used for the DoD GISR Act Report.

**Identifying Information.** DSCA was requested to provide the system or network name, acronym, component owner, and information technology classification (mission critical or mission essential) in the identifying information section of the matrix. DSCA responded in the matrix that DSAMS was classified as a mission-essential information technology system. We verified that the identification information in the matrix was correct as stated in the DoD Information Technology Registry.

**Accreditation Information.** DSCA was requested to provide in the accreditation information section of the matrix the date of accreditation certification, the date of interim certification, the accreditation method, and whether formal documentation for certification and accreditation existed.

[4]Client and server architecture is an arrangement in which some software components reside on a central server and other software components reside on a client's personal computer or workstation separate from the main server.

**Accreditation Date.** DSCA was requested to provide the date that an accreditation process accredited DSAMS. DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)," March 21, 1988, establishes the minimum security requirements for DoD automated information systems. DITSCAP implements the Directive, assigns responsibility, and prescribes procedures for certification and accreditation. DSCA responded in the matrix that DSAMS was not accredited. We verified that the DSCA response was appropriate. DSCA was working on accrediting DSAMS and its goal was to have DSAMS accredited by the end of calendar year 2002.

**Interim Certification Date.** DSCA was requested to provide the date that an interim authority to operate was granted. According to the provisions of DITSCAP, interim authority should be based on the establishment of an acceptable level of risk in operating the system. DSCA responded in the matrix that an interim authority to operate had not been granted for DSAMS. We verified that DSAMS had been operating since calendar year 1998 without accreditation or interim authority to operate. However, on June 13, 2002, DSCA was granted a 180-day interim authority to operate DSAMS from the DSAMS Designated Approval Authority, the Deputy Director of DSCA. DSCA planned to complete the DSAMS certification and accreditation process prior to the expiration of the 180-day interim authority.

**Accreditation Method.** DSCA was requested to identify whether DSAMS was accredited under DITSCAP and, if not under DITSCAP, to describe other accreditation and certification procedures. Several policies govern actions of DSAMS program officials, but DITSCAP is the principal governing document for risk assessment and mitigation of DoD information technology systems. DITSCAP establishes the oversight mechanism that ensures identification of appropriate information to certify, accredit, and maintain a program's security. DSCA responded in the matrix that DSAMS was not accredited under DITSCAP or any other procedures. We verified that DSCA was following DITSCAP procedures to accredit and certify DSAMS but, as of August 1, 2001, DSAMS was not accredited. DSCA plans to receive DITSCAP accreditation by the end of calendar year 2002.

**Certification and Accreditation Documentation.** DSCA was requested to identify whether formal documentation existed that the Inspector General of the Department of Defense or other entities could use to verify accreditation. DITSCAP requires a System Security Authorization Agreement (SSAA) for each information technology system. The SSAA is a formal and binding document among the system program manager, the Designated Approving Authority, the Certifying Authority, and the user representative that establishes the level of security required. The SSAA guides the process and documents the results for certification and accreditation as well as implementation of information technology security requirements. DSCA responded in the matrix that it did not have formal documentation in effect for the DSAMS certification and accreditation process. We confirmed that DSCA had not formally documented the DSAMS certification and accreditation process with an SSAA. However, some of the plans, policies, and procedures normally included in an SSAA existed. DSCA planned to complete the development of the SSAA during the 180-day interim authority to operate.

**Assessment Criteria Information.** DSCA was requested to confirm that information assurance controls and plans in the assessment criteria information section of the matrix existed. According to the instructions provided for the matrix, ASD($C^3I$) developed the assessment criteria information section to assess selected systems on the basic program management, controls, and procedures that exist as part of the operation of the system.

**Access Controls.** DSCA was requested to identify whether access controls were in place. ASD($C^3I$) defined access controls as controls that limited access of information system resources to authorized users, programs, processes, or other systems. DSCA responded in the matrix that access controls were in place. We verified that DSCA had access controls in place. Those access controls that DSAMS used included: users were required to identify themselves during system login through the use of a protected mechanism (such as passwords) to authenticate user identity and user accounts; user accounts were deactivated after three unsuccessful login attempts; and passwords expired every 90 days.

**Risk Assessment and Management Plan.** DSCA was requested to identify whether a risk assessment and management plan had been completed. ASD($C^3I$) defined risk as the possibility of something adverse happening; risk assessment as the process of analyzing threats and vulnerabilities of an information system, and the potential impact of lost information; and risk management as the process of assessing risk, taking steps to reduce risk to an acceptable level, and maintaining that level of risk. DSCA responded in the matrix that a risk assessment and management plan was not completed. We verified that when DSCA submitted the matrix data as of August 1, 2001, it had not developed a DSAMS risk assessment and management plan. However, since that time, DSCA completed a DSAMS risk assessment and developed a DSAMS risk management plan.

**System Life-Cycle Plan.** DSCA was requested to identify whether a system life-cycle plan existed. System life-cycle plan guidance that ASD($C^3I$) provided with the matrix was that many system life-cycle models exist but most contain five basic phases: initiation, development and acquisition, implementation, operation, and disposal. DSCA responded in the matrix that a DSAMS life-cycle plan had not been completed. We confirmed that as of August 1, 2001, DSCA had not developed a DSAMS life-cycle plan. As of June 2002, a DSAMS life-cycle plan was being developed.

**System Security Plan.** DSCA was requested to identify whether a system security plan was in place. ASD($C^3I$) defined a system security plan as an overview of the security requirements of a system, a description of the controls in place or the controls planned for meeting those requirements, and delineation of responsibilities and expected behavior of the individuals who access the system. DSCA responded in the matrix that a DSAMS security plan had not been completed. We confirmed that as of August 1, 2001, DSCA had not developed a DSAMS security plan. However, since that time, DSCA developed a system security plan. The system security plan, the "DSAMS End Users Security Guide," identifies the security measures that must be enforced to operate DSAMS so that the system can securely process sensitive, unclassified information. In addition, the guide documents DSAMS information system security personnel responsibilities, security management responsibilities, and incident reporting responsibilities.

**Personnel Security Measures.** DSCA was requested to identify whether proper personnel security measures were in place. ASD($C^3I$) defined personnel security measures as a broad range of security issues related to how human users, designers, implementers, and managers of software and hardware interact with computers, and the access and authorities needed to do their jobs. DSCA responded in the matrix that DSAMS had personnel security measures in place. We confirmed that personnel security measures, in the form of access measures, were in place for DSAMS. DSAMS had segregation of duties, with varying levels of access and control for designers, developers, programmers, testers, and system administrators. DSAMS authorized personnel access to DSAMS through the use of password-protection procedures. DSAMS password-protection procedures require passwords to be changed every 90 days and user accounts to be closed after 180 days of inactivity.

Although personnel security access measures were in place, another personnel security issue addressed in Report No. D-2001-141 had not been corrected. We found that contractor employees were continuing development work on DSAMS software while their security clearances were pending. We readdressed that personnel security issue with DSCA in a classified memorandum, "Potential Security Risks to Department of Defense Information Systems," June 14, 2002. The Audit Followup and Technical Support Directorate, Inspector General of the Department of Defense, plans to perform follow up action on the personnel security issue.

**Physical Security Controls.** DSCA was requested to identify whether physical security controls were in place. ASD($C^3I$) defined physical security and environment security as the measures taken to protect systems, buildings, and related supporting infrastructures against threats associated with their physical environment. DSCA responded in the matrix that DSAMS had physical security controls in place. We verified that physical security controls were in place. All DSAMS equipment (servers and data storage) was secured by DISA at DECC Oklahoma City,[5] where the DSAMS application resides. DECC Oklahoma City physical security controls for DSAMS included that the support and administrative areas were protected by at least one physical barrier and that the computer room was protected by at least three physical barriers. The Defense Security Assistance Development Center network, Mechanicsburg, Pennsylvania (used to develop DSAMS software) was secured by at least two physical barriers.

**Administrative Controls.** DSCA was requested to identify whether administrative controls were in place. ASD($C^3I$) did not define administrative controls but suggested that administrative controls included the presence of a help desk and audit trail. Administrative controls are designed to promote operational efficiency and adherence to system policies and procedures. DSCA responded in the matrix that DSAMS had administrative controls in place. We verified the DSCA response. DSCA had established a help desk and an audit trail for DSAMS.

**Contingency Plans.** DSCA was requested to identify whether contingency plans were in place and, if so, when the last time was that a contingency drill, data loss drill, or power loss drill occurred. ASD($C^3I$) defined

[5]The DECC Oklahoma City site received DITSCAP certification and accreditation on September 15, 2000.

contingency planning as involving more than simply planning for a move offsite after a disaster destroys a facility. Contingency planning was to also include how to keep an organization's critical functions operational in the event of disruptions, both large and small. Although DoD Directive 5200.28 requires periodic testing of contingency plans for mission-critical systems, the Directive encourages contingency plans for all systems. DSCA responded in the matrix that DSAMS did not have a contingency plan in place and left the date the contingency plan was last exercised blank. We verified that DSCA did not have a complete DSAMS contingency plan; however, it did have a year 2000 DSAMS business contingency plan. That contingency plan addressed two business-specific contingencies, short-term loss and prolonged loss of system availability, but did not address site-specific contingencies, such as natural disasters (for example, fire, flood, and earthquake), civil disorders, and bomb threats. DSCA was revising the contingency plan to address additional events.

Short-term loss (less than 1 week) of DSAMS availability was addressed through users of the system holding foreign military sales data and the users inputting the data when DSAMS became operational. Prolonged loss (in excess of 1 week) of DSAMS availability was addressed with the use of manual methods to process the foreign military sales data (typewriters, word processors, faxes, telephones, couriers, and the use of existing reports). When DSAMS becomes operational, the manually processed data would then be inputted. Furthermore, if the DECC Oklahoma City operations site were to become inoperable, DSAMS would be restored at a DISA backup operations site in Louisiana from the nightly DSAMS backup files. As reported by DSCA, the contingency plan had not been fully exercised. However, DSCA had executed parts of the plan, such as the data backup and recovery processes. DISA last exercised DSAMS at the backup operations site in June 2002.

**Hardware and System Software Maintenance Plans.** DSCA was requested to identify whether hardware and software maintenance plans were in place. ASD($C^3$I) defined hardware and software maintenance plans as controls used for monitoring the installation of, and update to, hardware and software to ensure that the system functions as expected and that a historical record of changes is maintained. DSCA responded in the matrix that DSAMS had hardware and system software maintenance plans in place. However, we determined that DSAMS did not have hardware and system software maintenance plans when the matrix was submitted. DSCA officials agreed that the answer was incorrect as of August 1, 2001. As of June 2002, DSAMS had not developed hardware and system software maintenance plans.

**Data Integrity Processes.** DSCA was requested to identify whether data integrity processes were in place. ASD($C^3$I) defined data integrity processes as controls used to protect data from accidental or malicious alteration or destruction and used to provide assurance for users that the information met expectations about its quality and integrity. DSCA responded in the matrix that DSAMS had data integrity processes in place. We verified that DSAMS had data integrity processes. DSAMS was protected by virus detection and communication encryption software that guaranteed integrity and confidentiality. The data integrity processes were managed for DSAMS through the use of software controls and procedural measures at the DITSCAP-accredited DECC Oklahoma City site.

**Security Incident Response Plan.** DSCA was requested to identify whether a security incident response plan was in place. ASD($C^3$I) defined a security incident response plan as a formal description and evaluation of risks to an information system, and a process that identified and applied countermeasures commensurate with the value of the assets protected based on a risk assessment. An incident response plan should have help capability when an adverse event in a computer system or network causes a failure of a security mechanism or when an attempted breach of those mechanisms occurs. DSCA responded in the matrix by leaving the field blank. We confirmed that DSAMS did not have a security incident response plan in place at the time the matrix was submitted. However, since August 1, 2001, DSCA had developed a security incident response plan. The plan provides general guidelines for the systematic response to unauthorized intrusions, classified message incidents, malicious code, fraud and theft, errors in and omissions of data, employee sabotage and abuse, and denial of service incidents.

**Operations and Assessments Interest Items.** DSCA was requested to identify specific operational assessment mechanisms that existed as part of the operation of the system and to provide general comments to augment reporting efforts on basic program management, controls, and procedures. ASD($C^3$I) did not provide definitions for reporting elements contained in the operations and assessments interest items section of the matrix. Information contained in that section included network protections, vulnerabilities, and assessments.

**Network Protections.** ASD($C^3$I) requested data from DSCA on the network security functions of intrusion detection systems and firewalls.

**Intrusion Detection Software.** DSCA was requested to identify whether intrusion detection software protected the DSAMS. Intrusion detection software inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system.

**Firewalls.** DSCA was requested to identify whether boundary protections, such as firewalls, for DSAMS were present. A firewall is a boundary protection system that limits access between networks to prevent intrusions from outside the network. A firewall stops external intrusions but does not detect an attack from inside the network.

DSCA responded in the matrix that DSAMS was protected by intrusion detection software and had boundary protection in place. We confirmed that DSAMS was protected by intrusion detection and a firewall at DECC Oklahoma City. DSAMS uses client and server architecture; although DSAMS did not have intrusion detection software or firewalls at user sites, the DISA intrusion detection software and firewall at DECC Oklahoma City protected the DSAMS data.

**Vulnerabilities.** ASD($C^3$I) requested DSAMS information from DSCA concerning the red and blue team assessment, information assurance vulnerability alert process, and the vulnerability analysis and assistance program.

**Red and Blue Team Assessment.** DSCA was requested to identify the date for the most recent red and blue team assessment. According to a dictionary and reference guide used by the GISR Act Integrated Process Team, a red team is a simulated opposing force that uses active and passive actions, as well as technical and non-technical capabilities, to expose and exploit information operation vulnerabilities of a blue team (a simulated friendly force). DSCA responded in the matrix that DSAMS had not had a red and blue team assessment. We confirmed that the DSCA response was correct as of August 1, 2001. However, as part of an FY 2000 security review of DSAMS, the system's development contractor performed internal penetration testing for vulnerabilities. In addition, DISA had a red and blue team assessment performed for the DECC Oklahoma site.

**Connections.** DSCA was requested to identify whether DSAMS had a connection approval to connect to a larger backbone network. Connections are system interfaces to other information systems for the purpose of transmitting or receiving data. DSCA responded in the matrix that the DSAMS interface connections were approved. We confirmed that DSCA had a formal DSAMS system interface agreement with the external Defense Integrated Financial System of the Defense Finance and Accounting Service. Additionally, DSCA had system interface specifications for DSCA systems that connected to DSAMS. The DSAMS system interface specifications identify and map the data protocols for those internal and external DSCA systems that exchange data with DSAMS.

**Information Assurance Vulnerability Alert.** DSCA was requested to identify whether DSAMS was fully information assurance vulnerability alert compliant in both acknowledging and adhering to information assurance vulnerability alerts. An information assurance vulnerability alert is a process that incorporates identification and evaluation of new vulnerabilities, disseminates technical responses, and tracks compliance within DoD. Alerts are generated when a critical vulnerability that poses an immediate threat to DoD exists. DSCA responded in the matrix that DSAMS was fully information assurance vulnerability alert compliant. We confirmed that the DSCA response was appropriate as of August 1, 2001; DSAMS was information assurance vulnerability alert compliant.

**Vulnerability Analysis and Assistance Program.** DSCA was requested to identify whether DSAMS had a vulnerability analysis and assistance program assessment. According to a dictionary and reference guide used by the GISR Act Integrated Process Team, a vulnerability analysis and assistance program was a survey of the Non-Secure Internet Protocol Router Network, the SECRET Internet Protocol Router Network, and Joint Worldwide Intelligence Communications System networks for common computer security vulnerabilities. DSCA did not provide a response in the matrix. We confirmed that the DSCA response was appropriate as of August 1, 2001, and as of June 2002, no vulnerability analysis and assistance program assessment had been performed.

**Assessments.** DSCA was requested to identify the dates for the most recent:

- Joint Staff integrated vulnerability assessment,
- system requirements reviews,
- balance survivability assessment, and
- integrated vulnerability assessment.

DSCA provided no response in the matrix. We confirmed that the DSCA response was correct as of August 1, 2001, because the reporting elements in the section were specific assessments and technical controls that not all systems were required to perform, which included DSAMS. However, in May 2000, DISA performed a system requirements review at DECC Oklahoma City, which included a review of DSAMS.

## Conclusion

From our analysis of the data reported in the matrix for DSAMS, we concluded that DSCA was following DITSCAP to certify and accredit DSAMS. Although 1 of the 32 matrix responses was incorrect and audit issues from a prior audit remained unresolved, we concluded that DSCA was making progress in achieving full information security accreditation for DSAMS.

# Appendix A. Scope and Methodology

**Work Performed.** We verified and validated the DSAMS data supporting the DoD GISR Act Report. We also performed a review of DSAMS information security controls at the Defense Security Assistance Development Center, Mechanicsburg, Pennsylvania, to validate operational controls. To accomplish the audit objective, we:

- reviewed Public Law 106-398, Office of Management and Budget guidance, and DoD regulations and guidance related to the GISR Act;
- interviewed DSAMS personnel in DSCA who prepared the GISR Act matrix submission;
- verified the information reported on the GISR Act data collection matrix. Our verification consisted of reviewing the documentation that supported the answers DSCA provided on the GISR Act collection matrix as of August 1, 2001;
- interviewed personnel responsible for DSAMS development at the Defense Security Assistance Development Center; and
- reviewed site operations that documented the presence of operational controls at the Mechanicsburg site.

**Limitations to Scope.** We limited the audit scope to verification and validation of information in the DSAMS GISR Act collection matrix submitted by DSCA and certification and accreditation progress made since. Additionally, we did not review the management control program because DoD recognized information assurance programs as a material weakness in its FY 2000 Statement of Assurance, which was its most recent, signed Statement of Assurance.

**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.

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

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

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

## Prior Coverage

During the last 5 years, the Inspector General of the Department of Defense has issued two reports discussing DSAMS. Unrestricted Inspector General of the Department of Defense reports can be accessed at http://www.dodig.osd.mil/audit/reports.

### Inspector General of the Department of Defense (IG DoD)

IG DoD Report No. D-2001-141, "Allegations to the Defense Hotline on the Defense Security Assistance Management System," June 19, 2001

IG DoD Report No. 98-095, "Defense Security Assistance Management System," March 24, 1998

# Appendix B. Government Information Security Reform Act Collection Matrix Submission

We evaluated the DSAMS GISR Act collection matrix that DSCA submitted as of August 1, 2001, to ASD($C^3$I). The following is a summary of the data ASD($C^3$I) requested, the response from DSCA, and our analysis of the response for 27 of 32 fields on the data collection matrix. We did not include in the matrix below five administrative information data fields that identified the system. A list of acronyms is at the end of this appendix.

| Accreditation Information | | |
|---|---|---|
| **Data Requested** | **DSCA Response*** | **Audit Results** |
| Accredited? (Date) | No | DSAMS was not accredited.<br><br>The DSCA goal was to accredit DSAMS by the end of calendar year 2002. |
| Interim authority to operate? (Date) | No | DSAMS had been operating since February 1998 without accreditation or interim authority to operate.<br><br>On June 13, 2002, DSCA was granted a 180-day interim authority to operate DSAMS, from the Designated Approving Authority (Deputy Director, DSCA). |
| Accreditation under DITSCAP? | No | DSAMS was not accredited, but DSCA was following DITSCAP to certify and accredit DSAMS, and planned for accreditation by the end of calendar year 2002. |
| Not DITSCAP, describe other. | No | DSAMS was not accredited prior to the current effort to accredit under DITSCAP. |
| Formal documentation in effect? (SSAA or other certification and accreditation documentation) | No | No formal SSAA had been developed for DSAMS.<br>DSCA planned on developing an SSAA to formally document DSAMS certification and accreditation processes. |

*Some questions request a date only. If a date was provided, it can be implied that the answer was yes.

| Assessment Criteria Information | | |
|---|---|---|
| **Data Requested** | **DSCA Response*** | **Audit Results** |
| Access controls in place? | Yes | The DSAMS used passwords and user accounts.<br>– User accounts were user's first initial and full last name.<br>– Passwords were from 8 to 15 characters long, and had at least one uppercase, one lowercase, and either one numeric or one special character.<br>– After three unsuccessful login attempts, the DSAMS user account is deactivated.<br>– Passwords expired every 90 days. |
| Risk assessment and management plan completed? | No | DSCA had not developed a DSAMS a risk assessment and management plan at the time the matrix was submitted.<br><br>DSCA subsequently completed the risk analysis and management plan. The plan addresses four threats and comprises five parts:<br>– the threat,<br>– the probability of the threat occurring,<br>– the risk if the threat occurs,<br>– the possible cost if the threat occurs, and<br>– countermeasures that can be applied. |
| System life-cycle plan exists? | No | DSCA had not developed a DSAMS life-cycle plan at the time the matrix was submitted. The system life-cycle plan was being developed as of June 2002. |
| System security plan in place? | No | DSCA had not developed a DSAMS security plan at the time the matrix was submitted.<br><br>DSCA developed a system security plan since the matrix was submitted.<br><br>The plan provides an overview of DSAMS security requirements. |

*Some questions request a date only. If a date was provided, it can be implied that the answer was yes.

| Assessment Criteria Information (cont'd) | | |
|---|---|---|
| **Data Requested** | **DSCA Response*** | **Audit Results** |
| Proper personnel security measures in place? (includes assignment of duties and segregation of duties) | Yes | DSAMS had segregation of duties, with varying levels of access and control.<br>– Designers, developers, programmers, testers, and system administrators all had automated data processing level I, II, or III access privileges.<br>– The level of automated data processing access privileges granted was based on each position's job description.<br><br>Passwords were required to be changed every 90 days.<br><br>User accounts were closed after 180 days of inactivity.<br><br>**Unresolved issues from prior audit:**<br>– DSCA was not requiring completed security background investigations before allowing users and developers access to DSAMS.<br>– Contractor employees without completed background investigations have been developing DSAMS, some since calendar year 1996.<br>– Initial security background investigation requests for contractor employees were not submitted till FY 2000, and most of the clearances were still pending. |
| Physical security controls in place? | Yes | All DSAMS hardware was secured by DISA at DECC Oklahoma City.<br>DECC Oklahoma City received DITSCAP accreditation on September 15, 2000.<br>– DECC Oklahoma City support and administrative areas were protected by at least one physical barrier.<br>– DECC Oklahoma City computer room was protected by at least three physical barriers.<br>The Defense Security Assistance Development Center network, Mechanicsburg, was secured by at least two physical barriers. |

*Some questions request a date only. If a date was provided, it can be implied that the answer was yes.

| **Assessment Criteria Information** (cont'd) | | |
|---|---|---|
| **Data Requested** | **DSCA Response*** | **Audit Results** |
| Administrative controls in place? (includes help desk and audit trail) | Yes | DSCA had established a help desk and an audit trail for DSAMS. |
| Contingency plans in place? | No | DSCA had a year 2000 DSAMS business contingency plan. The plan had two contingency plans of action.<br>– Short-term loss (less than 1 week): Users of the system would hold work until DSAMS became operational.<br>– Prolonged loss (in excess of 1 week): Manual means would be put into effect (typewriters, word processors, faxes, telephones, couriers, and the use of existing reports), and data would be inputted when DSAMS became operational.<br><br>If DECC Oklahoma City operations site were to become inoperable, DSAMS would be restored at a DISA backup operations site in Louisiana from the nightly DSAMS backup file.<br><br>The contingency plan was being revised to address additional events. |
| Date contingency plans last exercised? | Blank | The contingency plan had not been fully exercised.<br>– DSAMS has been down for short-term periods.<br>– DSAMS data backup and recovery processes had been exercised.<br>– DSAMS was exercised at the backup operations site in June 2002. |
| Hardware and system software maintenance plans in place? (includes version control testing) | Yes | The DSCA response was incorrect. As of June 2002, DSCA still did not have maintenance plans in place for DSAMS. |

*Some questions request a date only. If a date was provided, it can be implied that the answer was yes.

| **Assessment Criteria Information** (cont'd) | | |
|---|---|---|
| **Data Requested** | **DSCA Response*** | **Audit Results** |
| Data integrity processes in place? (includes virus scans, system performance monitoring) | Yes | DSAMS was protected by virus detection and communication encryption software.<br>DSAMS data integrity is managed under the DECC Oklahoma City, DITSCAP-accredited system procedures and processes. |
| Security incident response plan in place? | Blank | DSCA did not have a security incident response plan at the time the matrix was submitted. However, DSCA subsequently developed a plan. The plan addresses:<br>– unauthorized intrusions;<br>– classified message incidents;<br>– malicious code;<br>– fraud and theft;<br>– errors in and omissions of data;<br>– employee sabotage and abuse; and<br>– denial of service incidents. |

*Some questions request a date only. If a date was provided, it can be implied that the answer was yes.

| Operations and Assessments Interest Items | | |
|---|---|---|
| **Data Requested** | **DSCA Response*** | **Audit Results** |
| Protected by IDS [Intrusion Detection Software]? | Yes | DSAMS was protected by IDS.<br><br>DECC Oklahoma City provides DSAMS IDS support as part of their operations. |
| Boundary protection in place? (For example, firewall) | Yes | DSAMS was protected by boundary protection (firewalls).<br>– DECC Oklahoma City provides DSAMS boundary protection as part of its operations.<br>– Unsuccessful login attempts are tracked. |
| Red and blue team assessment? (Date) | No | No red and blue team assessments had been performed on DSAMS.<br><br>A red and blue team assessment was performed for the DECC Oklahoma City site. |
| Connection approved? | Yes | DSAMS had a formal interface agreement with the Defense Finance and Accounting Service's Defense Integrated Financial System.<br><br>DSAMS had interface design specifications for internal DSCA systems |
| IAVA [Information Assurance Vulnerability Alerts] compliant? | Yes | DSCA had an IAVA policy in place and had allocated the personnel resources required to implement it. DSCA is using the DISA IAVA handbook as its IAVA policy. |
| VAAP [Vulnerability Analysis and Assistance Program] assessment complete? (Date) | Blank | No VAAP assessment had been completed for DSAMS. |

*Some questions request a date only. If a date was provided, it can be implied that the answer was yes.

| **Operations and Assessments Interest Items** (cont'd) | | |
|---|---|---|
| **Data Requested** | **DSCA Response*** | **Audit Results** |
| Joint Staff integrated vulnerability assessments complete? (Date) | Blank | No joint staff integrated vulnerability assessments had been completed for DSAMS. |
| System requirements reviews complete? (Date) | Blank | No system requirements reviews had been completed for DSAMS at the time DSCA submitted the matrix.<br><br>However, a system requirements review by DISA of DECC Oklahoma City included a review of DSAMS. |
| Balance survivability assessment complete? (Date) | Blank | No balance survivability assessment had been completed for DSAMS. |
| Integrated vulnerability assessment complete? (Date) | Blank | No integrated vulnerability assessment had been completed for DSAMS. |

*Some questions request a date only. If a date was provided, it can be implied that the answer was yes.

**Applicable Acronyms**

| | |
|---|---|
| ASD($C^3I$) | Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) |
| DECC | Defense Enterprise Computing Center |
| DISA | Defense Information Systems Agency |
| DITSCAP | Defense Information Technology Security Certification and Accreditation Process |
| DSAMS | Defense Security Assistance Management System |
| DSCA | Defense Security Cooperation Agency |
| GISR | Government Information Security Reform |
| IAVA | Information Assurance Vulnerability Alerts |
| IDS | Intrusion Detection Software |
| SSAA | System Security Authorization Agreement |
| VAAP | Vulnerability Analysis and Assistance Program |

# Appendix C. Report Distribution

## Office of the Secretary of Defense

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

## Department of the Army

Auditor General, Department of the Army

## Department of the Navy

Naval Inspector General
Auditor General, Department of the Navy

## Department of the Air Force

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

## Other Defense Organizations

Director, Defense Finance and Accounting Service
Director, Defense Information Systems Agency
    Inspector General, Defense Information Systems Agency
Director, Defense Logistics Agency
Director, Defense Security Cooperation Agency

## Non-Defense Federal Organization

Office of Management and Budget

## Congressional Committees and Subcommittees, Chairman and Ranking Minority Member

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

# Team Members

The Readiness and Logistics Support 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.

Shelton R. Young
Kimberley A. Caprio
Tilghman A. Schraden
Kathryn L. Palmer
Walter S. Bohinski
Glen B. Wolff
Daniel L. Messner
Elizabeth N. Shifflett