Audit Report

IMPLEMENTATION OF DOD INFORMATION SECURITY POLICY FOR PROCESSING ACCOMPLISHED AT DEFENSE ENTERPRISE COMPUTING CENTERS

Report No. D-2001-183 September 19, 2001

Office of the Inspector General
Department of Defense

Additional Copies

To obtain additional copies of this audit report, visit the Inspector General, DoD, Home Page at www.dodig.osd.mil/audit/reports or contact the Secondary Reports Distribution Unit of the Audit Followup and Technical Support Directorate at (703) 604-8937 (DSN 664-8937) or fax (703) 604-8932.

Suggestions for 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, 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

AIS	Automated Information System
ASD(C3I)	Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
C and A	Certification and Accreditation
CIO	Chief Information Officer
DAA	Designated Approval Authority
DISA	Defense Information Systems Agency
DITSCAP	DoD Information Technology Security Certification and Accreditation Process
GAO	General Accounting Office
GISRA	Government Information Security Reform Act
IATO	Interim Authority to Operate
IT	Information Technology
ISSO	Information Systems Security Officer
OMB	Office of Management and Budget

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

September 19, 2001

MEMORANDUM FOR ASSISTANT SECRETARY OF DEFENSE (COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE)
ASSISTANT SECRETARY OF THE AIR FORCE (FINANCIAL MANAGEMENT AND COMPTROLLER)
DIRECTOR, DEFENSE FINANCE AND ACCOUNTING SERVICE
DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY
DIRECTOR, DEFENSE LOGISTICS AGENCY
NAVAL INSPECTOR GENERAL
AUDITOR GENERAL, DEPARTMENT OF THE ARMY

SUBJECT: Audit Report on Implementation of DoD Information Security Policy for Processing Accomplished at Defense Enterprise Computing Centers (Report No. D-2001-183)

We are providing this audit report for review and comment. We conducted the audit in accordance with the provisions of the Government Information Security Reform Act, title X, subtitle G of the FY 2001 Floyd D. Spence National Defense Authorization Act (Public Law 106-398). We considered management comments on a draft of this report when preparing the final report. The comments of the Army, Air Force and the Defense Logistics Agency conformed to DoD Directive 7650.3; therefore, additional comments are not required.

DoD Directive 7650.3 requires that all unresolved issues be resolved promptly. The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) did not respond to Recommendation 1. The Navy did not respond to Recommendation 2. The Defense Information Systems Agency nonconcurred with Recommendation 3.c., and we are asking that it reconsider its position in response to the final report. We request that the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), the Navy, and the Defense Information Systems Agency provide management comments on the final report by October 19, 2001. Comments from the Defense Finance and Accounting Service were received too late to be considered in preparing the final report. Therefore, unless the Defense Finance and Accounting Service submits additional comments by October 19, 2001, we will consider the comments received as the response to the final report.

We appreciate the courtesies extended to the audit staff. For additional information on this report, please contact Mr. Robert K. West at (703) 604-8983 (DSN 664-8983) (rwest@dodig.osd.mil) or Ms. Judith I. Padgett at (703) 604-8990 (DSN 664-8990) (jpadgett@dodig.osd.mil). See Appendix D for the report distribution. The audit team members are listed inside the back cover.

David K. Steensma

David K. Steensma
Acting Assistant Inspector General
for Auditing

Office of the Inspector General, DoD

Report No. D-2001-183 **September 19, 2001**
(Project No. D2001AD-0071)

Implementation of DoD Information Security Policy for Processing Accomplished at Defense Enterprise Computing Centers

Executive Summary

Introduction. Public Law 106-398, "Government Information Security Reform," title X, subtitle G, FY 2001 Floyd D. Spence National Defense Authorization Act, requires that each agency obtain an independent assessment of its security posture. The Inspector General of each agency is to evaluate the agency's security posture based on a review of an independently selected subset of systems.

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 in Defense Enterprise Computing Centers and Detachments, which are part of the Defense Information Systems Agency. Customer applications from all DoD Components include financial accounting; personnel; pay and disbursement; materiel shipping, receiving, and storing; munitions maintenance; and weapon-systems-associated applications.

The Office of the Inspector General, DoD, identified its independent subset of systems as the 1,365 unique-name applications resident on the Defense Enterprise Computing Centers and Detachments as of February 2001. From that population, the Office of the Inspector General selected a random sample of 90 applications. The Army Audit Agency evaluated 34 applications, the Air Force Audit Agency evaluated 19, and the Office of the Inspector General evaluated 37, which served the Navy, the Defense Logistics Agency, and the Defense Accounting and Finance Service. The evaluations did not include the security measures exercised for the Defense Enterprise Computing Centers' and Detachments' computer hardware, executive software, or other support components.

Objectives. The overall audit objective was to respond to the requirements of the Government Information Security Reform Act, title X, subtitle G of the FY 2001 Floyd D. Spence National Defense Authorization Act (Public Law 106-398). Specifically, we selected a subset of DoD information technology to determine whether managers for that information technology had implemented DoD information security policy.

Results. DoD managers had not fully implemented DoD information security policy. Written, current certifications and accreditations were not available for applications estimated at more than 60 percent of the population. Certification and accreditation are

the technical evaluation of security features of an application or system and the formal declaration to operate the application or system. The status of systems for certification and accreditation was estimated for the population of 1,365 applications from the Defense Enterprise Computing Centers and Detachments as follows:

	Projected Results	Percent of Population
Current Certification and Accreditation or Interim Authority to Operate	501	36.7
Indeterminate: retired, transferred, insufficient detail available to find authority to operate status	410	30.0
Other technology with no Certification and Accreditation or Interim Authority to Operate	137	10.0
Expired Certification and Accreditation or Interim Authority to Operate	30	2.2
No Certification and Accreditation or Interim Authority to Operate or Certification only	288	21.1
Total	**1,366**[1]	**100.0**

As a result of incomplete policy implementation, DoD managers assumed risks that were not fully identified, assessed, accepted, and managed as a result of a deliberative process. Unmanaged information security risk may lead to loss of service, data corruption, unauthorized access, sabotage, tampering, misuse, and fraud in DoD information technology resources. For details of the audit results, see the Finding section of the report.

Summary of Recommendations. We recommend that the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) define information systems terminology to clearly and comprehensively assign responsibility, and use measurement tools developed in response to Public Law 106-398 to evaluate guidance and rectify omitted, obsolete, and confusing policy. We recommend that the Chief Information Officers of the Army, the Navy, the Air Force, the Defense Finance and Accounting Service, and the Defense Logistics Agency use information gathered in response to the Public Law to allocate resources and improve programs. We also recommend that the Chief Information Officers coordinate security efforts with the Defense Information Systems Agency, identify security officials, and oversee internal procedures to provide information security for processing accomplished jointly. We further recommend that the Director, Defense Information Systems Agency, establish a monitoring process and a performance goal for tracking customer certifications and accreditations and identifying information security personnel for all customers by the FY 2002 Government Information Security Reform reporting period.

[1] The projected results do not add up to the population due to rounding.

Management Comments. The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) stated that the out-of-date security policies that we cited in our report were being updated and will be reissued in October 2001 and early 2002. In addition, the Assistant Secretary stated that the report oversimplified in attributing DoD information security deficiencies to a lack of definition for systems and applications and unclear guidance. The Army, the Air Force, and the Defense Logistics Agency concurred with the recommendations to use information gathered in response to the public law to allocate resources and improve programs and to coordinate information security efforts for applications and other informational technology with service providers. The Defense Information Systems Agency concurred with coordinating information security efforts with customers to obtain their statements of approval to operate when beginning service arrangements and with maintaining a resource listing of officials responsible for information security for each customer of the Defense Enterprise Computing Centers and the Detachments. The Defense Information Systems Agency nonconcurred with establishing a monitoring process and performance goal for the Defense Enterprise Computing Centers' information security documentation and personnel. Although the Defense Finance and Accounting Service concurred with the recommendations, we received management's comments too late to be included in this final report. We will consider those comments as management's response to the final report unless management submits additional comments. The Navy did not provide management comments. A discussion of the management comments is in the Finding section of the report and the complete text is in the Management Comments section.

Audit Response. Current and clear guidance from the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), although not a guarantee of adherence, is a prerequisite for effective implementation and oversight of information security. Also, the Assistant Secretary did not specifically comment on the recommendations on defining information systems technology to clearly assign responsibility and on using measurement tools developed in response to Public Law 106-398 to evaluate guidance and rectify omitted, obsolete, and confusing policy. The Defense Information Systems Agency should establish a monitoring process because information security is a shared responsibility in which the Defense Information Security Agency has a critical role for its customers. Without current information about its customers and their security status, the Defense Information Security Agency could put all customers at increased risk. The comments from the Army, the Air Force, the Defense Logistics Agency, and the Defense Finance and Accounting Service were adequate and additional comments are not required. We request that the Assistant Secretary of Defense (Command, Control, Communications and Intelligence), the Chief Information Officer of the Navy, and the Defense Information Systems Agency provide comments on their respective recommendations by October 19, 2001.

Table of Contents

Background

General Provisions of Government Information Security Reform. On October 30, 2000, the President signed the FY 2001 Defense Authorization Act, (Public Law 106-398) that included title X, subtitle G, "Government Information Security Reform Act," (GISRA). Subtitle G provides for ensuring effective controls for highly networked Federal information resources, management and oversight of information security risks, a reporting mechanism for improved information system security oversight, and assurance for Federal information security programs. The GISRA directs each Federal agency (the DoD for purposes of this report) to evaluate its information security program and practices annually and, as part of the budget process, submit the results to the Office of Management and Budget (OMB). The GISRA covers unclassified and national security systems and creates the same management framework for each.

DoD and Inspector General Provisions of GISRA. The GISRA establishes parallel requirements for the agency and the agency Inspector General. It requires DoD to annually evaluate its information security program and practices and confirm their effectiveness by testing a subset of systems. GISRA requires the Office of the Inspector General to also evaluate the DoD information security program and practices and to independently select and test a subset of systems to confirm information security program effectiveness.

The DoD Information Technology Universe. The DoD has thousands of information technology (IT) processes that comprise its IT universe. Those processes can be categorized according to a variety of criteria; for example, function, criticality, and owner or operator. Two categories, or populations, identified in DoD for the FY 2001 GISRA report were the IT Registry systems and the processes supported by the Defense Enterprise Computing Centers (the Centers), for which DISA billed its customers. Those processes or applications that are Center supported may also be on the IT Registry database, though not all are.

IT Registry Database of Systems. The IT Registry database is required by title VIII, subtitle B, "Information Technology," section 811, "Acquisition and Management of Information Technology," Public Law 106-398. All mission-critical and mission-essential IT systems must be registered with the DoD Chief Information Officer (CIO) before they can be funded. The IT Registry database requires 17 data fields, including system name, description, functional area, and program manager information. As of April 2001, 3,739 IT systems were registered in the IT Registry database.

Center-Supported Applications. The Centers and Detachments of the Defense Information Systems Agency (DISA) provide general support systems, including mainframe computers, minicomputers, and local area networks for its customers' applications. Each Center operates under the control of the Center commanding officer, with system security functions accomplished by the designated security manager and the information systems security manager. The DISA has five Centers that are located in Mechanicsburg, Pennsylvania;

Columbus, Ohio; St. Louis, Missouri; Oklahoma City, Oklahoma; and Ogden, Utah. In addition, there are Detachments or satellite sites at 14 other locations. The Center customers are the Military Departments and other Defense agencies with installations throughout the United States. The customer applications that the Centers and Detachments run to support DoD installations include financial accounting; personnel; pay and disbursement; materiel shipping, receiving, and storing; munitions maintenance; and weapon-systems-associated applications. DISA bills the customers for running 4,939 applications.

The Subset Selected by the Office of the Inspector General. The Office of the Inspector General, DoD, identified its independent subset of systems as the applications supported by the Centers and Detachments of DISA. Analysis of the 4,939 applications identified 1,365 items based on unique names that became the source of the subset sample. The random sample included applications supporting multiple DoD Components, installations, and functions. The Army Audit Agency evaluated 34 applications and the Air Force Audit Agency evaluated 19 applications supporting their respective Components. The Office of the Inspector General, DoD, evaluated the balance of 37 applications, which supported the Navy, the Defense Finance and Accounting Service, and the Defense Logistics Agency. The evaluation did not include the Centers' and Detachments' security measures exercised for the computer hardware, executive software, or other components of Center support.

The DoD Information Security Program. The primary document establishing the DoD information security program is DoD Directive 5200.28, "Security Requirements for Automated Information Systems," March 21, 1988, which provides the mandatory, minimum security requirements for automated information systems (AISs) based on acceptable levels of risk. Directive 5200.28 has several companion regulatory and procedural documents, including DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process," (DITSCAP), December 30, 1997.

The DITSCAP Program. DoD Instruction 5200.40 implements DoD Directive 5200.28; it prescribes procedures to accomplish policy goals and establishes standards for certifying and accrediting the security of DoD systems throughout their life cycle.

Objectives

The overall audit objective was to respond to the Government Information Security Reform provisions in title X, subtitle G of the FY 2001 Floyd D. Spence National Defense Authorization Act (Public Law 106-398). Specifically, we selected a subset of IT in the DoD and determined whether the managers had implemented DoD information security policy. We did not evaluate the management control program separately because the DoD recognized information security and assurance programs as a material weakness in its most recent Statement of Assurance. In addition, the General Accounting Office (GAO) identified information security as a high risk. See Appendix A for a discussion of the audit scope and methodology. See Appendix B for prior coverage related to the audit objectives.

Implementation of DoD Information Security Policy

DoD managers had not fully implemented information security policy for the DISA Center- and Detachment-supported applications, as shown by the number of applications that had written, current certification and accreditation (C and A) or interim authority to operate (IATO). Written, current C and As were not available for an estimated 60 percent of applications residing on Center and Detachment computer systems. The projected point estimates to the population of 1,365 for authority to operate for the sample of 90 applications were as follows:

	Projected Results	Percent of Population
Current C and A or IATO	501	36.7
Indeterminate: retired, transferred, insufficient detail available to find status	410	30.0
Other technology with no C and A or IATO	137	10.0
Expired C and A or IATO	30	2.2
No C and A or IATO, or certification only	288	21.1
Total	**1,366**[1]	**100.0**

The DoD managers had not fully implemented information security policy because definitions for system, application, and other means of establishing security parameters and responsibilities were unclear. The parameters of and responsibility for information security were further obscured by the DoD practice of approving different organizations to design, develop, manage, use, and operate IT applications. In addition, the policy proponent, the Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) [ASD (C3I)]; the service provider, DISA; and the Component heads provided little oversight of policy implementation or policy applicability to the current IT environment. As a result of incomplete policy implementation, DoD managers assumed risks to IT that were not fully identified, assessed, accepted, and managed as a result of a deliberative process. Unmanaged risk could lead to loss of service, data corruption, unauthorized access, sabotage, tampering, misuse, and fraud in DoD IT systems and applications.

[1] The projected point estimates do not add up to the population of 1,365 due to rounding.

Guidance on Information Security for AISs

OMB Circular A-130. The purpose of OMB Circular A-130, Revised, "Management of Federal Information Resources," February 8, 1996,[2] appendix III, "Security of Federal Automated Information Resources," is to establish a minimum set of controls to be included in Federal automated information security programs. Circular A-130 requires agencies to establish controls that ensure adequate security for all information that is processed, transmitted, or stored in Federal automated information systems. The Circular also states that agencies should include controls that assign responsibility for security, security planning, periodic review of security controls, and management authorization.

DoD Directive 5200.28 Requirements for Accreditation Process and Security Responsibility. DoD Directive 5200.28 applies to all AISs, including stand-alone systems, communications systems, and computer systems of all sizes. The Directive specifically states that an AIS accreditation should be accomplished and supported by a certification plan, a risk analysis of the AIS in its operational environment, an evaluation of the security safeguards, and a certification report. The Directive also states that a Designated Approval Authority (DAA) should approve the documents supporting each accreditation. The DAAs should reaccredit AISs at least every 3 years or before declaring a revised system operational.

In addition to the DAA approval responsibility, Directive 5200.28 assigns responsibility to the DAA for acting on security deficiencies that would preclude the certification process. The DAAs must review the safeguards and issue certification statements for each AIS under their jurisdiction, based on the acceptability of the security safeguards for the AIS.

Directive 5200.28 also establishes the responsibility of the Information System Security Officer (ISSO) to monitor the AISs for security compliance, report security incidents to the DAA, and maintain a plan for system security improvements and the progress towards meeting certification.

DoD Instruction 5200.40, DITSCAP. The 1997 DITSCAP implements a standard approach for protecting and securing DoD information systems and provides procedures for accomplishing the certification and accreditation process established in DoD Directive 5200.28. The DITSCAP applies 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: definition, verification, validation, and post accreditation. The DoD Instruction discusses the DAA, ISSO, program manager, and certification authority as essential to the DITSCAP process.

[2] OMB issued a revised Circular A-130 November 30, 2000. The November 2000 revision did not change the requirements cited here.

Assigning Responsibility for Information Security

From the sample of 90 applications, 33 applications met the minimum requirements for information security programs in assigning responsibility and accomplishing a current C and A or IATO. The results from the sample projected to 501 applications for the population that met minimum requirements.

Responsibility for information security was not assigned for 39 sample applications in four of the five C and A categories: no C and A, 2 of 19 applications; current C and A, 1 of 33 applications; other technology, 9 applications; and indeterminate, 27 applications.

Managers for two applications had not assigned DAAs or ISSOs for applications falling in the no C and A category. Managers for one application in the current C and A category had a DAA but no ISSO. Personnel contacted for nine applications that were categorized as other technology did not identify a DAA or an ISSO because the sample application did not meet the managers' definition of a system or an application. The nine items included five data sets, one database, and three software management tools. (See Appendix C for details of sample items.)

For 27 of the sample applications, personnel identified as DISA customer points of contact were unable to identify the application's DAA and ISSO or provide information about the C and A. As of March 2001, DISA billed a customer for each of the 27 applications. The customer points of contact reported that 6 applications were retired, 1 was transferred to a different service provider, 2 were in development, and 3 were classified. The customer points of contact for 15 applications did not recognize the application for which DISA was billing them as one supporting their organization or functions.

DISA could not provide further information regarding the applications, the DAA and ISSO for the applications, or the C and A status. DISA did not require customers to document completed DoD information security procedures before accepting the customers for Center and Detachment services. DISA resolutely delineated its security responsibilities for the hardware, executive software, and other supporting components from the security responsibilities for the customer applications.

According to OMB Circular A-130, appendix III, agency IT security programs should assign responsibility for security. The Circular discusses the need to assign responsibility as both a general control and as a major application control. DoD Directive 5200.28 states that DoD Component Heads should appoint a DAA and assign the responsibility for overall AIS security. The DAA also has the responsibility to make sure that management names an ISSO for each AIS.

The ISSO should implement security policy by monitoring each assigned AIS for appropriate operation, use, maintenance, and disposal. The ISSO verifies user qualifications for access and monitors audit trails periodically.

The applications that did not have a DAA or an ISSO appointed for security responsibility did not meet the minimum security program requirements established in OMB and DoD guidance. Approximately 40 percent, 547 applications (410 projected indeterminate and 137 other technology), of the 1,365 applications were estimated to have no appointed information security officers or approval authority. In our opinion, all the IT resident on the Centers and Detachments should have personnel assigned responsibility to ensure IT security, based on paragraph 2.3 in DoD Directive 5200.28, which states:

> This Directive applies to all AISs including stand-alone systems, communications systems, and computer network systems of all sizes, whether digital, analog, or hybrid; associated peripheral devices and software; process control computers; embedded computer systems; communications switching computers; personal computers; intelligent terminals; word processors; office automation systems; application and operating system software; firmware; and other AIS technologies, as may be developed.

Although data sets, databases, and software tools are not specifically mentioned, they are also not specifically exempted. Because those non-application and non-system items were resident on a computer, they should have been subject to security evaluation or included as a component of another AIS C and A. In addition, owners and operators of applications and other IT should sufficiently identify applications and other IT to provide accountability throughout its life cycle, including transfer and retirement.

Authorizing AISs to Operate

The sample of 90 applications had 21 applications without a current C and A. Managers for 7 applications had not obtained C and A or an IATO and managers for 12 applications had obtained certification of the applications but had not obtained an accreditation. Managers for two applications had allowed the C and A or IATO to expire (C and A more than 3 years old, IATO more than 1 year old).

The guidance in OMB Circular A-130, appendix III, states that one of the minimum requirements for an information security program is an authorization process to implement the agency security plan. The Circular asserts that authorization should occur at least every 3 years.

The DoD Directive 5200.28 requires official management authorization that it calls accreditation. The definition of accreditation states that authorization to operate should be based on a certification process and should show that due care was taken for security. The Directive specifies that reaccredidation should occur before a revised system is declared operational, or every 3 years regardless of revisions.

The managers of the applications that did not have a current C and A or IATO, an estimated 318 (30 expired and 288 with no C and A) of the 1,365 applications, did not have documented evidence that they evaluated risk, planned mitigating procedures, and accepted risk, or that they exercised due care regarding information security.

Defining the Parameters for Information Security

Another factor in establishing parameters, besides information technology that falls outside the conceptual framework of an application or a system, is the interface between applications and operating systems. Personnel for three Air Force applications and nine Navy applications disagreed on who was responsible for accreditation of applications. For example, the DISA Center personnel at Mechanicsburg consistently described their responsibility for security as one that ends at the interface point with a specific customer's data processing application. Navy personnel at Mechanicsburg believed that, although they could certify an application, only the Center personnel could accredit a system because a system would include all hardware and software required to accomplish a process.

However, the Navy position was not consistent with its documentation. The security certification documents, prepared by the organization that developed the applications, state that:

> "FMSO [Fleet Material Support Office] certifies that this Application has been examined for ADP [Automatic Data Processing] Security safeguards in accordance with OPNAVINST 5239.1A [Navy Operating Instruction] and is in compliance with proper ADP Security design conventions, *necessary for User Activity Accreditation* [emphasis added]."

The user activity, according to the October 13, 1993, memorandum transmitting the above security statement, was the Navy Ships Parts Control Center. The Center at Mechanicsburg was not an addressee for the certification statement. The Air Force and the Navy personnel associated with the 12 applications believed that they fulfilled their responsibility for information security when application developers certified the security features designed into the applications.

Other relationships among organizations can also add complexity to assigning responsibility for information security. In addition to the Center with its responsibility for the operating software and the hardware, an application could have other organizations providing and using data, developing the application, and providing the communications among the process parts. The applications and other items billed for by DISA do not always have the same user and payer, and the division of responsibility for security can be uncertain with multiple organizations involved. The Centers, Detachments, and DISA did not maintain records of customer security responsibility similar to records for customer paying responsibility.

Providing Oversight on Policy Implementation and Applicability

Although DoD Directive 5200.28 specifically assigns oversight and review of implementation of its stated policies to the ASD (C3I), the ASD (C3I) had no mechanism in place to provide that oversight. Additionally, the Directive assigns responsibility to DoD Component Heads, including DISA, for implementing and ensuring compliance with the Directive, and for programming funds and resources to support information security. The DoD Components also had no mechanisms to comprehensively measure compliance with the Directive.

Mechanism to Evaluate Security Posture. In a February 9, 2001, memorandum to all the Components, the ASD (C3I) stated that the DoD had several vehicles in place to assess information assurance and meet the intent of GISRA. However, according to the memorandum, the DoD required a means of evaluating and consolidating information assurance data to report the DoD information security posture. With the February memorandum, the ASD (C3I) established an integrated process team to accomplish that goal.

The integrated process team developed a matrix of features about which they would obtain responses from system managers. A sample of systems was randomly selected from the IT Registry, the DoD subset for testing policy effectiveness for the FY 2001 GISRA reporting period. The responses to the matrix of questions would provide a test of the implementation of IT security policy, and provide an opportunity to evaluate weaknesses in the overall DoD policy. The Office of the Inspector General, DoD, and the GAO provided earlier evaluations of the DoD information security policy during specific issue audits and reviews.

Policy Status Based on Evaluations. The evaluations conducted by the Office of the Inspector General, DoD and the GAO have repeatedly recommended updating policies and procedures to provide consistent management and monitoring of information security and assurance throughout the DoD. The DoD received recommendations related to DoD Directive 5200.28 and DoD Instruction 5200.40 in May 1996 (2 recommendations), September 1996 (1 recommendation), September 1997 (2 recommendations) and December 1999 (2 recommendations) that were open as of July 2001.

The overarching policy contained in DoD Directive 5200.28 no longer corresponded with other policy and directives because it predated them. For example, DoD Directive 5200.28 refers its users to DoD Directive 5010.38, "Internal Management Control Program," for independent review procedures, but those procedures are found in DoD Instruction 5010.40, "Management Control (MC) Program Procedures," August 28, 1996. Directive 5010.38 was reissued August 26, 1996, and the companion Instruction 5010.40 was issued August 28, 1996, resulting in a disconnect between the 1988 IT policy and other DoD policy and procedures.

Existing Information Security Policy. Oversight on implementation of the DoD information security policy should also identify the age and corresponding credibility of existing DoD Directive 5200.28 companion documents. The Directive refers its users to DoD 5200.28-Standard, "Department of Defense Trusted Computer System Evaluation Criteria," December 1985, for guidance on risk assessments and associated level of trust. The Directive also refers its users to DoD 5200.28-M, "ADP Security Manual," administratively reissued incorporating change 1 on May 24, 1979, for guidance on marking and disposition of media. The standard and the manual had not been updated for the IT environment that exists in the year 2001. That environment includes architectures of highly networked systems and media, such as writable compact disks.

Instruction 5200.40 provides detail on what needs to be completed for a certification and accreditation package, but it does not provide enough detail on how to prepare the documentation required in a certification package. The detailed description about how to complete the documentation required for a certification package first became available July 31, 2000, when DoD 8510.1-M, "DoD Information Technology Security Certification and Accreditation Process, Application Manual," was issued.

Different Assessment Tools Used for Certifying and Accrediting. Different assessment tools were used to certify and accredit DoD information systems, which led to delays in implementing and enforcing the DITSCAP. For example, the Navy did not use the DITSCAP to certify and accredit its systems; it used Navy Instruction 5239.1A, "Department of the Navy Automatic Data Processing Security Program," April 1, 1985. The Navy Instruction was to be updated and replaced by Navy Instruction 5239.1B, which was in draft as of June 2001. One of the major areas of concern to be addressed in Navy Instruction 5239.1B was the oversight of information assurance. According to Navy CIO personnel, the DITSCAP allows the Services to use Service-specific guidance to certify and accredit their information systems.

The Air Force started using the DITSCAP, effective April 1, 2001, for certifying and accrediting its information systems. Before using the DITSCAP, the Air Force used Air Force System Security Instruction 5024, volume 1, "The Certification and Accreditation Process," September 1, 1997. The Air Force Instruction has the same requirements as the DITSCAP. Owners of Air Force systems that were using the Air Force Instruction to certify their systems and applications were allowed to continue; however, future certification and accreditation will comply with the DITSCAP. We believe that moving to a common evaluation tool, the DITSCAP, will help to develop common terminology and parameters for information security and provide more uniform levels of policy implementation.

Conclusion

Although DoD has guidance and policies on information technology security and information assurance, DoD Components, including DISA, had not thoroughly implemented and enforced them. Therefore, unclassified applications and other

information resources operating or residing on DISA Centers and Detachments were not certified and accredited in accordance with the current DoD IT guidance and policy. The absence of clearly defined responsibilities and boundaries and limited oversight to maintain contemporary guidance pose unidentified and unmanaged risks. Those risks include the potential for loss of service, data corruption, unauthorized access, sabotage, tampering, misuse and fraud involving DoD information technology systems. In addition, when decisionmakers do not identify the specific risks or the magnitude of risk they must manage, they cannot assign the personnel or the funds to manage the risk.

Management Comments on the Finding and Audit Response

Office of the Secretary of Defense Comments. The Director, Information Assurance, Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), stated that the draft report made no mention of DoD CIO Guidance and Policy Memorandum 6-8510, "DoD Global Information Grid (GIG) Information Assurance and Information Assurance Implementation Guide," June 16, 2000, which is more contemporary guidance. The Director also stated that a draft DoD Directive 8500.1, "Information Assurance," and a draft DoD Instruction 8500.2, "Information Assurance Implementation," have been prepared to replace both DoD Directive 5200.28 and Policy Memorandum 6-8510. The Directive and the Instruction should be in coordination by October 2001. The Director also stated that DoD Instruction 5200.40, known as DITSCAP, was being revised to better define the certification and accreditation process and to address issues discussed in this audit report. The new DITSCAP will be issued as DoD Instruction 8510.1 in early 2002. The Director indicated that the report oversimplified in attributing DoD information security deficiencies to a lack of definition for systems and applications and unclear guidance. In addition, the Director did not agree that DoD Directive 5200.28 applied to data sets and databases. He said that such an interpretation would require all "files" to be certified and accredited.

Audit Response. The DoD CIO Global Information Grid guidance and policy memorandum issued June 16, 2000, may not be considered binding by DoD personnel. DoD Directive 5025.1, "DoD Directives System," July 27, 2000, states that, for directive-type memorandum, "A DoD issuance will be issued within 180 days of signature of the memorandum," and its predecessor guidance stated within 90 days. Also, DoD Directive 8500.1 and DoD Instruction 8500.2 were to have been completed by May 2001. Although current and clear guidance does not guarantee that the guidance will be followed, it is a prerequisite for effective implementation and oversight, and provides further assurance that responsible personnel are certifying and accrediting their systems and applications consistently. In addition, we do not advocate the certification and accreditation of files; however, any item resident on a computer represents a vulnerability and should be identified with a system or application that has been certified and accredited. During our audit, data sets and databases could not be traced back to applications that had been certified and accredited.

DISA Comments. DISA agreed that more vigilance is needed to ensure a secure information technology environment. DISA stated that it had taken a

number of proactive steps to ensure that its support to the Services and Defense agencies and, ultimately, the warfighter meet this requirement. DISA stated that information security is a shared responsibility and that DISA partners with its customers and vendors to accomplish the requirements of GISRA.

Recommendations, Management Comments and Audit Response

1. We recommend that the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence):

a. Define systems, applications, networks, and other terminology so boundaries and interfaces can be clearly established and comprehensive information security responsibility can be assigned. The definitions should also provide guidance on the applicability of information security to information technology items, such as data sets, databases, and software management tools.

b. Use the data collection effort designed in response to the reporting requirements of the Government Information Security Reform Act to identify information security policy and programs that are omitted, obsolete, or confusing, and expeditiously modify or update the policy and programs as needed.

Management Comments. The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) [ASD(C3I)] did not specifically respond to the recommendations. Therefore, we request that the ASD(C3I) provide comments to recommendations in response to the final report.

2. We recommend that the Chief Information Officers for the Army, Navy, Air Force, the Defense Finance and Accounting Service, and the Defense Logistics Agency:

a. Use the data collected in response to the Government Information Security Reform Act to identify weaknesses, such as expired accreditations, in their Component information security programs so they can provide resources to improve the programs.

b. Coordinate information security efforts for applications and other information technology with service providers, such as the Defense Information Systems Agency, to include clearly designated security and approval officials.

Army Comments. The Army concurred with Recommendations 2.a. and 2.b. The Army is implementing the DITSCAP as the standard for all its information systems. The Army's information assurance professionals at all levels are involved in the DITSCAP process, not only for applications that run on Defense Enterprise Computing Centers, but also for all information systems. The Army recommended to the Government Information Security Reform working group

that DoD make the development of better definitions a high priority requirement and that revisions to the DITSCAP application manual specifically address certification and accreditation requirements for applications and other entities. The Army suggested that DoD consider registering Defense Enterprise Computing Centers' applications in the IT registry database. In August 2001, the Army directed that responsible personnel for all systems and applications currently in the IT registry review and update all required identifying data. In addition, the Army will recommend to the ASD(C3I) that additional information security data fields be added to the IT registry database.

Audit Response. The Army's suggestion for registering DECC applications on the IT registry has merit. Office of Inspector General, DoD, Report No. D-2001-175, August 22, 2001, discusses more wide-ranging use of the IT registry database.

Navy Comments. The Navy did not comment on a draft of this report. Therefore, we request that the Chief Information Officer for the Navy provide comments to the final report.

Air Force Comments. The Air Force concurred with Recommendations 2.a. and 2.b. The Air Force will incorporate Government Information Security Reform data fields into the Air Force System Compliance Database, which will track Air Force systems for certification and accreditation and GISRA requirements. The Air Force has collected similar data, in support of GISRA, which yielded similar findings. The acting CIO for the Air Force made information security a priority by putting together a tiger team of Air Force experts to construct and guide the Air Force's implementation of an information assurance strategy. The Air Force strategy will be a collaborative effort with external agencies, including DISA and the Office of the Secretary of Defense.

Defense Logistics Agency Comments. The Defense Logistics Agency concurred with Recommendations 2.a. and 2.b. The Defense Logistics Agency stated that it would include weaknesses identified in response to GISRA in its Annual Statement of Assurance. It also stated that those weaknesses were included in its Information Assurance Program Plan and System Security Authorization Agreements for systems, networks, and websites. Furthermore, the Defense Logistics Agency planned or implemented schedules to mitigate those security weaknesses. It developed System Security Authorization Agreements in accordance with DoD Instruction 5200.40 for all five of the systems selected for review in this audit. One system was certified, accredited, and issued approval to operate on July 29, 2001; two are currently being certified with approval to operate planned for September 2001; and the remaining two should achieve approval to operate in November 2001. In addition, the Defense Logistics Agency information security efforts have been coordinated as part of service level agreements and memoranda of agreement.

Defense Finance and Accounting Service Comments. We received comments from the Defense Finance and Accounting Service too late to be included in the final report. However, management concurred with the recommendations. The

draft report comments will be treated as the comments to the final report unless the Defense Finance and Accounting Service wants to provide additional comments on the final report.

3. We recommend that the Commander, Defense Information Systems Agency, Western Hemisphere:

a. Coordinate information security efforts with customers to obtain their statements of approval to operate when beginning service arrangements and periodically thereafter.

b. Maintain a resource listing of officials responsible for information security for each customer of the Defense Enterprise Computing Centers and Detachments. Those officials should be contacted if their application is the source of security risks or affected by other customer or Defense Enterprise Computing Centers risks.

c. Establish a monitoring process and performance goal for Defense Enterprise Computing Centers to document current certifications and accreditations, interim authority to operate, and the designated approval authority and information systems security officer for all customers by the end of the FY 2002 Government Information Security Reform reporting period.

Management Comments. DISA concurred with Recommendation 3.a. DISA specifies in each service level agreement that the customer is responsible for the system or application certification and accreditation. In the future, the customer will be asked to document that the systems or applications are certified and accredited, or the steps taken to accomplish certification and accreditation, along with a schedule for completion. The customer will also be asked to identify the risks that the customer assumed to implement the work prior to completing the certification and accreditation process. That guidance will be transmitted to DISA Headquarters and field activities through a policy letter by October 1, 2001.

DISA concurred with Recommendation 3.b. DISA stated that all operational sites currently maintain the names and contact information for functional points of contact for all applications that run on systems at the Defense Enterprise Computing Centers and Detachments. The points of contact interface between the customers, the Defense Enterprise Computing Center, and the Detachments to address operational problems. If a security-related issue occurs, site personnel of DISA Western Hemisphere coordinate through the customer's functional point of contacts to resolve the problem with the customer's functional and security personnel.

DISA nonconcurred with Recommendation 3.c. DISA stated that the Office of the Secretary of Defense is responsible for this policy issue because the Office of the Secretary of Defense is in the position to require the Services and DoD agencies to update and maintain their portion of the information security records. DISA supports having a central repository for DAA information for

applications and major systems. DISA recommends that either a central repository be developed or that the IT registry be expanded to maintain the data at the Office of the Secretary of Defense level.

Audit Response. Although DISA concurred with Recommendation 3.b., the audit found gaps in the process described. The audit identified the Defense Enterprise Computing Center points of contact. However, as stated in this report, for 27 of the sample applications, DISA customer points of contact were unable to identify the application's DAA and ISSO or provide information about certification and accreditation. Further, for 15 applications, the customer points of contact did not recognize the applications for which DISA was billing them as one supporting their organization or functions. The DISA actions on Recommendation 3.a. should result in identifying customer points of contact that are aware of and maintain the appropriate information security data.

With respect to Recommendation 3.c., we agree that the Office of the Secretary of Defense has a principal role in issuing the policy to require the Services and Defense agencies to provide the information. However, as DISA acknowledges in its response, information security is a shared responsibility and DISA must partner with various parties to ensure that the requirements of information security are met. In our opinion, DISA has an essential role to monitor information collection on current certifications and accreditations, the interim authority to operate, and the designated approval authority and information systems security officer for all customers. In response to the final report, we request that DISA reconsider its position on establishing a monitoring process.

Appendix A. Audit Process

Scope

Work Performed. In February 2001, we selected a subset of applications, as required by the GISRA. Our subset of systems was independent from the sample that DoD selected in April from the IT Registry database. We selected our sample from items residing on and billed by Centers and Detachments, a listing obtained in response to our request for applications operating at Centers and Detachments. Operations research analysts aggregated the population of 4,939 billable line items to 1,365 items based on unique names. The operations research analysts then selected a simple random sample of 90 applications. Of the 90 sample items from the Center population, 31 also occurred in the IT Registry population.

We interviewed personnel and reviewed information security documentation from DISA Centers and Detachments, as well as the Navy, Marine Corps, Army, Air Force, Defense Finance and Accounting Service, and Defense Logistics Agency.

We analyzed DoD Directives, Instructions, and other guidance to determine whether information assurance and security policies and procedures were clear, comprehensive, and consistent with Federal policy and one another. We compared certification and accreditation documentation to DoD and Component guidance for determining compliance. See Methodology for details of the sample selected from the Center and Detachment population of applications.

Limitations to Scope. We did not review the management control program because DoD recognized information security and assurance programs as a material weakness in its FY 1999 Statement of Assurance, which was its most recent signed Statement of Assurance.

DoD-Wide Corporate Level Government Performance and Results Act Coverage. In response to the Government Performance and Results Act, the Secretary of Defense annually establishes DoD-wide corporate level goals, subordinate performance goals, and performance measures. This report pertains to achievement of the following corporate level goal and performance measure.

- **FY 2001 DoD Corporate Level Goal 2:** Prepare now for an uncertain future by pursuing a focused modernization effort that maintains U.S. qualitative superiority in key warfighting capabilities. Transform the force by exploiting the Revolution in Military Affairs, and reengineer the Department to achieve a 21st century infrastructure. **(01-DoD-02)**

- **FY 2001 Performance Measure 2.5.3:** Qualitative Assessment of Reforming Information Technology (IT) Management. **(01-DoD-2.5.1.)**.

DoD Functional Area Reform Goals. Most major DoD functional areas have also established performance improvement reform objectives and goals. This report pertains to achievement of the following functional area objective and goal.

> **Information Management Functional Area. Objective:** Ensure DoD's vital information resources are secure and protected. **Goal:** Make Information Assurance (IA) an integral part of DoD Mission Readiness Criteria. **(IM-4.1)**

GAO High-Risk Area. The GAO lists information assurance as a high-risk area. Although the Secretary of Defense annually establishes DoD-wide corporate level goals and performance measures to address the requirements of the Government Performance and Results Act, the DoD does not currently provide corporate level goals for information assurance.

Methodology

To assess the information technology security posture of DoD, we selected a random sample of applications from a subset of systems. For those applications, the objective was to identify security personnel, such as the ISSO and the DAA, and to determine whether the applications had a C and A or an IATO. We constructed a spreadsheet in which to compile and analyze results from our subset of systems.

Use of Computer-Processed Data. Computer-generated information was the source for selecting the subset, but was not used as evidence in a finding.

Universe and Sample. We defined applications operating or residing on the DISA Centers and Detachments as our subset of systems, the universe for this sample. In response to our request for DISA supported-applications, DISA Western Hemisphere provided a listing of 4,939 applications on Center and Detachment systems that were billed to customers. Analysis of the 4,939 applications determined that multiple occurrences of the same names appeared. Operations research analysts from the Quantitative Methods Division, Office of the Assistant Inspector General for Auditing, aggregated the list based on unique-named applications, which left 1,365 applications. The analysts then generated a simple random sample of 90 applications.

Measurement Issues. The listing of applications that DISA Western Hemisphere provided consisted of every line item billed by DISA. Some items were not, in fact, applications, but space on the network that customers must pay to use. Inactive or unacknowledged applications were also found, so the sample items could not be tested for the attributes demonstrating security policy

implementation. See Appendix C for details of the 90 sample applications. The sample results categories and the number of applications in each category are shown below:

Table A1. Sample Results by Certification and Accreditation Status Category

Category	Sample Result
Current C and A or IATO	33
Out of Date C and A or IATO	2
No C and A and no IATO, or incomplete	19
Other IT	9
Unable to test the C and A and IATO status	27
Total	**90**

Measurement Results. The operations research analysts projected these sample results to the subset universe of 1,365 applications using a 90 percent confidence level. The results shown in the report are the point estimates projected. The complete results of the projections are shown below:

Table A2. Certification and Accreditation Status Projected to the Population of Applications

Category	Lower Bound	Point[1] Estimate	Upper Bound
Current C and A or IATO	383	501	618
Out of date C and A or IATO	--[2]	30	72
No C and A and no IATO, or incomplete (certification only)	187	288	389
Other IT	60	137	213
Unable to test the C and A and IATO status	297	410	522

[1]The point estimate does not add up to the population due to rounding.
[2]The lower bound estimate is below zero, therefore, it is not reported.

Use of Audit Assistance. The Air Force Audit Agency and the Army Audit Agency gathered and analyzed data for those sample items that belonged to customers within their respective Component. The Air Force Audit Agency gathered and analyzed data for 19 sample items, and the Army Audit Agency gathered and analyzed data for 34 sample items. The data were merged into a common spreadsheet for interpretation of the overall sample results.

Use of Technical Assistance. One computer engineer from the Technical Assessment Division, Office of the Assistant Inspector General for Auditing, assisted in planning the audit. In addition, two operations research analysts from the Quantitative Methods Division, Office of the Assistant Inspector General for Auditing, assisted in selecting the random sample from the subset of applications and interpreting the results.

Audit Type, Dates, and Standards. We conducted this program audit from January through July 2001, in accordance with generally accepted Government auditing standards, except that we did not have time to independently retest or validate the audit work of the Army Audit Agency and the Air Force Audit Agency. In addition, we were unable to obtain an opinion on our system of quality control. Our most recent external quality control review was withdrawn on March 15, 2001, and we will undergo a new review.

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

Appendix B. Prior Coverage

GAO

GAO Report No. GAO-01-525, "Information Technology: Architecture Needed to Guide Modernization of DoD's Financial Operations," May 17, 2001

GAO Report No. GAO-01-307, "Information Security: Progress and Challenges to an Effective Defense-wide Information Assurance Program," March 30, 2001

GAO Report No. GAO-01-341, "Information Security: Challenges to Improving DoD's Incident Response Capabilities," March 29, 2001

Inspector General, DoD

Inspector General, DoD, Report No. D-2001-044, "Accreditation Policies and Information Technology Controls at the Defense Enterprise Computing Center Mechanicsburg," February 9, 2001

Inspector General, DoD, Report No. D-2001-017, "Unclassified but Sensitive Internet Protocol Router Network Security Policy," December 12, 2000

Inspector General, DoD, Report No. D-2001-016, "Security Controls Over Contractor Support For Year 2000 Renovation," December 12, 2000

Inspector General, DoD, Report No. D-2000-124, "Information Assurance Challenges - A Summary of Audit Results Reported December 1, 1998, Through March 31, 2000," May 15, 2000

Inspector General, DoD, Report No. 99-069, "Summary of Audit Results - DoD Information Assurance Challenges," January 22, 1999

Appendix C. Sample Application Results

From the randomly selected sample of 90 applications operating or residing on DISA Centers and Detachments, the points of contact for 54 applications acknowledged the applications. For those 54 applications, the status was as follows:

- 6 had current C and As,
- 27 had current IATOs,
- 1 had an expired C and A,
- 1 had an expired IATO,
- 12 had certifications and no accreditation (grouped with no C and A in finding),
- 7 did not have a C&A, an IATO, or a certification without an accreditation.

For the 54 applications discussed above, managers for 52 had assigned a DAA and for 51 had assigned an ISSO. A summary of the results appears in the table on the following pages.

The table also lists the items that did not meet the criteria for applications and the reason the items did not fit. From the randomly selected sample of 90, the using or bill paying customer identified 9 sample items as other information technology residing on Center systems. The DISA customer points of contact for 15 sample items did not recognize the application name as one supporting their functions or as a segment of a larger application supporting their functions. Therefore, the status of those items for security officials and security procedures was undetermined. Also, the status of applications for C and A or IATO could not be established as follows: 6 retired, 3 classified, 2 unfielded (in development), and 1 transferred to a non-DISA service provider. A summary of the results appears in the table on the following pages.

Results of Sample

	Application Name	Owner	C&A		IATO		Cert. Only		No C&A, IATO, or Cert.	DAA		ISSO		See Notes
			Current	Out-of-Date	Current	Out-of-Date	Current	Out-of Date		Yes	No	Yes	No	
1.	(AC/AG/AK/AO/AS/AW) Personnel Data System Civ	AFPC*	X							X		X		
2.	Automated Data Report Submission System	Air Force Communications Agency and Standard System Group	X							X			X	
3.	Personnel Data System Mil (Dual CBPO)	AFPC	X							X		X		
4.	Comprehensive Engine Management System	AFMC	X							X		X		
5.	Comprehensive Engine Management System TCTO Mgt	AFMC	X							X		X		
6.	Central Procurement Accounting System	DFAS	X							X		X		
7.	Cooperative Log Supply Spt. Arrangements Spt. List	CECOM-LSSO		X						X		X		
8.	Interactive Voice Response System/EDIFY/ACD	DLA-HROC			X					X		X		
9.	Management Analysis and Statistical System	DLA			X					X		X		
10.	Online Job Announcement Builder	DLA-HROC			X					X		X		
11.	Status of Funds System	DFAS-DE			X					X		X		
12.	Puget Sound DSS Processing	J-64			X					X		X		
13.	Ammunition Surveillance	OSC			X					X		X		
14.	Methods & Standards	DFAS			X					X		X		
15.	Automated Digital Network System	HQ DLA Complex ITS			X					X		X		
16.	Automated Bidset Interface	Defense Supply Center Philadelphia			X					X		X		

*See acronym list on page 23.

Results of Sample (cont'd)

	Application Name	Owner	C&A		IATO		Cert. Only		No C&A, IATO, or Cert.	DAA		ISSO		See Notes
			Current	Out-of-Date	Current	Out-of-Date	Current	Out-of-Date		Yes	No	Yes	No	
17.	Quality Assurance Maint Insp	OSC			X					X		X		
18.	Army Master Data File Update	CSC-StL			X					X		X		
19.	Budget Stratification Correction LDV Processing				X					X		X		
20.	Catalog Data Element Preparation	CSC-StL			X					X		X		
21.	CCSS/PADS Communication	CSC-StL			X					X		X		
22.	Closeout/Carryover Purge	CSC-StL			X					X		X		
23.	Exercise Capability	CSC-StL			X					X		X		
24.	Fielding Requirements Data Base Explosion	CSC-StL			X					X		X		
25.	Log Pipeline Analyzer Extract	CSC-StL			X					X		X		
26.	Repair Parts and Special Tools List File Maint	CSC-StL			X					X		X		
27.	Requirements Computation	CSC-StL			X					X		X		
28.	Supply Control Study Format and Print	CSC-StL			X					X		X		
29.	User Command Requisitions	CSC-StL			X					X		X		
30.	Cost Distribution Adjustment Retrieval and Update	CSC-StL			X					X		X		
31.	Industrial Base Engineering Post War Requirements	CSC-StL			X					X		X		
32.	Interfund Disbursement Process	CSC-StL			X					X		X		
33.	Operational Project Database Conversion	CSC-StL			X					X		X		
34.	Radioactive/Hazardous Data Base	CSC-StL			X					X		X		
35.	Financial Inventory Reporting System	OPLOC San Diego				X				X		X		
36.	Virtual MISR	FMSO					X			X		X		
37.	(FI) Aero Veh & Sel Items of Equip MSN CAP/AWP Rpt	AF/ILSP & AFMC/LG					X			X		X		
38.	(ZT) Shipping Information System	AFMC					X			X		X		
39.	Maintenance Planning and Execution	AFMC/LG					X			X		X		

Results of Sample (cont'd)

	Application Name	Owner	C&A		IATO		Cert. Only		No C&A, IATO, or Cert.	DAA		ISSO		See Notes
			Current	Out-of-Date	Current	Out-of-Date	Current	Out-of-Date		Yes	No	Yes	No	
40.	General IDMS CV	FMSO					X			X		X		
41.	DLSC & In-House Screening	FMSO						X		X		X		
42.	General Purpose R/T Retrieve Programs	FMSO						X		X		X		
43.	Gen Update Utilities	FMSO						X		X		X		
44.	Family Relations	FMSO						X		X		X		
45.	Load List Consolidation	FMSO						X		X		X		
46.	Purchase Support Operation	FMSO						X		X		X		
47.	UICP-IM Sup ATD	FMSO						X		X		X		
48.	Program Budget and Accounting System-Order Control	DFAS							X	X		X		
49.	ITEM Applications	MCLBASE Albany							X	X		X		
50.	WRM List RQR & Spares Supt Lists System	AFMC							X	X		X		
51.	(C8) AFMC 181 System	AFMC							X	X		X		
52.	AFLC Management and Control of Provisioning	AFMC							X	X		X		
53.	Recurring Reports	Marine Corps, Manpower & Reserve Affairs							X		X		X	
54.	Tool Inventory MGT Application	AFMC/LG							X		X		X	
55.	Stock Point Data	Commander Naval Supply Systems Command									X		X	D
56.	File Quality Assurance Programs	NAVICP Mechanicsburg									X		X	D
57.	Microfiche Dist	NAVICP Mechanicsburg									X		X	D
58.	Resystem String Test DB Load	NAVICP Mechanicsburg									X		X	D
59.	Temp Work Data Sets	NAVICP Mechanicsburg									X		X	D
60.	THF	Naval Sea Logistics Center Mechanicsburg									X		X	D
61.	Exchange E-Mail	Air Logistics Center Defense Megacenter-Ogden									X		X	D

Results of Sample (cont'd)

	Application Name	Owner	C&A		IATO		Cert. Only		No C&A, IATO, or Cert.	DAA		ISSO		See Notes
			Current	Out-of-Date	Current	Out-of-Date	Current	Out-of-Date		Yes	No	Yes	No	
62.	Message Transfer Agent	Air Logistics Center Defense Megacenter-Ogden									X		X	D
63.	Web Connect Processing	Air Logistics Center Defense Megacenter-Ogden									X		X	D
64.	CAIMS 85 Trans Prod Library	Naval Ordnance Center Ammunition Atlantic Division									X		X	C
65.	Allow Process	Naval Ordnance Center Ammunition Atlantic Division									X		X	C
66.	IM Decision Making	Naval Ordnance Center Ammunition Atlantic Division									X		X	C
67.	DFAS Integration Engine	DFAS									X	X		I
68.	Defense Procurement Payment System	DFAS									X		X	I
69.	Cost Performance and Production Module	Air Logistics Center Defense Megacenter-Ogden									X		X	N
70.	Master Index Allowance	NAVICP Mechanicsburg									X		X	R
71.	NAVSEA OP-Review IDMS CV	Naval Sea Logistics Center Mechanicsburg									X		X	R
72.	(GW) MICAP Automated Sourcing System	Air Combat Command									X		X	R
73.	AMC Reports of Discrepancy Tracking System	ACALA									X		X	R
74.	Army Procurement Appropriation Commitments	ACALA									X		X	R
75.	Defense Std Ammunition Computer Sys	Army Materiel Command/ Army Anniston Depot									X		X	R
76.	Financial Reporting	NAVICP Mechanicsburg									X		X	U
77.	(PI) Visibility and Management of Op and Supt Cost Prepoc	AFMC									X		X	U
78.	APAACT-LSSA Reconciliation Extract	ACALA									X		X	U

Results of Sample (cont'd)

	Application Name	Owner	C&A		IATO		Cert. Only		No C&A, IATO, or Cert.	DAA		ISSO		See Notes
			Current	Out-of-Date	Current	Out-of-Date	Current	Out-of-Date		Yes	No	Yes	No	
79.	Army Procurement Appropriation Reports Process	ACALA									X		X	U
80.	Reject Dollar Amts by Appropriation and DOC ID COD	ACALA									X		X	U
81.	Somards Batch Edit Process	ACALA									X		X	U
82.	Std Labor Master List by Cost CTR Manager Process	ACALA									X		X	U
83.	Integrated Facilities System Document File	LOGSA									X		X	U
84.	Clear Files	ACALA									X		X	U
85.	Delmars Weekly Report	ACALA									X		X	U
86.	Mainframe Interlink Data Access System	LOGSA									X		X	U
87.	Marine Corps Reserve Support Center Mgmt System	DFAS-KC									X		X	U
88.	Readiness Integrated Database	LOGSA									X		X	U
89.	Unit Item Tracking	LOGSA									X		X	U
90.	Ammunition Demand Automated Process	Industrial Operation Command									X		X	U

Notes:
- D Data Set/Database/Software Tool
- C Classified
- R Retired
- N Not operating on DISA Platform
- I In Development
- U Unknown (ambiguous application name/could not be identified)

ACALA	U.S. Army Armament and Chemical Acquisition and Logistics Agency
AFMC	Air Force Materiel Command
CECOM	Communications Electronics Command (Army)
Cert.	Certification
CSC-StL	Computer Science Corporation – St. Louis
DE	Denver
DFAS	Defense Finance and Accounting Service
DLA	Defense Logistics Agency
FMSO	Fleet Materiel Supply Office
HROC	Human Resource Operations Center
HQ	Headquarters
AF/IL	Headquarters Air Force, Deputy Chief of Staff for Installations and Logistics
ILSP	Integrated Logistics Support Program
ITS	Integrated Technology Security
J-64	DLA Enterprise Business Systems, Directorate J-64
KC	Kansas City
LOGSA	Logistics Support Activity (U.S. Army Materiel Command)
LSSO	Logistics Systems Support Office
LG	Defense Communications Systems/Logistics
MCLBASE	Marine Corps Logistics Base
MSG	Materiel Systems Group (Air Force)
NAVICP	Naval Inventory Control Point
OPLOC	Operating Location
OSC	U.S. Army Operations Support Command

Appendix D. Report Distribution

Office of the Secretary of Defense

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

Department of the Army

Chief Information Officer, Department of the Army
Auditor General, Department of the Army

Department of the Navy

Assistant Secretary of the Navy (Manpower and Reserve Affairs)
Commandant, Marine Corps
Naval Inspector General
Auditor General, Department of the Navy
Navy Chief Information Officer

Department of the Air Force

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

Other Defense Organizations

Inspector General, Defense Intelligence Agency
Director, Defense Logistics Agency
Director, Defense Finance and Accounting Service
  Chief Information Officer
Inspector General, Defense Information Systems Agency

Non-Defense Federal Organization

Office of Management and Budget
General Accounting Office

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

Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) Comments

COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE

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

31 AUG 2001

MEMORANDUM FOR INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE

SUBJECT: Audit Report on Implementation of DoD Information Security Policy for Processing Accomplished at Defense Enterprise Computing Centers (Project D2001AD-0071)

This office has reviewed the draft report and has the following comments.

While DoD Directive 5200.28 is cited as out of date, it has been supplemented by the DoD CIO Guidance and Policy Memorandum 6-8510, DoD Global Information Grid (GIG) Information Assurance and Information Assurance Implementation Guide, dated June 16, 2000. The draft report makes no mention of that important contemporary guidance, which was developed under the sponsorship of the DoD CIO Executive Board in parallel with other GIG memoranda addressing issues such as networks, network operations, information management and enterprise computing, all of which also addressed security and IA in the context of their subject matter. It should also be noted that a draft DoD Directive 8500.1, Information Assurance, and a draft DoD Instruction 8500.2, Information Assurance Implementation, have been prepared to replace both DoD Directive 5200.28 and Policy Memorandum 6-8510. Those issuances should be in formal coordination in October 2001. Additionally, DoD Instruction 5200.40, DITSCAP, is being revised to better define the certification and accreditation process and address problems such as those identified in this audit. It will be issued as DoD Instruction 8510.1 in early 2002.

The first sentence of the last paragraph on page three of the draft report assigns responsibility for all DoD information security deficiencies to a lack of definitions for system and application, along with unclear means for establishing security parameters and responsibilities. It seems to us the problem is much more complex and involves such issues as Title 10 responsibilities and authorities, allocation of resources, and rapid technology turnover. Finally, we do not agree with the auditor's interpretation that DoD Directive 5200.28 applies to data sets and databases (page 6 of the draft report). The audit notes that although these items are not specifically mentioned, they are also not specifically excluded, and that since they are resident on a computer, they should be subject to a security evaluation. This is incorrect, as this interpretation would require all

"files" to be certified and accredited. The applications that created the data/databases should be evaluated, not the files they create.

My point of contact for this action is Mr. Gus Guissanie, (703) 614-6132, e-mail: gary.guissanie@osd.mil.

Robert F. Lentz
Director, Information Assurance

Department of the Army Comments

Office, Director of Information Systems for Command, Control, Communications, & Computers

DEPARTMENT OF THE ARMY
OFFICE OF THE SECRETARY OF THE ARMY
107 ARMY PENTAGON
WASHINGTON DC 20310-0107

SAIS-IAS (380-19)

5 September 2001

MEMORANDUM FOR U.S. ARMY AUDIT AGENCY, ATTN: MR. ANGEL RIAZ

SUBJECT: Audit Report on Implementation of DoD Information Security Policy for Processing Accomplished at Defense Enterprise Computing Centers (Project D2001AD-0071)

1. Reference: Audit Report on Implementation of DOD Information Security Policy for Processing Accomplished at Defense Enterprise Computing Centers (Project D2001AD-0071

2. We concur with the DoD Inspector General recommendations in paragraph 2, subparagraphs 2a and 2b, of reference stating that the Chief Information Officers for the Army, Navy, Air Force, Defense Finance and Accounting Service, and Defense Logistics Agency perform the following:

Recommendation 2a: Use the data collected in response to the Government Information Security Reform (GISR) to identify weaknesses, such as expired accreditations, in their Components information security programs so they can provide resources to improve the programs

Response: The Army takes certification and accreditation very seriously. We are fully engaged in ensuring that the Department of Defense Information Technology Security Certification and Accreditation (C&A) Process (DITSCAP) is implemented as the standard for all our information systems. Our Information Assurance Program Managers and Information Assurance professionals at all levels are actively involved in the DITSCAP process, not only for applications that run on Department of Defense Enterprise Computing Centers (DECC) but for all information systems. Unfortunately, the GISR process clearly disclosed that the definitions/terms of reference (TOR) for applications vis-à-vis systems (such as the DECCs) are not clearly defined and that C&A requirements for applications are not well developed. One of our rcommendations to the GISR Working Group is that DoD make the development of better definitions/TOR a high priority requirement and that revisions to the DITSCAP Application Manual specifically address C&A requirements for applications and other entities. Accomplishing the definition/TOR requirement is a prerequisite to establishing timelines as indicated in reference.

SAIS-IAS
SUBJECT Audit Report on Implementation of DoD Information Security Policy for Processing Accomplished at Defense Enterprise Computing Centers (Project D2001AD-0071)

The applications selected for the subject audit came from DISA's billing records and not a central database, which makes it diffecult to track accreditation status. We suggest that DoD consider registering DECC applications in the IT Registry, possibly as a separate "applications" category aside from the Mission Critical and Mission Essential Systems. Since the component IT Registries feed the DoD IT Registry, this would provide the DoD CIO structure visibility on the status of accreditations for Mission Critical and Mission Essential systems and defense level applications.

Recommendation 2b: Coordinate information security efforts for applications and other information technology with service providers, such as the Defense Information Systems Agency, to include clearly designated security and approval officials:

Response: As noted by the above recommendation, the GISR process disclosed that officials responsible for systems and applications, to include C&A responsibilities, were not always clearly identified. To correct this situation, in August 2001 the Army directed that responsible authorities for all systems/applications currently in the DoD IT Registry review and update all currently required identifying data. In addition, at the September 2001 GISR follow up meeting, Army will recommend that the Assistant Secretary of Defense for Command Control, Computers, and Intelligence require the addition of the following Information Assurance data fields to the DoD IT Registry:

- Designated Approval Authority (DAA) identifying data, to include name, address, email address, and telephone number
- Date of accreditation
- Date of the Authority to Operate (ATO)/Interim Authority to Operate (IATO)

Army will direct that all responsible officials gather the requisite information for these new data fields so that the new fields can be populated within 30 days of the date these fields are added to the DoD IT Registry.

3. The POC for this action is Mr. William J. Buzinski, (703) 607-5888, DSN 327-5888. Email: William.Buzinski@hqda.army.mil

THADDEUS A. DMUCHOWSKI
LTC(P), GS
Director, Information Assurance

Department of the Air Force Comments

DEPARTMENT OF THE AIR FORCE
HEADQUARTERS UNITED STATES AIR FORCE
WASHINGTON, DC

MEMORANDUM FOR ASSISTANT INSPECTOR GENERAL FOR AUDITING, OFFICE OF THE INSPECTOR GENERAL DEPARTMENT OF DEFENSE

FROM: HQ AF/SCM
1250 Air Force Pentagon
Washington DC 20330-1250

SUBJECT: DoDIG Draft Report, Implementation of DoD Information Security Policy for Processing Accomplished at Defense Enterprise Computing Centers, (Project Code D2001AD-0071)

We concur with the findings and recommendations of the DoDIG Draft Report of Audit in subject line. Specific management comments are attached.

If you have any questions or concerns with our comments, please contact Mr. Charlie Vaughters, AF/SCMIP, DSN 425-6177.

Michael C. Marro

MICHAEL C. MARRO, Colonel, USAF
Deputy Director of IT Enterprise Operations

Attachment:
Management Comments

Inspector General
Department of Defense
Draft Report of Audit, Implementation of DoD Information Security Policy for
Processing Accomplished at Defense Enterprise Computing
(Project D2001AD-0071)

Recommendation:

2. We recommend that the Chief Information Officers for the Army, Navy, Air Force, the Defense Finance and Accounting Service, and the Defense Logistics Agency:

a. Use the data collected in response to the Government Information Security Reform (GISR) to identify weaknesses, such as expired accreditations, in their Component information security programs so they can provide resources to improve the programs.

b. Coordinate information security efforts for applications and other information technology with service providers, such as the Defense Information Systems Agency, to include clearly designated security and approval officials.

AF/SCM Comments:

2. Concur. AF/SC will

Incorporate GISR data fields into the AF/SC System Compliance Database (SCD). The SCD will be utilized to track AF systems for Certification and Accreditation (C&A) process and Government Information System Reform requirements. The SCD will allow us to track mandatory requirements and coordinate information security efforts.

The Acting AF CIO has made information security a priority. The Air Force had recently collected similar data, also in support of GISR, which yielded similar findings. The Acting AF CIO has already taken aggressive steps and has built a Tiger Team, consisting of Air Force experts, to construct and guide the Air Force's implementation of an information assurance strategy. Our strategy will be a collaborative effort with both affected Air Force personnel and external agencies, such as DISA and OSD - Defense Information Assurance Program (DIAP). The Acting AF CIO continues to make information security a high interest item throughout the Air Force and is committed to securing the Air Force's information in support of the warfighter.

Defense Information Systems Agency Comments

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

IN REPLY
REFER TO: INSPECTOR GENERAL (IG) 4 September 2001

MEMORANDUM FOR INSPECTOR GENERAL, DEPARTMENT OF DEFENSE

SUBJECT: Response to DOD IG Draft Report: Implementation of DoD Information Security Policy for Processing Accomplished at Defense Enterprise Computing Centers Project (Project No. D2001AD-0071)

1. The enclosed document provides a response from the Defense Information Systems Agency on the subject DoD IG Draft report.

2. If you have any questions, please call Teddie Lou Steiner, Audit Liaison, at (703) 607-6316 or Liz Lippmann, Assistant Audit Liaison, at (703) 607-6306.

FOR THE DIRECTOR:

Enclosure a/s

RICHARD T. RACE
Inspector General

Quality Information for a Strong Defense

INTEROFFICE MEMORANDUM

TO: Inspector General (IG)

FROM: Commander, DISA WESTHEM (WE)

DATE: AUG 31

SUBJECT: Response to DOD IG Draft Report, Project D2001AD-0071

Reference: Implementation of DOD Information Security Policy for Processing Accomplished at Defense Enterprise Computing Centers Project, dated 8/3/01

Preparer: G. Knaggs/WE05/681-2246

1. DISA WESTHEM concurs with the need for an ever-increasing vigilance in assuring a secure information technology environment, as referenced in the subject report. Our organization has taken a number of proactive steps to ensure that the support WESTHEM provides to the Services and Defense Agencies, and ultimately the warfighter, meets this requirement. We view this as a shared responsibility and actively partner with our customers and vendors to accomplish our distinct roles and responsibilities in meeting the requirements of the Government Information Security Reform Act.

2. WESTHEM's response to the subject report has been revised to address comments provided by Ms. Teddie Steiner, Office of the Inspector General (IG), and is forwarded as an enclosure.

PAUL E. HALLOWELL
Vice Commander

1 Enclosure:
Revised Response

Copy to:

Field Security Office (D331)
WESTHEM Operations (WE03)
WESTHEM Business Management (WE05)

DODIG DRAFT REPORT
DODIG CODE # D2001AD-0071

IMPLEMENTATION OF DOD INFORMATION SECURITY POLICY FOR PROCESSING ACCOMPLISHED AT DEFENSE ENTERPRISE COMPUTING CENTERS PROJECT

We recommend that the Commander, Defense Information Systems Agency, Western Hemisphere:

a. Coordinate information security efforts with customers to obtain their statements of approval to operate when beginning service arrangements and periodically, thereafter.

RESPONSE: Concur. WESTHEM currently specifies in each Service Level Agreement (SLA) that the customer is responsible for the system or application's certification and accreditation (C/A). Henceforth, the customer will be asked to provide materials that document that either C/A has been completed or what steps have been taken to accomplish C/A, a schedule for its completion, and what risks the customer is assuming in implementing the work prior to fully completing the C/A process. This guidance will be promulgated to our Headquarters elements and all field activities through a WESTHEM Commander's policy letter that will be distributed no later that October 1, 2001.

b. Maintain a resource listing of officials responsible for information security for each customer of the Defense Enterprise Computing Centers and Detachments. Those officials should be contacted if their application is the source of security risks or affected by other customer or Defense Enterprise Computing Centers risks.

RESPONSE: Concur. All WESTHEM operational sites currently maintain the names and contact information for functional points of contact (POCs) for all of the applications that run on systems at Defense Enterprise Computing Centers (DECCs) and Detachments (Dets). These functional POCs provide the interface between customers and DECCs and Dets to address operational problems, as required. If a security-related issue occurs, WESTHEM site personnel coordinate through the customer's functional POCs to resolve the problem with both the customer's functional and security personnel. As the majority of customer contacts are non-security related, this process meets the DECCs and Dets need to resolve operational issues quickly with their key points of contact while having a ready access to each customer's security personnel, which is needed only periodically.

DODIG DRAFT REPORT
DODIG CODE # D2001AD-0071

c. Establish a monitoring process and performance goal for Defense Enterprise Computing Centers to document current certifications and accreditations, interim authority to operate, and the designated approval authority and information systems security officer for all customers by the end of the FY 2002 Government Information Security Reform reporting period.

RESPONSE: Non-Concur. Clearly, this is an Office of the Secretary of Defense (OSD) policy issue. DISA WESTHEM supports the idea of having a central repository for Designated Approval Authority (DAA) information for applications and major systems. Since the authority for accreditation and appointment of responsible security personnel rests with the DAAs, we recommend that either a central repository be developed or that the IT registry be expanded to allow maintenance of this database at the OSD level. Previous efforts at the DISA WESTHEM level to obtain and maintain current, reliable customer information have proven unsuccessful. Only OSD is in the position to require the Services and DoD agencies to update and maintain their portion of the records on a predetermined, recurring basis.

Defense Logistics Agency Comments

DEFENSE LOGISTICS AGENCY
HEADQUARTERS
8725 JOHN J. KINGMAN ROAD, SUITE 2533
FT. BELVOIR, VIRGINIA 22060-6221

IN REPLY REFER TO J-3

31 AUG 2001

MEMORANDUM FOR ASSISTANT INSPECTOR GENERAL FOR AUDITING
DEPARTMENT OF DEFENSE

SUBJECT: Implementation of DoD Information Security Policy for Processing Accomplished at Defense Enterprise Computing Centers, D2001AD-0071

Enclosed is our response to the subject draft report dated August 3, 2001. If you have any questions, please contact Mrs. Peggy Hayes, (703) 767-6262.

Encl

HAWTHORNE L. PROCTOR
Major General, USA
Director, Logistics Operations

31 AUG 2001

SUBJECT: Implementation of DoD Information Security Policy for Processing Accomplished at Defense Enterprise Computing Centers (Project No. D2001AD-0071)

FINDING: Implementation of DoD Information Security Policy.

DoD managers had not fully implemented information security policy for the DISA Center-and Detachment-supported applications, as shown by the number of applications that had written, current certification and accreditation (C and A) or interim authority to operate (IATO). Written, current C and As were not available for an estimated 60 percent of applications residing on Center and Detachment computer systems. The projected point estimate to the population of 1,365 for authority to operate for the sample of 90 applications were as follows:

	Projected Results	Percent of Population
Current C and A or IATO	501	36.7
Indeterminate: retired, transferred, insufficient detail available to find status	410	30.0
Other technology with no C and A or IATO	137	10.0
Expired C and A or IATO	30	2.2
No C and A or IATO, or certification only	288	21.1
Total	**1,366**	**100.0**

The DoD managers had not fully implemented information security policy because definitions for system, application, and other means of establishing security parameters and responsibilities were unclear. The parameters of and responsibility for information security were further obscured by the DoD practice of approving different organizations to design, develop, manage, use, and operate IT applications. In addition, the policy proponent, the Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) [ASD (C3I)]; the service provider, DISA; and the Component heads provided little oversight of policy implementation or policy applicability to the current IT environment. As a result of incomplete policy implementation, DoD managers assumed risks to IT that were not fully identified, assessed, accepted, and managed as a result of a deliberative process. Unmanaged risk could lead to loss of service, data corruption, unauthorized access, sabotage, tampering, misuse, and fraud in DoD IT systems and applications.

INTERNAL MANAGEMENT CONTROL WEAKNESS:
Concur; weakness will be reported in the DLA Annual Statement of Assurance.

ACTION OFFICER: Dennis Heretick, J-633, 703 767-1587
J-6 APPROVAL: Capt Ted Case

31 AUG 2001

SUBJECT: Implementation of DoD Information Security Policy for Processing Accomplished at Defense Enterprise Computing Centers (Project No. D2001AD-0071)

RECOMMENDATION 2: We recommend that the Chief Information Officers for the Army, Navy, Air Force, the Defense Finance and Accounting Service, and the Defense Logistics:

a. Use the data collected in response to the Government Information Security Reform Act to identify weaknesses, such as expired accreditations, in their Component information security programs so they can provide resources to improve the programs.

b. Coordinate information security efforts for applications and other information technology with service providers, such as the Defense Information Systems Agency, to include clearly designated security and approval officials.

DLA COMMENTS:
a. DLA has used data collected in response to Government Information Security Reform (GISR) to identify weaknesses. These security weaknesses have been identified in the DLA IA Program Plan, dated June 2001 and System Security Authorization Agreements (SSAAs) for DLA's systems, networks and web sites. Schedules to mitigate these security weaknesses have also been planned and/or implemented. Resources required for implementation have been identified in DLA's budget and POM. SSAAs using DoDI 5200.40, Defense Information Technology Security Certification and Accreditation Process (DITSCAP), have been developed for all five of the systems selected for review in this audit. One of these systems, Automated Bidset Interface (ABI), was certified, accredited, and issued Approval to Operate (ATO) by the Designated Approving Authority (DAA) on July 29, 2001. Of the other four systems, two are currently being certified with ATO planned for completion in September 2001. The remaining two systems are planned to achieve ATO in November 2001

b. DLA information security efforts have been coordinated as part of service level agreements and memoranda of agreement. Requested copies of these documents have been provided to the DoD IG as part of this audit.

DISPOSITION: Ongoing. ECD: 30 November 2001

ACTION OFFICER: Dennis Heretick, J-633, 703 767-1587
J-6 Approval: Capt. Ted Case

Audit Team Members

The Acquisition Management Directorate, Office of the Assistant Inspector General for Auditing, DoD, prepared this report. Personnel of the Office of the Inspector General, DoD, who contributed to the report are listed below.

Mary L. Ugone
Robert K. West
Judith I. Padgett
Walter L. Jackson
Bryon J. Farber
Heather L. Jordan
Setranique T. Clawson
Mandy L. Rush
Richard O. Williams
Henry D. Barton
Dharam V. Jain
Ann Ferrante
Jacqueline N. Pugh

INTERNET DOCUMENT INFORMATION FORM

A . Report Title: Implementation of DOD Information Security Policy for Processing Accomplished at Defense Enterprise Computing Centers

B. DATE Report Downloaded From the Internet: 11/01/01

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

D. Currently Applicable Classification Level: Unclassified

E. Distribution Statement A: Approved for Public Release

F. The foregoing information was compiled and provided by:
DTIC-OCA, Initials: __VM__ **Preparation Date 11/01/01**

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