# Audit Report

OFFICE OF THE INSPECTOR GENERAL

**INFORMATION RESOURCES MANAGEMENT AT THE DEFENSE INFORMATION SYSTEMS AGENCY**

Report No. 94-080

April 11, 1994

## Department of Defense

**Additional Copies**

To obtain additional copies of this report, contact the Secondary Reports Distribution Unit, Audit Planning and Technical Support Directorate, at (703) 614-6303 (DSN 224-6303) or FAX (703) 614-8542.

**Suggestions for Future Audits**

To suggest ideas for or request future audits, contact the Planning and Coordination Branch, Audit Planning and Technical Support Directorate, at (703) 614-1868 (DSN 224-1868) or FAX (703) 614-8542. Ideas and requests can also be mailed to:

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

**DoD Hotline**

To report fraud, waste, or abuse, call the DoD Hotline at (800) 424-9098 (DSN 223-5080) or write to the DoD Hotline, The Pentagon, Washington, D.C. 20301-1900. The identity of writers and callers is fully protected.

**Acronyms**

| | |
|---|---|
| ARMS | Automation Resources Management System |
| AIS | Automated Information System |
| DCA | Defense Communications Agency |
| DISA | Defense Information Systems Agency |
| DISANET | Defense Information Systems Agency Network |
| DECCO | Defense Commercial Communications Office |
| FAR | Federal Acquisition Regulation |
| FIRMR | Federal Information Resources Management Regulation |
| GSA | General Services Administration |
| IRM | Information Resources Management |
| ITABBS | Information Technology Acquisition Bulletin Board System |
| OSD | Office of the Secretary of Defense |
| TMSO | Telecommunications Management and Services Office |
| WWOLS | Worldwide On Line System |

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

April 11, 1994

MEMORANDUM FOR DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY

SUBJECT: Audit Report on Information Resources Management at the Defense Information Systems Agency (Report No. 94-080)

We are providing this final report for your review and additional comments. The report focuses on the management of information resources within the Defense Information Systems Agency. We concluded that the Defense Information Systems Agency needs to strengthen its policies, programs, and procedures for overseeing the management and use of information resources. We also determined that the security of automated information systems did not comply with Federal and DoD requirements and information in those systems may not be adequately protected.

Comments on a draft of this report were considered in preparing the final report. Management concurred in all recommendations in the draft report, however, we could not determine how the planned actions in response to Recommendation A.2.b., which concerns verification of automated information system life-cycle management practices, will be implemented to achieve the corrective action intended. Clarification on this matter should be provided in response to this final report.

DoD Directive 7650.3 requires that all audit recommendations be resolved promptly. Therefore, we request that you provide comments in response to this final report by June 10, 1994.

The courtesies extended to the audit staff are appreciated. If you have any questions on this audit, please contact Ms. Mary Lu Ugone at (703) 692-3320 (DSN 222-3320) or Mr. James W. Hutchinson at (703) 692-2898 (DSN 222-2898). Copies of this report will be distributed to the organizations listed in Appendix H.

Robert J. Lieberman
Assistant Inspector General
for Auditing

## Office of the Inspector General, DoD

Report No. 94-080 April 11, 1994
(Project No. 2RE-0049)

# INFORMATION RESOURCES MANAGEMENT AT THE DEFENSE INFORMATION SYSTEMS AGENCY

## EXECUTIVE SUMMARY

**Introduction.** The Assistant Secretary of Defense (Command, Control, Communications and Intelligence) asked the Inspector General, DoD, to review the Defense Information Systems Agency (DISA) Information Resources Management (IRM) Program. Within DISA, the Chief Information Officer is responsible for the effective and efficient acquisition, management, and use of information and information systems supporting DISA's requirements. The Chief Information Officer develops and implements policies, programs, and procedures to plan for, manage, and control information resources. For FYs 1992 and 1993, DISA budgeted about $875 million for its information resources.

**Objective.** The audit objective was to determine whether DISA effectively and efficiently managed its information resources in accordance with Federal and DoD requirements and guidelines. We also evaluated related internal controls.

**Audit Results.** Oversight of DISA's IRM programs and functions needed improvement.

o The oversight role of the Chief Information Officer had not been clearly defined, enhanced oversight procedures and policies were needed, and internal controls were undocumented. Accordingly, the Chief Information Officer could not validate that IRM resources were effectively and efficiently used or managed in accordance with Federal policy and requirements (Finding A).

o Senior Agency managers had not endorsed the security posture for 24 of 45 automated information systems as adequate, the Chief Information Officer had not implemented an effective Automated Information System Security Review Program, and training for security personnel and users was inadequate. As a result, systems did not meet security requirements and DISA had little assurance its systems were reasonably protected (Finding B).

**Internal Controls.** The audit identified internal control weaknesses, but they were not considered material. The Chief Information Officer needed to use a disciplined process to develop a system of internal controls and to enhance controls for overseeing the management of agency information resources. Part I of the report discusses the controls assessed, and the findings in Part II discuss the weaknesses.

**Potential Benefits of Audit.** DISA will have accurate, complete, and current information on which to base decisions on acquiring and managing IRM resources. Additionally, DISA's Automated Information System Security Program will meet Federal and DoD security requirements. No monetary benefits are associated with this report, but other potential benefits are described in Appendix F.

**Summary of Recommendations.** We recommended that DISA clarify information resources management and oversight roles and responsibilities, strengthen oversight of its IRM programs and activities, issue uniform acquisition policies and procedures, and improve the Chief Information Officer's system of internal management controls. Additionally, we recommended that automated information system security be reemphasized on an agency-wide basis and that related training, guidance, and oversight be improved.

**Management Comments.** The Director, Defense Information Systems Agency, concurred with all recommendations. A discussion of the DISA comments is in Part II, and the complete text of the comments is in Part IV.

**Audit Response.** We consider DISA's comments to be responsive to the draft report except for one recommendation regarding verification of life-cycle management practices. We could not determine how the recommendation would be accomplished through the actions described. We requested that DISA provide additional comments on the unresolved issue by June 10, 1994.

# Table of Contents


Executive Summary i

**Part I - Introduction** 1

Background 2
Objective 3
Scope and Methodology 3
Internal Controls 4
Prior Audits and Other Reviews 5
Other Matters of Interest 5

**Part II - Findings and Recommendations** 7

Finding A. Oversight of Information Resources Management 8
Finding B. Automated Information Systems Security 27

**Part III - Additional Information** 33

Appendix A. Statistical Sampling Methodology 34
Appendix B. Contracts Reviewed for FIRMR Compliance 37
Appendix C. IG, DoD, Risk Assessment of the Office of the Chief Information Officer 38
Appendix D. AISs Reviewed and Related Security Data 39
Appendix E. Summary of Other DISA IRM Programs 42
Appendix F. Summary of Potential Benefits Resulting From Audit 47
Appendix G. Organizations Visited or Contacted 49
Appendix H. Report Distribution 50

**Part IV - Management Comments** 53

Defense Information Systems Agency 54

# Part I - Introduction

## Background

Historically, primary responsibilities of the Defense Information Systems Agency (DISA) have been to provide long-haul communications support to DoD Components and to support the command, control, and communications needs of the Joint Staff. Since the early 1990s, the DISA has been tasked with providing DoD-wide information management and systems support services. DISA budgeted about $375 million in FY 1992 and $500 million in FY 1993 for information resources. Those resources include automated data processing equipment, software, telecommunications, personnel, and other related information resources. The objective of the DISA's Information Resources Management (IRM) Program is to ensure that information resources are used in the most effective and efficient manner in support of DISA's mission and are in compliance with Federal and DoD laws, guidelines, and regulations. The Office of the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) requested that the IG, DoD, evaluate the effectiveness of the DISA's IRM Program.

In 1965, the Brooks Act gave the General Services Administration (GSA) overall responsibility for the management and acquisition of automated data processing equipment by Federal agencies. To help meet that responsibility, GSA requires DISA to obtain specific procurement authority to acquire information resources valued in excess of $2.5 million. GSA also publishes the Federal Information Resources Management Regulation (FIRMR), which establishes Federal requirements and procedures for acquiring and managing information resources.

In 1980, the Congress enacted the Paperwork Reduction Act to promote greater economy and efficiency in Federal agencies' information management activities. The Paperwork Reduction Reauthorization Act in 1986 expanded the Brooks Act's definition of automated data processing equipment. GSA now refers to automated data processing equipment as part of a broader definition: Federal Information Processing resources. The Paperwork Reduction Reauthorization Act requires Federal agencies to designate senior officials responsible for verifying FIRMR compliance.

As DISA's Senior Information Resources Management Representative, the Chief Information Officer is responsible for the effective and efficient acquisition, management, and use of information and information systems supporting agency requirements. In that capacity, the Chief Information Officer develops and implements policies, programs, and procedures to efficiently and effectively plan for, manage, and control information resources.

## Objective

The objective of the audit was to determine whether DISA effectively and efficiently managed its information resources in accordance with Federal and DoD requirements and guidelines. We also evaluated the internal management control system established by the Chief Information Officer.

## Scope and Methodology

**Audit Coverage.** We evaluated DISA's management of Federal Information Processing resources. To accomplish the evaluation, we patterned our audit on the methodology used by GSA to perform its Information Resources Procurement and Management Reviews. Additionally, we reviewed other IRM topics that were of particular interest to the Assistant Secretary of Defense (Command, Control, Communications and Intelligence). Specifically, we evaluated 15 IRM areas:

- o organizational structure,
- o strategic planning,
- o life-cycle management,
- o information processing equipment inventory,
- o records management,
- o reports management,
- o forms management,
- o mail management,
- o security of automated information systems,
- o management of delegations of procurement authority,
- o contracting for information processing resources,
- o IRM review program,
- o computer access by users with disabilities,
- o DISA's progress in implementing GSA's Trail Boss Program, and
- o DoD's Corporate Information Management initiative.

**Audit Period.** The audit was made from June 1992 through March 1993. Audit work was primarily done at DISA's directorates in the Washington, D.C., metropolitan area. Also, we visited DISA's directorates at Scott Air Force Base, Illinois; Fort Huachuca, Arizona; and Denver, Colorado. Organizations visited or contacted are listed in Appendix G. This economy and efficiency audit was made in accordance with auditing standards issued by the Comptroller General of the United States as implemented by the IG, DoD, and accordingly included such tests of internal controls as were considered necessary.

**Limitations and Audit Universe.** Our audit focused on information resources and systems primarily used by DISA for internal purposes. We restricted our evaluation of information resource acquisitions to internal resources procured from October 1990 through June 1992. We did not review support services or

equipment acquired for the White House, Joint Staff, or Military Departments. Also, we excluded the acquisition of long-haul telecommunications systems designed to provide DoD-wide support. However, in our opinion, the audit results and issues discussed in this report are applicable to all DISA information resources, whether used within DISA for internal purposes or in support of other DoD Components.

We examined contracting procedures used by the two DISA contracting offices to acquire internally used information resources. Using statistical sampling techniques recommended by the Quantitative Methods Division, IG, DoD, we projected that DISA's Contracts Management Division had awarded 91 contracts, valued at about $10 million, to meet internal DISA information resource needs. The other contracting office, the Defense Commercial Communications Office (DECCO), awarded 58 contracts valued at about $11 million. We did not make an assessment of information resource contracts awarded to support requirements of the Defense Information Technology Services Organization, because that organization was newly organized and was not an integral part of the DISA at the time of our audit.

**Use of Computerized Data.** We used inventory data extracted from a computerized data base, the DoD Automation Resources Management System, to evaluate the accuracy of automated data processing equipment inventory information used by DISA for planning and oversight purposes. Because we did not extensively evaluate or test related system controls, the risk exists that system control deficiencies are materially responsible for inaccurate DISA inventory records. However, we believe that risk to be extremely low when viewed in context with other factors as discussed in Part II of this report. Accordingly, we believe related opinions, conclusions, and recommendations in this report are valid.

## Internal Controls

We identified numerous internal control weaknesses; however, none were material. We reviewed the Chief Information Officer's system of internal management controls, which was developed in accordance with the DISA's implementation of the DoD Internal Management Control Program. We identified weaknesses in the process used to develop the Chief Information Officer's system of internal management controls and in individual controls related to IRM oversight and security. Each finding details internal controls assessed, discusses control deficiencies, and contains recommendations which, if implemented, should correct the weaknesses. No monetary benefits are associated with this report; however, other benefits are described in Appendix F.

## Prior Audits and Other Reviews

Office of the Inspector General, DoD, Inspections Report No. 91-INS-08, "Defense Communications Agency," May 10, 1991, addresses the effectiveness and efficiency of Defense Communications Agency (since renamed DISA) in fulfilling communication support requirements. The report describes inadequate security policies for automated information systems and their oversight and states that the DISA's organizational structure did not promote efficient or economical mission accomplishment. The report recommended updating security policies and procedures and reassessing DISA's organizational structure, functional alignment, and resources allocation. Management initiated actions to assess its organizational structure and updated the security policy for automated information systems in August 1991.

Office of the Inspector General, DoD, Inspections Report No. 89-INS-03, "Report on Information Resources Management Within DoD," February 17, 1989, and GSA report "Information Resource Procurement and Management Review, Office of the Secretary of Defense FY 1991," evaluate the effectiveness of IRM programs within DoD. The reports discuss organizational oversight; IRM policies, procedures, and guidelines; system security; life-cycle management; and procurement and contracting. The reports identified weaknesses in the oversight of IRM activities and information resource acquisition, security, FIRMR implementation, IRM program responsibility, and standardization of information resources. All recommended actions, which were addressed to the Office of the Secretary of Defense (OSD), were related to improving OSD oversight of DoD IRM programs and activities. OSD generally concurred with the recommendations and initiated actions to implement them.

Office of the Inspector General, DoD, Report No. 88-130, "Audit Report on Acquisition of Automatic Data Processing Equipment at the Defense Communications Agency," April 12, 1988, states that DISA's inventory system was inaccurate and that no formal reconciliation of inventory for data processing equipment had been made since 1984. The report recommended that management perform annual inventory reconciliations. DISA nonconcurred with the finding, stating that inventory reconciliations were performed twice a year. Our current audit concluded, however, that management had not implemented corrective actions and that DISA continues to have inventory problems (Finding A).

## Other Matters of Interest

**Other DISA IRM Areas.** The audit showed that several components of DISA's IRM Program were adequately managed and executed. Other components had relatively minor deficiencies, involved few resources, or were still in a developmental stage. Audit results for each of those information management areas are summarized in Appendix E.

**DISA Organizational Environment.** In June 1991, the Defense Communications Agency (DCA) was renamed the Defense Information Systems Agency to reflect additional mission responsibilities of providing information management support to the Assistant Secretary of Defense (Command, Control, Communications and Intelligence). In September 1992, DoD decided to implement Defense Management Report Decision 918, "Defense Information Infrastructure," which again expanded the DISA mission. Decision 918 required DISA to provide information systems support for DoD business-related functions, such as finance, accounting, and logistics. To provide that support, DISA staffing was expected to grow from about 5,000 to about 25,000. However, on June 28, 1993, the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) substantially revised the implementation of Defense Management Report Decision 918. DISA staff growth is still anticipated, but not to the level originally expected.

Beginning in 1991, DISA executed the first of three planned reorganizations to better meet its expanded mission. The reorganizations were meant to transition DISA from an entity of several dissimilar, autonomous directorates to one of few components (commonly called directorates by DISA personnel) that operate in a highly integrated and coordinated fashion. DISA is accomplishing that goal, but with some difficultly. The reorganizations have negatively affected the organizational cohesiveness and efficiency of DISA information management. Information management roles, responsibilities, and authorities were not well-defined or understood by most DISA directorates. In our opinion, organizational confusion and uncertainty hindered the effective management and execution of IRM oversight and system security.

# Part II - Findings and Recommendations

# Finding A. Oversight of Information Resources Management

Oversight of DISA IRM programs and functions needed improvement. This condition occurred because oversight roles had not been well defined, oversight mechanisms were incomplete or inaccurate, and the Chief Information Officer's internal controls did not identify effective oversight procedures. Accordingly, the Chief Information Officer could not verify that DISA's information resources were efficiently and effectively used and managed in accordance with DoD policy. Additionally, the Chief Information Officer's decision to delegate procurement authority to the Defense Commercial Communications Office was not supported, and noncompetitive procurements were not adequately justified.

## Background

In 1986, Congress reauthorized the Paperwork Reduction Act of 1980 and amended the Act to require that Federal agencies designate a senior IRM official responsible for IRM programs and functions. DoD Directive 8000.1, "Defense Information Management Program," October 27, 1992, requires DISA to establish an information management program to implement and oversee information management principles, policies, and procedures established by the DoD. IRM, a component of DISA's Information Management Program, includes the management of Federal Information Processing resources. In 1991, the Director, DISA, designated the Chief Information Officer as the Agency's Senior Information Resources Management Representative. "Representative" is the title used by DoD agencies for senior IRM officials.

Oversight is one of the primary management functions of the Chief Information Officer and the IRM Division. The Division, with a staff of eight, is responsible for the development, implementation, management, and oversight of the DISA Information Management Program and related IRM programs and functions. The IRM Division staff also managed operational IRM programs; three staff members managed more than one program.

## Roles and Responsibilities of the Chief Information Officer

As the DISA senior IRM official, the Chief Information Officer was primarily responsible for the development of related policy and for ensuring the implementation of that policy throughout the various DISA directorates. However, the Director, DISA, had not clearly defined the Chief Information Officer's role and responsibilities to other DISA directorates. Consequently,

some DISA managers believed the purview of the Chief Information Officer was limited to information systems and resources that supported internal DISA requirements. The absence of agency-wide oversight reviews by the Chief Information Officer reinforced that perception. Accordingly, the Chief Information Officer could not effectively perform as the senior IRM official and the DISA had inadequate assurance that all of its IRM programs and activities functioned effectively and efficiently.

**Effects of Chief Information Officer's Unclear Role.** DISA Notice 640-45-123, July 15, 1991, established the Office of the Chief Information Officer. The Notice included the mission and function statements, but did not clearly delineate which functions of the Chief Information Officer were agency-wide. Also, due to extensive reorganizations, managers in other DISA directorates did not have a good understanding of the Chief Information Officer's high-level role in DISA's Information Management program.

Because the role of the Chief Information Officer was not clearly defined or fully understood, coordination with other DISA directorates was adversely affected. To effectively respond to DoD or Federal requests and taskings, the Chief Information Officer must rely on information from other DISA directorates that manage information resources. When the needed information could not be obtained, the agency-level response was often inaccurate or incomplete. For example, in response to an OSD request for the DISA IRM Strategic Plan, the Chief Information Officer requested related information from 11 DISA directorates. Only three directorates responded to the request. Lacking the broad base of information necessary to formulate a comprehensive, DISA-wide strategic plan, the Chief Information Officer submitted to OSD the architectural plan for one automated administrative system. Accordingly, the plan submitted was not an agency-wide strategic plan premised on DISA's total information needs, automated information system programs, technology requirements, and associated resources necessary to support DISA missions.

**IRM Oversight Responsibilities Affected by Management Perceptions.** The Chief Information Officer was responsible to implement and oversee the DISA IRM program. Current Federal and DoD definitions of IRM include the management of automated information systems and other information processing resources. Additionally, Federal and DoD definitions of an automated information system have evolved to include not only traditional data processing systems, but also communications networks. Some DISA managers, however, did not consider systems used to support external customers, or used by DISA directorates in providing that support, to be IRM assets or to be subject to Chief Information Officer oversight. Accordingly, the Chief Information Officer's IRM program management responsibilities, including oversight, were in effect limited to internally used automated information systems.

For example, managers at DISA's Defense Network Systems Organization did not consider the networks they managed to be automated information systems because they transported information for external customers and the networks did not process or manipulate that information. Managers at the Defense Information Technology Services Organization believed that the Chief Information Officer had oversight of only internally used systems. Those

managers also believed that systems managed and operated by DISA to support "external" customers were not subject to review by the Chief Information Officer. Those opinions reflect DISA's historical managerial philosophy and approach, but could not be supported by the audit. To the contrary, current Federal and DoD guidance define the automated assets of both directorates as IRM assets. Because the FIRMR and DoD Directive 8000.1 do not segregate the management of IRM, excluding external information resources from consideration as IRM assets was not appropriate. Additionally, the exclusion of "external" IRM assets from oversight by the Chief Information Officer directly contradicted the concept of a single responsible official for IRM.

We could not determine the costs of "external" automated information systems and related resources, but we believe they account for the majority of DISA information resource budgets. For example, an amended FY 1992 and FY 1993 President's Budget Submission reflected estimated costs of about $709 million for DISA information technology systems during FY 1991 and FY 1992. For FY 1991 and FY 1992, we estimated that DISA had contract costs of about $21 million for "internal" information resources, or about 3 percent of its information technology budget for DISA information resources.

## Oversight Methods and Procedures

The Chief Information Officer had not effectively established life-cycle management procedures for automated information systems, an accurate Federal Information Processing inventory, or an effective IRM Review Program to oversee DISA IRM programs and functions.

**Life-Cycle Management of Automated Information Systems.** DoD Directive 7920.1, "Life-Cycle Management of Automated Information Systems," June 20, 1988, and the subsequent DoD Directive 8120.1, "Life-Cycle Management of Automated Information Systems," January 14, 1993, defines life-cycle management as a management process, applied throughout the life of an automated information system, that bases all programmatic decisions on the expected mission and economic benefits derived over the life of the system. DoD Directive 8120.1 also establishes five phases in this management process: concept exploration and definition, validation and demonstration of the selected concept, system development, system production and deployment, and system operations and support.

DoD Instruction 7920.2, "Automated Information System Life-Cycle Management Process, Review, and Milestone Approval Procedures," March 7, 1990, and the subsequent DoD Instruction 8120.2, "Automated Information System Life-Cycle Management Process, Review, and Milestone Approval Procedures," January 14, 1993, establish specific review responsibilities and approval procedures for the five phases and their milestones. Life-cycle management responsibilities extend beyond the deployment of an automated information system. Periodic reviews throughout the operational life of an automated information system are required to determine whether the system

continues to satisfy validated mission needs, requires modernization, or should be terminated. In the event that modernization or system replacement is required, the life-cycle management process is reinitiated at the appropriate phase. The Chief Information Officer is responsible for implementing DoD life-cycle requirements by establishing appropriate management policy and overseeing the execution of that policy. However, the Chief Information Officer neither established adequate policy for life-cycle management nor instituted effective practices.

**DISA's Policy on Life-Cycle Management.** At the time of our audit, the Chief Information Officer developed draft DISA Instruction 630-230-1, "Life-Cycle Management of Automated Information Systems," to implement DoD Directive 8120.1 and DoD Instruction 8120.2 and to consolidate eight related DISA instructions. However, the DISA draft instruction, as well as existent DISA life-cycle management policy, differed significantly from DoD guidance and requirements. Major differences were as follows.

o Both the draft instruction and existing DISA policy established automated information system classifications based on dollar thresholds. However, neither the draft instruction nor existing policy specified management review levels for the various thresholds or specified milestone approval processes and procedures. Lacking senior management visibility at established life-cycle phases, costly information systems may not have received appropriate scrutiny.

o The draft instruction did not implement DoD policy for determining whether a system qualified as a Major Automated Information System, which requires OSD-level life-cycle management milestone review. The draft instruction specified a higher dollar threshold than DoD in determining qualification as a Major Automated Information System. These draft provisions, if implemented, would exclude more costly DISA information systems from required OSD milestone reviews.

o Both the draft instruction and existing DISA policy focused on acquisition processes and procedures instead of on functions associated with specific life-cycle management phases and milestones. For instance, both contained little discussion of the operations and support phase, typically one of the most costly life-cycle phases. This focus masks the total cost of automated information systems and could allow systems to grow virtually unchallenged by DISA or OSD management.

**Life-Cycle Management Practices.** The Chief Information Officer relied on the various DISA directorates to perform life-cycle management reviews and did not monitor or review practices, procedures, or documentation to verify that life-cycle management principles were met. However, DISA directorates had not established management review responsibilities or milestone approval procedures to effectively implement the process. DISA managers generally equated life-cycle management to the acquisition process. Review of available documentation substantiated that view; most documents were related to acquisition requirements rather than to life-cycle management phases or milestone reviews. Additionally, the Chief Information Officer's staff reviewed

purchase request documentation for compliance with laws and regulations governing acquisitions, but did not participate in life-cycle management milestone reviews. Deficiencies in the management of the Worldwide On Line System (WWOLS) and the DISA Network (DISANET) may have been averted through a more effective application of life-cycle management principles and practices.

**WWOLS Hardware Replacement.** In 1990, DISA began to buy mainframe computers to upgrade the WWOLS. WWOLS supports the planning, operations, and management of the worldwide Defense Communications System. DISA bought seven International Business Machines, Inc., computers (four of model 3090 and three of model 4381), for about $4 million. However, of the seven computers, only two were installed at DISA sites as originally planned. As a result of substantial problems in fielding the computers, the warranty of one model 3090 expired before installation because the computer had been stored for the 1-year warranty period. Although bought in December 1990, another model 3090 had not been used for WWOLS purposes. Additionally, management planned to consolidate the work loads of the two remaining model 3090 computers and to excess one after consolidation.

Documentation related to life-cycle management activities for the WWOLS upgrade was not available. DISA officials told us a requirements analysis was developed, validated, and approved. However, DISA officials could not provide documentation that showed an analysis or validation of requirements or documentation that clearly related to a life-cycle management phase or milestone approval. As discussed above, the planning and validation activities for deploying the computers were deficient. Only two of the model 3090 computers were deployed as planned because the overseas sites could not accommodate the computers without significant additional costs and time needed for facility preparation. Instead, two model 4381 computers, which were originally purchased for use at backup sites, were installed because the model 4381 computers required no facility preparation.

**DISANET Development.** Life-cycle management principles were not applied in the development of DISANET; therefore, its cost-effectiveness is unknown. The DISANET is a collection of interconnected local area networks. Each local area network provides access to standard DISA administrative software and to DISA mission data bases and applications. Information critical to life-cycle management processes and decisions, such as anticipated benefits and historical costs, could not be identified. Official files and documentation were not centrally maintained or readily available, primarily because DISA did not assign responsibility for DISANET development to a project manager. The roles and responsibilities for DISANET functions were being defined during our audit. The application of life-cycle management principles and practices would have provided enhanced focus and direction to DISANET development and implementation.

**Information Processing Equipment Inventory.** The information processing equipment inventory used by the Chief Information Officer was not an effective, agency-level oversight and planning tool, because the inventory contained unreliable data. DoD Directive 7950.1, "Automated Data Processing Resources

Management," September 29, 1980, designated the DoD Automation Resources Management System (ARMS) as the principal, official source of management information on Federal Information Processing resources within the Department of Defense. The Directive tasked DoD Components to verify that information in the ARMS data base was accurate and timely. Although the Chief Information Officer had established an ARMS Program, the Chief Information Officer relied on other DISA directorates to establish and maintain accurate ARMS data. However, most DISA directorates viewed the ARMS data base as a low-priority responsibility and expended little effort in verifying its accuracy. Consequently, ARMS inventory data on DISA's information processing resources were highly inaccurate.

**Actions to Improve DISA ARMS Program.** Although ARMS was the only centralized source of management information on information processing resources available to the Chief Information Officer and other DISA managers, there was little agency-wide emphasis on establishing and maintaining the integrity of that information. Recognizing in March 1992 that ARMS information was not reliable, the Chief Information Officer planned to establish ARMS focal points in other DISA directorates to be primarily responsible for verifying that data discrepancies were identified, that corrections were made, and that the reliability of ARMS data would be maintained. Those actions were planned to be completed by October 1992. By March 1993, the focal points had been designated and were being trained, but no substantial progress had been made in validating the accuracy of ARMS data.

**ARMS Data Accuracy.** The DISA-related data in ARMS were inaccurate and outdated and did not provide DISA officials with an effective tool for managing information resources or for planning for future requirements. We obtained DISA inventory records from the ARMS data base and physically verified a statistical random sample of those records to determine whether the selected assets were at the indicated DISA location, had been excessed or transferred to another DISA site, or could not be located or accounted for. Our sampling methodology and approach is described in Appendix A. We verified the ARMS inventories for assets located at the Defense Commercial Communications Office (DECCO) and the Telecommunications Management and Services Office (TMSO), both located at Scott Air Force Base, Illinois, and at several DISA offices in the National Capital Region. We considered DISA assets located at Fort Ritchie, Maryland, within the National Capital Region. The sample universe consisted of 1,118 items of information processing equipment valued at about $42 million. Our actual sample was 222 items, valued at about $6.3 million. Sampling results for each site are provided in Table 1. Based on sampling results, we concluded that the DISA ARMS inventory records were, on average, only 27 percent correct, and that 53 percent of the ARMS inventory items had been excessed or transferred. We could not locate or account for 20 percent of the sample items, which were valued at about $778,000.

**Table 1. Results of DISA ARMS Inventory Verification**

| | Number of Assets Sampled | | | |
|---|---|---|---|---|
| | DECCO | TMSO | NCR* | Total |
| Correct | 25 | 10 | 24 | 59 |
| Excessed or Transferred | 42 | 32 | 45 | 119 |
| Not Located | 15 | 16 | 13 | 44 |
| Total Sampled | 82 | 58 | 82 | 222 |

*NCR National Capital Region

DISA acquired substantial information resources that had not been entered into the ARMS data base. For example, the seven previously discussed computers bought for WWOLS were not reflected in the ARMS data base. Additionally, officials in one DISA directorate estimated that $7 million had been spent on information processing equipment during FY 1993, but none of the equipment had been entered into the ARMS data base. Further, DISA Directorates had not updated ARMS inventory records since 1991.

Failure to maintain accurate inventories of information processing equipment affected the ability of DISA managers to effectively plan for meeting information technology needs or information resource requirements. For instance, the lack of an accurate agency-wide inventory contributed to the Chief Information Officer's previously-discussed problems in formulating a DISA IRM Strategic Plan.

Inaccurate DISA-related data in ARMS also negatively affected other DoD Components. In November 1992, the OSD queried the ARMS data base for a DoD inventory of computers, each of which cost at least $100,000. OSD needed that information to analyze potential consolidations of data processing activities. The query showed that 25 DISA computers were in that inventory. Our verification of those results showed that OSD relied on DISA-related data that were only 36 percent accurate. Of the 25 DISA computers, we determined that 9 were operational, 14 were excessed or otherwise disposed of, and 2 could not be accounted for.

**IRM Review Program Results.** The Chief Information Officer had an ongoing IRM Review Program, but the reviews performed were not thorough or focused on areas involving substantial resources or having significant effect on mission accomplishment. FIRMR part 201-22, "Review and Evaluation," January 1990, and DoD Directive 7740.3, "Information Resources Management Review Program," February 7, 1989, require that DoD agencies perform periodic reviews of IRM programs to ensure they are being accomplished in an

efficient, effective, and economical manner and that IRM policies, procedures, standards, and guidelines are being followed. Although the scope of possible review areas is broad, DoD requires IRM areas to be selected for review based on mission impact, resources involved, and potential vulnerabilities.

The same employee who managed the DISA IRM Review Program also managed another IRM-related program. About 15 to 20 percent of that employee's time was spent managing the IRM Review Program. Due to limited resources, contractors were tasked to perform most reviews.

For FY 1991, OSD required the Chief Information Officer, as the DISA Senior IRM Representative, to review a minimum of five IRM areas: compliance with the Paperwork Reduction Act of 1980, management of major information systems, implementation of DoD life-cycle management requirements, software modernization, and the accuracy of ARMS data. Each area was reviewed, but the reviews were not performed in a thorough and comprehensive manner. A contractor employee took about 6 weeks to review four of the IRM areas and to issue associated reports. We evaluated those reports and concluded that they were lacking in substance and did not provide meaningful results. For instance, the report on DISA's implementation of DoD life-cycle management requirements was based on discussions held with two staff members, representing the Chief Information Officer's organization, and four personnel from two other DISA directorates. Although the report concluded that DISA had implemented DoD life-cycle management requirements, the report did not describe how that conclusion was reached or the factors considered. Also, the report provided no indication that verification procedures were performed. The IRM Review Program manager examined the other required IRM area, but retained only summary documentation that was forwarded to OSD.

OSD did not require that a particular IRM area be reviewed during FY 1992, but the Chief Information Officer reviewed three areas: the management of reports, mail, and technical data. A contractor, other than the one used in FY 1991, performed the reviews. For two reviewed areas, mail and reports management, the contractor used published GSA guidelines, checklists, and bulletins as evaluation guidance. Because GSA had not published evaluation guidance for technical data, the contractor developed its own methodology and related checklists and questions based on DoD technical data directives, instructions, and manuals. We concluded that the FY 1992 reviews were performed in a more structured and thorough manner.

As previously discussed, we evaluated life-cycle management and information processing equipment inventory, two areas also reviewed in FY 1991 by the Chief Information Officer. We determined that, because the Chief Information Officer did not fully implement recommendations resulting from the FY 1991 reviews, inaccurate inventories and inadequate life-cycle management documentation still existed. In accordance with DoD requirements, the Chief Information Officer should select IRM areas for future review that involve significant resources or have a high potential to significantly affect mission accomplishment.

## Acquisition Oversight

The Chief Information Officer did not exercise adequate oversight of the acquisition of information resources. As a result, DISA procurement policy for information processing resources was not uniformly applied, adherence to acquisition limitations granted by the GSA could not be assured, acquisition documentation did not comply with the FIRMR, and justifications for noncompetitive procurements were inadequate.

**DISA Compliance with FIRMR.** DISA acquired information processing resources through the Acquisition Management Organization's two contracting offices: the Contracts Management Division, at DISA Headquarters, Arlington, Virginia, and the DECCO at Scott Air Force Base, Illinois. FIRMR part 201-20, "Acquisition," and part 201-39, "Acquisition of Federal Information Processing Resources by Contracting," and Defense Federal Acquisition Regulation Supplement part 239, "Acquisition of Information Resources," govern DoD's acquisition of information resources. Defense Communications Agency Letter 88-004, "Acquisition How To Guide" (the Guide) implements Federal and DoD regulations at DISA and requires that a series of documents, collectively referred to as an acquisition package, be prepared for review and approval by the Chief Information Officer.

**Acquisition Packages.** We reviewed acquisition packages in 14 contract files at the Contracts Management Division. The acquisition packages were usually prepared by DISA directorates requesting the information resources and were submitted to the Chief Information Officer for evaluation of FIRMR compliance. According to the Guide, acquisition packages should consist of purchase requests and other necessary documentation to support the need for the procurement. At the Contracts Management Division, acquisition packages were submitted to its contracting officers after review and certification by the Chief Information Officer for compliance with the FIRMR and the Guide. We reviewed acquisition documentation in 15 DECCO contract files. DECCO policy did not require the development of formal acquisition packages. At DECCO, we reviewed comparable documentation, titled "Interoffice Memorandum(s)," which was retained in contract files. We reviewed the acquisition packages related to the contracts shown in Appendix B.

To evaluate compliance with the FIRMR, we compared acquisition packages to requirements defined in FIRMR part 201-20 and in chapter 3 of the Guide. We focused on requirements analyses, alternatives analyses, and, if applicable, justifications for "other than full and open competition." Since DECCO used acquisition guidance that differed from that used by the Contracts Management Division, we added an additional step to review DECCO documentation. We compared the content of interoffice memorandums prepared for DECCO contracting officers with the content of acquisition packages prepared for Contracts Management Division contracting officers. For discussion purposes, this report also refers to DECCO's documentation as acquisition packages.

**Contracts Management Division.** At the Contracts Management Division, 12 of 14 sampled acquisition packages complied with

FIRMR requirements. The acquisition packages described the requirements, referenced the purchase request, detailed a justification for the need, and provided reference to other completed analyses and information resource considerations. Although the documents were not presented as formal analyses, they were sufficient for evaluation. Overall, the acquisition packages reviewed at the Contracts Management Division contained information required by the Guide and met the intent of the FIRMR.

**DECCO.** At DECCO, 13 of the 15 acquisition packages partially complied with the FIRMR, 1 acquisition package complied, and 1 did not comply. DECCO acquisition packages provided only brief statements on the requirements, alternatives, and justifications. For example, in the acquisition package for contract DCA200-92-F-5409, DECCO inappropriately identified a specific make or model rather than a functional requirement; incorrectly justified that specific requirement based on vendor reputation and use by nearby organizations; and inadequately evaluated alternatives to select the specific requirement, even though the acquisition package stated that DECCO had "no one capable of making a qualitative judgment" on the system. Therefore, by not preparing compliant acquisition packages, DECCO contracting officers were procuring information processing resources with no assurance that valid needs were identified, valid certifications were made, or less costly alternatives were available.

**Delegation from Chief Information Officer.** In July 1991, the Chief Information Officer delegated procurement authority to the DECCO. The delegation allowed DECCO to review and approve acquisitions of information processing resources that cost less than $250,000 for internal use. The Guide provides the Chief Information Officer authority to delegate that responsibility. Chapter 3 of the Guide requires that delegations by the Chief Information Officer to other DISA directorates be based on prior performance, knowledge of the FIRMR, and completion of specified training. However, the Chief Information Officer's staff had not requested nor was it provided evidence that DECCO met those requirements.

The delegation required DECCO to certify that each acquisition was compliant with FIRMR and Federal Acquisition Regulation (FAR) requirements. Because DECCO had not designated a certifying official, none of its 15 acquisition packages were certified. The delegation also required that the Chief Information Officer review and approve acquisition packages for Federal Information Processing resources that exceeded $250,000. Seven such acquisition packages, valued at a total of $6,730,644, were identified, but none had been forwarded to or approved by the Chief Information Officer. Consequently, DECCO did not comply with the delegation terms in obtaining information resources valued at $7,424,532.

**FIRMR Implementation.** Although the Guide was developed by DISA, it was not used by both of its procurement offices. DECCO used DCA-DECCO Instruction 260-70-1, "Procurement Policies and Procedures," commonly referred to as the "Red Book," and the Contracts Management Division used the Guide. Portions of the Guide relating to acquisition of information resources were written by the Chief Information Officer for agency-wide application and

pertained directly to DISA's acquisition of information resources. The Chief Information Officer was unaware that DECCO did not use the Guide until we presented our interim audit results.

DECCO's Red Book did not adequately implement FIRMR part 201-20, and it did not apply acquisition guidance similar to that in chapter 3 of the Guide. For instance, the Red Book did not contain policy on the acquisition of internal information resources or clearly define the controls over the requirements process as did the Guide. Also, the DISA policy and procedures for purchase requests and agency procurement requests had not been prescribed. As a result, the DECCO staff did not implement appropriate procedures for reviewing and approving requirements. Inadequate review and approval procedures can lead to situations such as discussed in Procurements for ITABBS (page 20).

The Red Book was tailored to DECCO's predominant business interest of procuring long-haul telecommunications for other DoD Components and did not provide guidance on the acquisition of information processing resources for DECCO's internal use. Although DECCO's business operations were mostly for other DoD Components, the value of information processing resources it procured was comparable to that procured by the Contracts Management Division from FY 1990 through FY 1992. Additionally, DECCO's business interests may expand under the Defense Management Report Decision 918, "Defense Information Infrastructure." Accordingly, we believe DECCO should follow the strong procedural controls in the Guide, which are consistent with the FIRMR.

**Oversight of Delegations of Procurement Authority.** For fully competitive acquisitions of information processing resources valued in excess of $2.5 million (or in lesser amounts, depending on the restrictions that limit competition), DISA is required to obtain a Delegation of Procurement Authority (Delegation) from GSA. Delegations normally specify a maximum dollar limit and may impose other specific contracting limitations. As the DISA's senior IRM representative, the Chief Information Officer is responsible for ensuring compliance with Delegation limitations. However, the Chief Information Officer had not established effective procedures to monitor related contracts to verify that specific Delegation terms and conditions were met.

GSA granted eight Delegations to DISA from FY 1990 through FY 1992. We reviewed contracts related to the Delegations and found that one exceeded the dollar limitations of the Delegation. Additionally, the scope of that contract was amended without the Chief Information Officer's knowledge or approval. Although we found only one instance of noncompliance with a Delegation, the potential exists for other contracts to exceed limitations. Further, that noncompliance demonstrates that the Chief Information Officer needs to develop and document effective contract tracking procedures in order to monitor compliance with Delegations. To meet the responsibilities given by Defense Management Report Decision 918, we believe that DISA will need to obtain even more Delegations in the future. Accordingly, DISA can ill afford for GSA to conclude that DISA does not exercise adequate oversight and control of

Delegation-related acquisitions. In past instances, GSA has lowered an agency's monetary threshold requiring a Delegation when GSA believed the agency did not exercise appropriate oversight and control of acquisition for Federal Information Processing resources.

**Contract Review.** The FAR subpart 6 requires the use of competitive procedures to obtain full and open competition, and the FIRMR part 201-39 specifies the need for supporting documentation when information resources are not procured in a competitive manner. Competitive procedures include synopsizing requirements in the *Commerce Business Daily*, soliciting "invitation for bids" from prospective contractors, and conducting market research to identify the best means to satisfy requirements. Noncompetitive procedures include identification of a sole source of the supply or service needed and identification of requirements that are so specific that use of any other brand or model of resource would not satisfy the need.

The use of noncompetitive procedures must be clearly stated in a justification for other than full and open competition and the justification must be approved by the appropriate contracting official level. If contracting officers determine that noncompetitive procedures would result in the best contracting approach, the officers must certify to that effect in accordance with FAR subpart 6.3. When contract actions are noncompetitive, FIRMR part 201-39.6 and FAR subpart 6.3 require certification by the contracting officer for proposed actions not exceeding $100,000 and by the competition advocate for proposed actions not exceeding $1 million. For actions valued from $1 million to $10 million, the head of the contracting activity approves justifications, and the Director of DISA approves justifications involving at least $10 million.

Since the Chief Information Officer's IRM Division is responsible for reviewing all DISA purchase requests for information resources, we conducted a review of the procurements resulting from those requests. We used random statistical sampling techniques to select contracts for review. We selected 14 Contracts Management Division contracts valued at $2,291,683 and 15 DECCO contracts valued at $7,424,532. We used statistical sampling at the Contracts Management Division to project a contract population since the Contracts Management Division did not have a means to readily track procurements for internally used DISA information resources.

We estimated that from October 1990 to August 1992, 91 contracts valued at about $10 million were for internally used information resources procured by the Contracts Management Division. During the same period, we determined that 58 contracts, valued at about $11 million were procured by DECCO for internally used information resources. We concluded that the Contracts Management Division provided adequate assurance for reviewing and approving justifications for information resource procurements that used noncompetitive procedures. However, as discussed below, DECCO needed to improve its review and approval procedures for noncompetitive procurements. The sampling methodology is discussed in Appendix A, and the contracts reviewed are listed in Appendix B.

**Justifications for Other Than Full and Open Competition.** Six DECCO orders (see Table 2.) placed against GSA nonmandatory award schedule contracts[1] for specific make and model requirements lacked adequate justifications for other than full and open competition. Additionally, none of the six justifications was certified by a DECCO contracting official in accordance with FAR subpart 6.3 or chapter 3 of the Guide. Those regulations require contracting officers to certify justifications for other than full and open competition, and the Guide requires the contracting officer certification when the procurement action will be greater than $2,500. DECCO's Red Book does not provide similar procedures.

**Table 2. GSA Nonmandatory Award Schedule Contracts Not Competed**

| Contract Number | Award Amount | Justification Adequate | Reason for OTFOC* |
|---|---|---|---|
| DCA200-92-F-5120 | $114,399 | No | Specific Make/Model |
| DCA200-92-F-5409 | 49,407 | No | Specific Make/Model |
| DCA200-92-F-5438 | 25,536 | No | Specific Make/Model |
| DCA200-92-F-5442 | 30,364 | No | Specific Make/Model |
| DCA200-92-F-5480 | 47,280 | No | Specific Make/Model |
| DCA200-92-F-5636 | 82,204 | No | Specific Make/Model |
| Total | $349,190 | | |

*OTFOC - Other Than Full and Open Competition

Because DECCO did not develop adequate justification for limiting competition and DECCO contracting officers did not certify that limited competition was appropriate, we concluded that three procurements for the Information Technology Acquisition Bulletin Board System (ITABBS) were questionable.

**Procurements for ITABBS.** DECCO did not provide for full and open competition in its procurement of computer hardware and software for ITABBS. Estimated to cost $650,000, ITABBS is a state-of-the-art bulletin board acquisition system that allows prospective contractors to place offers, via remote access, in response to DECCO's information resource requirements. Although

[1]A GSA nonmandatory award schedule contract allows Federal agencies to procure resources directly from a prenegotiated contract. The use of this type of contracting method permits certain deviations from competitive procedures defined in FAR part 6. Specific procedures for using GSA nonmandatory contracts are defined in FIRMR part 201-39.

access, in response to DECCO's information resource requirements. Although we did not audit the acquisition of ITABBS, we determined that three delivery orders for the system's hardware and software did not comply with FIRMR requirements.

DECCO personnel did not submit the hardware and software requirements to contracting officers as a single system, but presented the requirements through separate purchase requests, resulting in multiple procurement actions. The FIRMR states that to promote competition, requirements must be synopsized in the *Commerce Business Daily* when the contract is valued at greater than $50,000. In addition, FIRMR part 201-20 states that procurements of specific make and model resources are considered noncompetitive and must be justified in accordance with the FAR subpart 6.3.

The three specific make and model justifications for the ITABBS hardware and software should have been questioned by a contracting official because written justifications did not support a specific make and model and because an evaluation of alternatives was not completed. At least three contracting actions, totaling $127,051, were initiated within a 6-week period. All three were presented to the DECCO contracting officers as sole source, specific make and model procurements.

None of the three contracting actions were publicized or certified by a contracting official in accordance with FAR subpart 6.3. FAR procedures were not followed because requirements were presented in a fragmented manner. We concluded that, based on the appearance of the ITABBS procurements, the three specific make and model justifications for the ITABBS hardware and software should have been questioned by a contracting official.

If the Chief Information Officer's IRM Division had reviewed the ITABBS' requirements for FIRMR compliance, the requirements may not have resulted in separate contract actions. The ITABBS' requirements should have been consolidated and procured through a single contract action. Also, that consolidated procurement should have been reviewed by DISA's competition advocate, and any restrictions to full and open competition should have been questioned. If the procurements had been consolidated, we believe the DISA competition advocate would have questioned the procurement's restrictiveness because supporting documentation did not justify a specific make and model and the requirements may have been satisfied by available information resources on the open market.

## Internal Management Controls

The Chief Information Officer's system of internal management controls needed improvement. Effective Federal management requires that a system of internal accounting and administrative controls be established to provide reasonable assurance that: obligations and costs comply with law, assets are safeguarded, and revenues and expenditures are accounted for and properly recorded. The

Office of Management and Budget Circular A-123 (Revised), "Internal Controls Systems," August 1986, prescribes policies and procedures for agencies to follow in establishing and maintaining their internal controls program. DoD Directive 5010.38, "Internal Management Control Program," April 1987, establishes the DoD program for internal management control. DCA Instruction 630-125-6, "DCA Internal Management Control Program," July 1987, prescribes policy, procedures, and responsibility for the internal management control program within DISA.

The objective of an internal management control program is to ensure sufficient management controls are in place to prevent fraud, waste, and mismanagement of an organization's assets. The Office of Management and Budget recommends the following approach in evaluating and reporting on internal control: organize the process; segment the agency; conduct vulnerability assessments; develop plans for subsequent actions; conduct internal control reviews; take necessary corrective actions; and prepare a report on internal controls. Historically, DISA has segmented the agency along organizational lines, with each major organization responsible for evaluating and reporting on its system of internal management controls. Accordingly, the Chief Information Officer annually certifies that an appropriate system of internal management controls has been established.

In August 1992, the Comptroller, as DISA's senior internal management control official, issued guidance for developing management control plans for FY 1993 through FY 1997. Believing that past risk assessments were unrealistically low, the Comptroller required that each major DISA program and functional area perform at least 10 control tests within the 5-year period. To help meet that requirement, the Chief Information Officer requested that we test selected internal management controls. However, upon examining the Chief Information Officer's internal management controls, we determined that the Chief Information Officer complied with related DISA guidance in form but failed to meet its full intent when performing risk analyses, defining control techniques, and documenting the system of internal management controls.

**Risk Assessment.** The risk assessments for the Chief Information Officer's four divisions were not supported by a documented, quantitative methodology. A risk assessment examines the susceptibility of a program or function to waste, loss, unauthorized use, or misappropriation due to its nature or environment. Office of Management and Budget "Internal Control Guidelines," December 1982, describes a risk assessment as a three-step process used to determine the relative potential for loss: an analysis of the general control environment in which a program functions, an analysis of a program's inherent risks, and a preliminary evaluation of safeguards within a program.

The Chief Information Officer's Year-End Certification Letter and Internal Management Control Plan for FY 1992 reported moderate risk in three divisions and low risk in the other division. Because those risk assessments were purely judgmental, we performed an independent risk assessment of each division. In applying Office of Management and Budget guidelines, we

administered a questionnaire for each of the four divisions designed to measure the general control environment, the inherent risk, the safeguards, and the overall vulnerability to risk. Questionnaires were completed by 83 percent (20 of 24) of the Chief Information Officer's staff.

The results of our analysis, which are shown in Appendix C, reflect that three divisions had a high vulnerability to risk and that one division was moderately vulnerable. Our analysis also showed that the Chief Information Officer's inherent risks and safeguards posed high vulnerabilities to risk, while its general control environment was moderately risky. Overall, our analysis indicated that the Chief Information Officer's organization had a high vulnerability to risk. Although our analysis is not fully conclusive, it provides a quantitative indication that the risk ratings developed by the Chief Information Officer were significantly understated.

**Control Techniques Needed to Meet Control Objectives.** The Chief Information Officer had not developed sufficient control techniques needed to meet corresponding control objectives for the four divisions. Control techniques, such as specific policies, procedures, plans of organization, physical arrangements, processes, and documentation, are the mechanisms by which control objectives are achieved. The Chief Information Officer adopted control techniques from DCA Instruction 630-230-6, Supplement 1, without tailoring them to effectively meet the objectives of each Division.

We evaluated the control techniques and concluded that 81 percent did not have a clear relationship to its associated objective. For instance, one division had the following control objective.

> Review the DISA Information Processing Systems and Services Purchase Requests for compliance with technical, administrative, physical and personnel security requirements.

The division used the following control technique to meet the above objective.

> Access to and Accountability for Resources. Passwords are assigned to the Division personnel required to access restrictive data bases and bulletin boards. Personnel sign for accountable items in their custody.

The above technique fails to satisfy the control objective of assuring that DISA's systems and purchase requests complied with technical, administrative, physical and personnel security requirements. This example was not an isolated case, but rather illustrates the techniques used by the four divisions. Additionally, control technique documentation was not available.

**Internal Management Control Documentation.** The four divisions did not maintain adequate documentation to support their internal management controls. DoD requirements and DCA Instruction 630-125-6 require internal management control systems to be clearly documented and readily available for examination. Systems documentation is made up of policies and procedures, manuals, flowcharts, organizational charts, and written and graphic materials. This type of documentation describes organizational structure, administrative practices,

operating procedures, and assigns program responsibility. The Chief Information Officer did not document risk assessments or control technique processes. Additionally, internal management control documentation did not include organizational structure, operating procedures, and administrative practices.

## Summary

The Chief Information Officer was not fully successful in centrally overseeing the management of DISA information resources. The Chief Information Officer's IRM role and responsibilities were not well-defined and understood by all DISA directorates and were not uniformly recognized throughout DISA. Additionally, the Chief Information Officer had neither instituted the systems and procedures necessary for agency-level oversight nor developed or documented effective controls. Defense Management Report Decision 918 tasked DISA with greatly expanded information management responsibilities. Implementation of the following recommendations will help DISA achieve more effective and efficient management of its information resources and will illustrate that DISA fully intends to meet the challenge of its expanded role.

## Recommendations for Corrective Actions

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

a. Clarify the role of the Chief Information Officer as the Defense Information Systems Agency's senior information resources management official and specify the Chief Information Officer's oversight responsibilities as they pertain to all information resources managed by the Defense Information Systems Agency.

b. Direct that all Defense Information Systems Agency contracting offices use consistent acquisition policy and procedures to acquire internally used Federal Information Processing resources. Additionally, the acquisition policy and procedures used should fully comply with requirements in the Federal Information Resources Management Regulation parts 201-20 and 201-39.

2. We recommend that the Chief Information Officer, Defense Information Systems Agency:

a. Revise the Defense Information Systems Agency's life-cycle management policy for automated information systems to comply with DoD life-cycle management requirements, to include milestone review and approval procedures.

b. Conduct periodic reviews to verify that Defense Information Systems Agency life-cycle management practices and procedures for automated information systems comply with DoD life-cycle management requirements.

c. Require that Defense Information Systems Agency directorates update and maintain the Federal Information Processing inventory in the Automation Resources Management System data base.

d. Conduct periodic Automation Resources Management System inventory reconciliations.

e. Direct the Manager of the Information Resources Management Review Program to review information resource programs and activities that have substantial mission impact, resources, or potential vulnerabilities.

f. Conduct an "Information Resources/Procurement Management Review" at the Defense Commercial Communications Office to determine compliance with Federal and DoD information resource development, acquisition, and reporting requirements.

g. Reevaluate the vulnerability of each Chief Information Officer division, develop specific control techniques that achieve related control objectives, and develop and maintain internal management control documentation.

3. We recommend that the Chief Information Officer, with the assistance of the Director, Acquisition Management Organization, establish a process to monitor and track contract actions relative to Delegations of Procurement Authority.

## Management Comments and Audit Response

The Defense Information Systems Agency generally agreed with the finding and concurred with each recommendation. The reply described the completed and planned actions relative to each recommendation. Those actions will improve the oversight of DISA IRM programs and functions. DISA comments are fully responsive except those on Recommendation A.2.b., which concerns oversight reviews of AIS life-cycle management practices and procedures.

In response to Recommendation A.2.b., the reply stated that the DISA "Acquisition How To Guide" was updated in August 1993 to detail procedures for delegating authority to procure IRM assets. Further, two staff positions were added to the Office of the Chief Information Officer to better determine whether the terms and conditions of the Delegations have been met. Once the positions have been filled and appropriate training has been provided, the Chief Information Officer will initiate on-site inspections of DISA contracting offices and other offices that have been delegated procurement authority.

We fully endorse enhanced acquisition oversight by the Chief Information Officer, but that was not the intent of Recommendation A.2.b. Rather, our intent was that DISA manage its automated information systems from a life-cycle perspective and in accordance with the DoD guidelines and requirements discussed in the section entitled "Life-Cycle Management." We found scant evidence that DISA managers had instituted an AIS life-cycle milestone review and approval process. Accordingly, we believe the Chief Information Officer should perform oversight reviews to encourage the establishment of AIS life-cycle management responsibilities, procedures, and practices. We ask that DISA clarify its position on Recommendation A.2.b. in additional comments on this final report.

# Finding B. Automated Information Systems Security

DISA had not endorsed 25 of 45 automated information systems as being adequately secure, did not have an effective security review program for its systems, and did not adequately staff security positions or provide security training. These conditions occurred because the DISA did not adequately implement its security program for automated information systems. As a result, systems did not comply with Federal and DoD security directives and guidance, and DISA had no assurance that its systems were reasonably protected.

## Background

Office of Management and Budget Circular A-130, "Management of Federal Information Resources," December 1985, requires Federal agencies to prepare policies, standards, and procedures and implement and maintain an Automated Information System (AIS) security program. DoD Directive 5200.28 "Security Requirements for Automated Information Systems," March 1988, establishes DoD's policy for safeguarding classified, unclassified-sensitive, and unclassified information processed in systems. DISA Instruction 630-230-19, "Security Requirements for Automated Information Systems," August 1991, details the responsibilities of all AIS security personnel, prescribes the security accreditation process, provides guidelines for developing and maintaining security documentation, recommends minimum qualifications for security officers, and describes related training for all DISA employees. The Instruction also designated the Chief Information Officer as primarily responsible for all matters relating to systems security and compliance and for managing the DISA AIS Security Program.

The Chief Information Officer established the Information Systems Security Division to implement and manage the DISA AIS Security Program. The Division, with a staff of three, had established security points of contact within the DISA directorates, provided assistance to DISA directorates for evaluating AIS security, and revised DISA Instruction 630-230-19. During the audit, the Division also coordinated the development of an AIS security training program with DISA's Center for Agency Services and established a working group to develop procedures to guard against and report computer viruses. However, the AIS Security Program could be more effective if senior management placed more emphasis on security compliance, the Chief Information Officer conducted security reviews, and DISA enhanced security staffing and training.

## Compliance With Federal and DoD Security Regulations

DISA managers did not place enough emphasis on compliance with Federal and DoD AIS security requirements. Although Federal, DoD, and DISA security objectives and specific requirements for automated information systems have existed for years, DISA officials have routinely postponed meeting those requirements, even when systems were clearly deficient in meeting security requirements. The Chief Information Officer, as the AIS Security Program manager, had not been successful in implementing timely system accreditations; developing system security plans; or ensuring that the DISANET, the automated information system most commonly used by DISA employees, met security requirements.

**AIS Accreditation.** As of March 1, 1993, 25 of 45 DISA internal automated information systems were not accredited. DoD Directive 5200.28 requires DoD agencies to assign an official as the Designated Approving Authority responsible for accrediting each automated information system under the official's jurisdiction and for ensuring compliance with security requirements. Accreditation is a formal declaration by the Designated Approving Authority that the automated information system is approved to operate in a particular security mode, using a prescribed set of safeguards. The accreditation shall be supported by a certification plan, a risk analysis of the system in its operational environment, an evaluation of the security safeguards, and a certification report. Automated information systems containing classified or sensitive data are required to be reviewed and reaccredited once every 3 years or upon a significant change in design or facilities.

We identified 45 DISA automated information systems, excluding office automation systems, that contained classified or unclassified-sensitive information. Nine classified systems and fifteen unclassified-sensitive systems were not accredited. Another system was granted an interim authority to operate. Although 11 systems had been accredited since July 1, 1992, 25 were unaccredited as of March 1993. Appendix D identifies the accredited and unaccredited systems.

At the time of the audit, only three DISA directorates were in the process of accrediting office automation systems. We considered clusters of personal computers, whether or not connected to DISANET, as office automation systems. One directorate accredited the office automation systems in four of its five divisions. The second directorate was correcting deficiencies identified in its risk analysis. The third began the risk analysis process in March 1993.

**Security Plans for Information Systems.** DISA had not fully complied with the Computer Security Act of 1987, which requires Federal agencies to identify each computer system that contains sensitive information and to prepare and implement a plan for the security and privacy of those systems. A security plan had not been developed or provided to the Chief Information Officer for each of DISA's unclassified-sensitive systems. In August 1990, the Chief Information Officer asked DISA directorates to forward a security plan for each unclassified-sensitive system. The Chief Information Officer received 22 security plans,

16 of which were for office automation systems or unique local area networks. In January 1993, the Chief Information Officer asked DISA directorates to submit security plans for FY 1993. The Chief Information Officer received 32 plans, 11 of which were for office automation. Only half of the directorates submitted security plans to the Chief Information Officer for FY 1993.

DISA Instruction 630-230-19 references the security plan as one of the documents to be reviewed during the accreditation process and provides a guideline for development. However, that Instruction did not explicitly state how often security plans are to be revised or require the directorates to submit a copy to the Chief Information Officer. During our audit, we identified one directorate that had completed four security plans, but forwarded none to the Chief Information Officer.

**Status of DISANET in Meeting Security Requirements.** Although DISANET was DISA's most widely used automated information system, it was not accredited or in compliance with several security requirements. A risk analysis was completed in March 1991 and an interim authority to operate was granted at that time. However, that authority expired on March 31, 1992. In April 1991, DISANET operational responsibilities, which include AIS security, were assumed by DISA's Defense Systems Support Organization. DISANET had expanded to all DISA offices located in the National Capital Region. No security plan or comprehensive contingency plan for the DISANET existed at the time of the audit. According to officials in the Defense Systems Support Organization, the development of a security plan was deferred until approval of the final network architecture and the contingency plan was under development.

As of March 1, 1993, the configuration of DISANET did not meet the minimum security requirements prescribed by DoD. DoD Directive 5200.28 requires that systems containing sensitive data meet specific security requirements by 1992. The minimum classification for unclassified-sensitive systems is a C2[2] security rating. To address security deficiencies identified in the March 1991 DISANET risk analysis, the Defense Systems Support Organization contracted for a security evaluation of DISANET in order to effectively meet DoD security requirements. The evaluation was completed October 1, 1992.

The contractor reported that the network operating system used by DISANET did not meet the required DoD security capabilities. An alternative network operating system was recommended to meet applicable security requirements. At the end of our audit, the Defense Systems Support Organization estimated that the new software would be operational throughout DISA by February 1994. As of March 1993, DISA had not decided whether the Defense Systems Support Organization or the Chief Information Officer would be the overall Designated Approving Authority for DISANET. Neither directorate could provide an estimate of when DISANET would be accredited.

[2]A C2 rating requires controlled access on a need-to-know basis, accountability, and audit capabilities.

Accreditation affixes security responsibility with the Designated Approving Authority and shows that due care has been taken for security. Without the risk analysis, certification, and accreditation, DISA would not necessarily know the potential for threats, vulnerabilities, and loss. With the heavy reliance on computers for the day-to-day activities of an organization, a loss or partial loss of the system could be detrimental to the organization.

## AIS Security Reviews

Although the Chief Information Officer was responsible for conducting AIS security compliance reviews, none had been performed as of the time of our audit. The Chief Information Officer did not maintain information on DISA's automated information systems for oversight and review planning purposes. For example, the Information Systems Security Division could not provide a complete list of systems or related information, such as dates of accreditations, major safeguards employed, or relationships to other automated information systems. DISA Instruction 630-230-19 does not require DISA directorates to submit security data to the Chief Information Officer.

Because the Chief Information Officer could not provide security oversight information, we contacted the directorate AIS security officer at nine DISA directorates, DECCO, and TMSO. The directorate security officers are responsible, on a day-to-day basis, for ensuring that adequate security is provided for and implemented throughout the life cycle of directorate automated information systems. However, 8 of 11 directorate security officers either could not readily identify systems they were responsible for or could not provide other relevant security information, such as the accreditation status or the latest risk analysis date of applicable systems. For example, one security officer could not provide a complete list of systems by the end of the audit. Another security officer began compiling a centralized list of systems before the start of the audit, but related accreditation data were not readily available. A third directorate security officer provided security-related information pertaining to the office automation system, but did not provide information about the other automated information systems.

## Security Staffing and Training

Only two directorates had full-time AIS security personnel. Most DISA AIS security personnel (directorate security officers, system security officers, terminal area security officers, and network security officers) had other primary duties. We asked eight directorate security officers and five system security officers, who are responsible for the security of specified AISs, how much of their time was spent on security. Two security officers stated it was a full-time duty, four spent about 50 percent of their time on security, six spent from 10 to 20 percent, and one reported no time spent on security matters.

We also asked the same 13 security officers about their prior experience and related training. Only 4 of the 13 had prior AIS security experience, and 5 had received training before acquiring security responsibilities.

No comprehensive training program for security officers, functional managers, executives, operators, or users of automated information systems had been implemented. The Security Act of 1987 requires mandatory periodic training for all personnel involved in management, use, or operation of Federal computer systems containing sensitive information. All DISA automated information systems identified during the audit contained sensitive information. Although security training responsibilities were assigned by DISA Instruction 630-230-19 to the Center for Agency Services in August 1991, no security training was provided until September 1992. By March 31, 1993, the Center for Agency Services had provided security training for about 80 DISA staff members. Two classes for directorate security officers, two security awareness classes for operators, users, and functional managers; and a class for executives had been conducted. Neither the Center for Agency Services nor the Chief Information Officer could provide an estimate on how many people still needed security training.

## Recommendations for Corrective Actions

We recommend that the Chief Information Officer, Defense Information Systems Agency:

1. Develop a plan, in conjunction with appropriate Defense Information Systems Agency officials, to bring the Defense Information Systems Agency into compliance with the Computer Security Act of 1987, DoD Directive 5200.28, "Security Requirements for Automated Information Systems," and DISA Instruction 630-230-19, "Security Requirements for Automated Information Systems."

a. Implement and monitor the plan.

b. Report periodically to the Director, Defense Information Systems Agency, on the plan's implementation and any unresolved automated information system security issues.

2. Conduct periodic automated information system security reviews in compliance with DoD Directive 5200.28, "Security Requirements for Automated Information Systems," and Defense Information Systems Agency Instruction 630-230-19, "Security Requirements for Automated Information Systems," August 1991.

3. Identify security data required for effective oversight of the Defense Information Systems Agency's Automated Information System Security Program and revise Defense Information Systems Agency

Instruction 630-230-19, "Security Requirements for Automated Information Systems," August 1991, to require submission of that data to the Chief Information Officer.

4. Establish minimum experience and training qualifications for Automated Information System security personnel at the Defense Information Systems Agency and revise Instruction 630-230-19, "Security Requirements for Automated Information Systems," August 1991, to require that minimum qualifications are met.

## Management Comments

The Director, Defense Information Systems Agency, concurred with the finding and all recommendations. Planned corrective actions were also provided, and all actions were expected to be completed by October 1, 1994. The complete text of management's comments is in Part IV.

# Part III - Additional Information

# Appendix A. Statistical Sampling Methodology

## Inventory of Federal Information Processing Equipment

We performed three reviews to determine the accuracy of DISA's Federal Information Processing resources inventory in the Automated Resources Management System (ARMS). Reviews were performed within the National Capital Region and two field offices, DECCO and TMSO. The White House Communications Agency was excluded from the inventory review.

The Defense Automation Resources Information Center is the DoD principal source for equipment redistribution, sharing, and inventory management. To determine the sample universes for the three reviews, we extracted inventory data from the ARMS data base for items of Federal Information Processing equipment. For the National Captial Region, we limited our universe to equipment items that cost at least $25,000 each. For DECCO and TMSO, the universes represented all items in the ARMS data base, regardless of cost.

We developed an attribute sample for each universe using a 90-percent confidence level, 10-percent expected error rate, and a 5-percent precision rate. Items in each universe were numbered sequentially, and random numbers were selected to determine the specific items of equipment to be physically verified. Table A.1. shows the dates, universes, and sample sizes for the reviews.

**Table A.1. Sample of Inventory within DISA**

| | As of Date | Universe | Sample Size |
|---|---|---|---|
| DECCO | Nov. 10, 1992 | 497 | 82 |
| TMSO | Nov. 12, 1992 | 138 | 58 |
| NCR* | Dec. 10, 1992 | 483 | 82 |
| Total | | 1,118 | 222 |

*NCR National Capital Region

# Determination of Contract Population

**DD350 Query.** The Federal Information Processing resources population was derived from the DD350 data base, "Individual Contracting Action Reports," monitored by the Washington Headquarters Service. Contracts were selected based on the assigned Standard Industry Classification codes and their Federal Supply Classification codes. The codes helped identify information resource (nontelecommunications) contracts that satisfied internal DISA requirements.

In order to determine which contracts were internal to DISA needs, we presented the universe of contracts to DECCO and the Contracts Management Division for assistance. We easily determined the population at DECCO since it operated on a cost reimbursable basis and segregated contracts based on requirements. The Contracts Management Division did not operate on a cost reimbursable basis and was unable to break out those contracts applicable to internal DISA needs. As a result, we estimated the population for information resources that were procured for internal use by the Contracts Management Division.

**Population Determination at the Contracts Management Division.** We projected the internal resource population at the Contracts Management Division to 91 contracts valued at about $10 million. Precision limits for the projection are plus or minus 32 contracts and plus or minus $5.8 million. The projection was based on a weighted sample of the total information resources universe (internal and external) at the Contracts Management Division. The weights were applied to 14 randomly selected contracts among 3 strata, identified as internal resources contracts. The three strata were developed in relationship to the dollar thresholds for delegations of procurement authority. The attribute sample was developed using a 90-percent confidence level, 5-percent error rate, and 10-percent occurrence rate. Replacement sampling was done for files not present due to warehousing or classification. Contracts that fell below the $25,000 threshold were dropped from the sample.

The dollar values assigned to each stratum are shown in Table A.2.

**Table A.2. Breakout of Dollar Value**

| | |
|---|---|
| Stratum I | $25,000 through $249,999 |
| Stratum II | $250,000 through $2,499,999 |
| Stratum III | $2,500,000 and greater |

No internal resource contracts were selected that fell within the third stratum. Calculations for the projection were based on data shown in Table A.3. and Table A.4.

**Table A.3. Sampling Results at the Contracts Management Division**

| | Universe | | Sample | | Results | |
|---|---|---|---|---|---|---|
| Stratum | No. of Contracts | Values | No. of Contracts | Values | No. of Contracts | Values |
| I | 347 | $ 29,482,133 | 52 | $ 6,355,714 | 13 | $1,801,868 |
| II | 118 | 86,289,047 | 28 | 26,609,862 | 1 | 489,816 |
| III | 19 | 135,619,365 | 8 | 67,776,415 | -- | -- |
| | 484 | $251,390,545 | 88 | $100,741,991 | 14 | $2,291,684 |

**Table A.4. Projection of Contract Universe at the Contracts Management Division**

| | Projection | |
|---|---|---|
| Stratum | No. of Contracts | Values |
| I | 87 | $8,358,292 |
| II | 4 | 1,588,349 |
| III | -- | -- |
| | 91 | $9,946,641 |

# Appendix B. Contracts Reviewed for FIRMR Compliance

| Contract Number | Amount | FIRMR Documents | GSA Schedule Contract | Extent Competed |
|---|---|---|---|---|
| **Contracts Management Division** | | | | |
| DCA100-90C-0038 | $159,214 | Complete | No | FOC[1] |
| DCA100-90C-0140 | 28,430 | Complete | No | FOC |
| DCA100-90C-0141 | 75,524 | Complete | No | FOC |
| DCA100-90C-0191 | 172,046 | Complete | No | FOC |
| DCA100-91C-0154 | 84,530 | Complete | No | OTFOC[2] |
| DCA100-91C-0182 | 74,532 | Complete | No | FOC |
| DCA100-91F-0045 | 246,468 | Complete | Yes | OTFOC |
| DCA100-91F-0270 | 122,457 | N[3] | Yes | OTFOC |
| DCA100-91F-0464 | 119,926 | Complete | Yes | OTFOC |
| DCA100-91F-0586 | 489,816 | N | Yes | FOC |
| DCA100-92C-0045 | 76,851 | Complete | No | OTFOC |
| DCA100-92C-0060 | 199,108 | Complete | No | OTFOC |
| DCA100-92F-0133 | 222,500 | Complete | Yes | OTFOC |
| DCA100-91F-0105 | 220,282 | Complete | No | FOC |
| **DECCO** | | | | |
| DCA200-90C-0028 | $358,792 | Incomplete | No | FOC |
| DCA200-90D-0059 | 1,398,000 | Incomplete | No | FOC |
| DCA200-91D-0023 | 1,970,511 | Incomplete | No | OTFOC |
| DCA200-91D-0034 | 1,136,801 | Incomplete | No | OTFOC |
| DCA200-91F-5636 | 48,742 | Incomplete | Yes | OTFOC |
| DCA200-92D-0026 | 255,344 | Incomplete | No | FOC |
| DCA200-92D-0053 | 1,339,619 | N | No | FOC |
| DCA200-92F-5084 | 153,144 | Incomplete | Yes | OTFOC |
| DCA200-92F-5120 | 114,399 | Incomplete | Yes | OTFOC |
| DCA200-92F-5147 | 113,555 | Incomplete | Yes | FOC |
| DCA200-92F-5175 | 271,577 | N | Yes | FOC |
| DCA200-92F-5222 | 31,775 | Incomplete | Yes | OTFOC |
| DCA200-92F-5409 | 49,407 | Incomplete | Yes | FOC |
| DCA200-92F-5480 | 47,280 | Incomplete | Yes | FOC |
| DCA200-92F-5438 | 25,536 | Incomplete | Yes | FOC |

[1]FOC - Full and Open Competition
[2]OTFOC - Other Than Full and Open Competition
[3]N - Not in the Contract File

# Appendix C. IG, DoD, Risk Assessment of the Office of the Chief Information Officer

**Risk Assessment by CIO Division**

| Vulnerability Assessment Factors | Data Administration | Information Resources | Plans and Architecture | Security Program |
|---|---|---|---|---|
| Control Environment[1] | High | Moderate | High | Low |
| Analysis of Inherent Risk[2] | High | High | High | High |
| Analysis of Safeguards[3] | High | Moderate | High | Low |
| Totals | High | High | High | Moderate |

[1]The environment in which activities are conducted has a major effect on the effectiveness of internal control within an agency. Several factors determine the general control environment, including the following: management attitude, organizational structure, personnel, delegation and communication of authority and responsibility, policies and procedures, budgeting and reporting, organizational checks and balances, and considerations for automatic data processing equipment.

[2]Requires an analysis for each identified program and administrative function of the inherent potential for waste, loss, unauthorized use, or misappropriation due to the nature of the activity itself. Matters to be considered in the analysis should include: mission purpose and characteristics, budget level, effect outside the agency, age and life expectancy, degree of centralization, special concerns, prior reviews, and management responsiveness.

[3]The key consideration is whether appropriate controls are in place to prevent or at least minimize waste, loss, unauthorized use, or misappropriation.

# Appendix D. AISs Reviewed and Related Security Data

## 20 Accredited Systems

| DAA [1] | AIS Name or Application | Classification [2] | Risk Analysis [3] | Accreditation [4] | Security Plan [5] |
|---|---|---|---|---|---|
| JIEO/JITC | Automated Procedure Software (APS) System | S | 04/22/1991 | 07/03/1991 | N/A |
| | Corporate Data Base | U-S | 11/02/1992 | 12/11/1992 | 02/22/1993 |
| | Government Open Systems Interconnection Profile Test Laboratory | U-S | 08/06/1992 | 08/20/1992 | None |
| | High Frequency Computer Operating System (HFCOS) | U-S | 11/02/1992 | 11/24/1992 | 02/22/1993 |
| | Joint Interface Test System (JITS) | S | 07/10/1992 | 08/04/1992 | 02/22/1993 |
| | Joint Portable Tactical Digital Information Link Tester (JPTT) | S | 05/10/1991 | 07/10/1991 | 02/20/1993 |
| | Message Loading Device (MLD-I) | U-S | 05/20/1991 | 07/03/1991 | None |
| | Microcomputer Message Analysis System (MicroMAS) | S | 04/29/1991 | 07/03/1991 | 02/22/1993 |
| | Multi-Processing System (MPS) | U-S | 11/19/1990 | 11/26/1990 | None |
| | National Imagery Transmission Format Test Facility (NITF) | U-S | 06/15/1992 | 07/13/1992 | None |
| | Packet Switching Network/Defense Data Network System Test Facility | S | 04/23/1991 | 07/03/1991 | 02/22/1993 |
| | Traffic Loading Device (TLD) | U-S | 01/07/1991 | 01/22/1991 | None |
| | Worldwide Military Command and Control System Testbed | TS | 09/01/1992 | 11/03/1992 | 02/22/1993 |
| DSSO | All-in-One (Mail 1) | U-S | None | 08/11/1992 | 07/31/1992 |
| | All-in-One (Mail 2) | U-S | None | 08/11/1992 | 07/31/1992 |
| | Defense Data Network Link 1 | U-S | None | 04/12/1992 | None |
| | Drafting and Building (diagrams) | U-S | None | 08/11/1992 | 07/31/1992 |
| | Integrated Data Service and Card Catalog | U-S | None | 08/11/1992 | 07/31/1992 |
| | Oracle Data Base Application | U-S | None | 08/11/1992 | 07/31/1992 |
| DECCO | Personnel Concept III Terminal | U-S | Unknown | 06/27/1991 | None |

See footnotes at end of table.

# 25 Unaccredited Systems

| DAA [1] | AIS Name or Application | Classification [2] | Risk Analysis [3] | Accreditation [4] | Security Plan [5] |
|---|---|---|---|---|---|
| JIEO/JITC | Joint Interoperability Evaluation System (JIES) | S | In Process[6] | 01/05/1993[7] | 02/20/1993 |
| | Reserve Component Automated System (RCAS) Testbed | S | In Process | None | 02/22/1993 |
| | Message Loading Device (MLD-II) | S | 11/05/1992 | I-Submit[8] | 02/22/1993 |
| | Test Procedures Generator (TPG) | S | In Process | I-Submit[8] | 02/20/1993 |
| DSSO | ADA Programming - Rational | U-S | None | None | None |
| | AT&T 3 B2 (Network test bed) | U-S | None | None | None |
| | Hyperchannel link | U-S | In Process | None | None |
| | Hyperchannel (testing) | U-S | None | None | None |
| | Joint Operations Planning and Execution Systems Data Configuration Management | U-S | None | None | None |
| | Softswitch (Defense Data Network, DISANET and WANG) | U-S | None | None | None |
| | Switching Terminal | U-S | None | None | None |
| | Defense Satellite Communications System Operational Support System Network | S | In Process | 11/19/1987[9] | N/A |
| | WWOLS - Site R | S | 06/19/1992 | 03/04/1988[9] | N/A |
| | WWOLS - National Capital Region | S | 06/19/1992 | 03/04/1988[9] | N/A |
| AMO | Archive Laser Disk System | U-S | None | None | None |
| | Automated Contract Preparation System (ACPS) | U-S | None | None | None |
| | Automated Planning and Tracking System (APTS) | U-S | None | None | None |
| | WWOLS - TMSO | S | None | 03/04/1988[9] | N/A |
| DECCO | DECCO On-Line | U-S | Unknown | 11/1990[10] | 10/15/1992 |
| | Defense Acquisition Bulletin Board System (DABBS) | U-S | None | None | None |
| | Information Technology Acquisition Bulletin Board System (ITABBS) | U-S | In Process | None | None |
| NCS | Telecommunications Emergency Decision Support System (TEDSS) | S | In Process | None | 06/19/1991 |
| | Telecommunications Service Priority (TSP)[11] | U-S | None | None | 02/13/1993 |
| CIO | Joint Actions Control Section (JACS) | S | In Process | In Process | N/A |
| COMP | Automated Accounting Invoice System | U-S | None | None | 02/22/1993 |

See footnotes on next page.

[1] DAA - Designated Approving Authority.
AMO - Acquisition Management Organization.
CIO - Chief Information Officer
COMP - Comptroller.
DSSO - Defense Systems Support Organization.
JIEO - Joint Interoperability and Engineering Organization.
JITC - Joint Interoperability Test Center.
NCS - National Communications System.

[2] Classification Levels.
S - Secret.
TS - Top Secret.
U-S - Unclassified-Sensitive.

[3] Date of Last Risk Analysis.

[4] Date of Last Accreditation.

[5] Date of Last Security Plan as prescribed by the Federal Security Act of 1987.
None - The Security Plan was not completed or could not be found.
N/A - The Security Act of 1987 refers to sensitive AISs, and OMB Bulletin 90-08, "Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information," July 9, 1990, excludes classified systems from security plans. However, in the FY 1993 CIO data request, the CIO also requested security plans for classified systems.

[6] Original risk analysis was completed in January 1991 and is undergoing revision.

[7] Interim Authority to Operate was granted.

[8] Interim Authority to Operate was requested.

[9] DoD Directive 5200.28 requires all systems to be reaccredited every 3 years. Because that requirement was not met, we considered this system to be unaccredited.

[10] System was accredited in November 1990; however, since that time, an installation change has occurred. Therefore, this system was unaccredited.

[11] System was terminated in March 1993.

# Appendix E. Summary of Other DISA IRM Programs

We reviewed the following IRM programs: Forms Management, Reports Management, Records Management, Mail Management, Trail Boss, Computer Accommodation Program, and DISA's implementation of the DoD Corporate Information Management initiative. Although the Chief Information Officer was responsible for the management of the Forms and Reports Programs, the Records and Mail Management Programs were under the control of the Center for Agency Services. As the senior IRM representative, the Chief Information Officer is responsible for all IRM programs; however, the Chief Information Officer did not coordinate with the Records and Mail Managers. The Computer Accommodation Program was placed under the direction of the Equal Employment Opportunity office of DISA. Since the Trail Boss (explained below) program was not mandatory for Federal agencies, neither DISA nor the Chief Information Officer appointed a program manager. Overall the Forms, Trail Boss, and Computer Accommodation programs were functioning adequately throughout DISA. At the time of our audit, it was too early to determine whether the Corporate Information Management initiative was progressing satisfactorily throughout DISA. We identified weaknesses in Reports, Records, and Mail Management, but they were relatively minor and, therefore, did not require formal recommendations.

**Forms Management.** Overall, the Forms Management Program functioned adequately throughout DISA. Forms management focuses on creating, reproducing, stocking, and distributing forms. FIRMR Bulletin B-3, "Standard and Optional Forms Management Program," January 30, 1991, provides procedures for obtaining approval for new, revised, or canceled Government-wide standard or optional forms, including electronically generated forms. DoD Directive 7750.7, "DoD Forms Management Program," May 31, 1990, requires that forms management satisfies valid needs, is cost-effective, promotes standardization, and complies with applicable laws and regulations. DCA Instruction 630-15-1, "DCA Forms Management Program," August 8, 1984, implemented that guidance within DISA.

DISA's Forms Management Program is managed by the Forms Official, a Chief Information Officer staff member. The Forms Official had no support staff, but DISA appointed forms coordinators in each directorate to help validate the need for forms, to prevent duplicate and "bootleg" forms, and to design or change forms as needed. The Forms Official maintains historical and current information on 237 internal DISA and 373 other Federal forms. In 1989, DISA began to develop and use electronically-generated forms. "Electronic" forms offer substantial advantages over paper forms in almost every aspect. By September 1992, DISA had developed 25 forms in an electronic format and planned to make another 38 available.

**Reports Management.** The Reports Management Program was considered a low priority and was given minimal attention. Reports management consists of managerial activities involved in the creation, processing, and use of reports. A

report is defined as data or information that is transmitted for use in determining policy; planning, controlling, and evaluating operations and performance; making decisions, or preparing other reports. FIRMR Bulletin B-2, "Interagency Reports Management Program," January 30, 1991, states that the purpose of the program is to ensure that interagency reports are based on need, are cost-effective, and comply with applicable laws and regulations. FIRMR section 201-9.202-2, "Creation, Maintenance, and Use of Records," October 1990, requires each agency to obtain GSA approval for each new, revised, or extended interagency report before implementation and to designate an agency-level, interagency reports liaison representative and alternate. As stated in DoD Directive 7750.5, "Management and Control of Information Requirements," August 7, 1986, the user is responsible and accountable for verifying that information requirements are valid, accurate, and essential to the mission of the user's directorate. DISA implemented that guidance in DCA Instruction 630-225-2, "Management and Control of Information Requirements," June 30, 1987.

**DISA Reports Management Program.** DISA's Reports Management Program lacked visibility and attention. Although DCA Instruction 630-225-2 does not require the appointment of coordinators, it does state it is the user's responsibility to validate that information requirements are valid, accurate, and essential to the mission of the user's directorate. All new or revised requirements for the generation of a report are forwarded by the user to the Reports Program Manager for the assignment of a control symbol for tracking purposes.

In June 1992, the Chief Information Officer asked the individual directorates to review a total of 108 registered internal reports to determine whether they were still current and had a valid requirement. The directorates reported that 76 reports were still valid, but the directorates canceled 21 other reports. As of July 1992, the Chief Information Officer was still awaiting responses on the remaining 11 reports. As a result of the revalidation, all history files were brought up to date. The revalidation process also provided indications that many reports were not sent to the Reports Manager for the assignment of a control symbol. Even though interagency and intra-DoD reports are revalidated by the Washington Headquarters Service, DISA's historical files on those reports were not current. DISA last published an index of all internal reports, intra-DoD reports, interagency reports, and canceled reports in 1987.

**Contractor Review of Reports Management Program.** During our audit, a contractor reviewed the Reports Management Program (the Program) and found that it was functioning adequately. However, the contractor discovered that the Program was not used by all DISA directorates and that many directorates were unaware of its existence. In addition, the contractor believed that due to minimum staffing, some Program functions were not fully effective.

**Records Management.** Electronic records within DISA headquarters and field offices were not included in the Records Management Program reviews. However, FIRMR Bulletin B-1, "Electronic Records Management," January 30, 1991, provides guidance related to the creation, maintenance, use, and

disposition of electronic records. FIRMR section 201-9.102, "Creation, Maintenance, and Use of Records," October 1990, requires each Federal agency to establish and maintain an active, continuing program for managing agency records, commensurate with agency size, organization, mission, and record-keeping activity. DoD Directive 5015.2, "Records Management Program," March 22, 1991, requires that adequate controls over the creation of Component records be established, Component functions be adequately and properly documented, operational recordings be kept to a minimum, and the accumulation of unnecessary records be prevented. DISA implemented that guidance in DCA Instruction 210-15-6, "Records Management," June 1985.

**DISA Records Management Program.** DISA's Records Management Program is managed by a Center for Agency Services' Records Manager (the manager). The manager did not review records outside the National Capital Region and minimally reviewed records within the National Capital Region. The appointed manager was responsible for 418 publications, but was not responsible for the oversight of electronic records. In addition, the manager was not aware of anyone assigned to provide oversight for electronic records. Furthermore, Chief Information Officer staff and the manager did not coordinate on records management issues.

**DISA Records Management Practices.** We reviewed four offices' records management practices for compliance with DoD and DISA guidance. No official records coordinators had been assigned, files were not labeled, the standard files locator (Form 166) was not utilized, and file cabinets were not labeled on the outside. During our audit, DISA personnel in two of the four offices told us that the Records Management Program Manager had also conducted compliance reviews during FY 1992.

**Mail Management.** DISA's Mail Management Program operated with occasional delays and minimal oversight. Its objective was to control official mail costs through proper and cost-effective use of the United States Postal Service as stated in DoD Manual 4525.8, "DoD Official Mail Manual," July 1987. DISA established policy and procedures for Mail Management in DCA Instruction 210-15-4, "Correspondence and Mail Management," January 27, 1987.

**DISA Mail Management Program.** The Mail Manager managed the travel and records management divisions and operated the mailrooms for DISA. Although DISA established standard operating procedures at its Headquarters mailroom, it established no standard operating procedures for mailrooms elsewhere. The DISA inspected its mailrooms once a year within the National Capital Region; however, DISA performed no inspections at its other locations. DISA decentralized the mailroom budget, implemented use of the nine-digit zip code, and installed a computer lock mail system. Since the decentralization of the postal budget, all sites were required to pay up front for meter use and report their quarterly volume of mail and dollars spent.

**Contractor Review of the Mail Management Program.** During the survey phase of our audit, a contractor reviewed the mail program and found that the mail operations at the individual facilities ran smoothly in terms of

receipt and delivery of mail. However, delays were routinely experienced in the distribution of internal and external mail for DISA and from the rerouting of mail incorrectly addressed to individuals who had relocated within DISA Headquarters. In addition, the contractor believed the Mail Management Program was weakened due to the official Mail Manager having only partial responsibility and no authority to enforce mail policies throughout the agency.

**Trail Boss.** DISA is implementing the Trail Boss Program. FIRMR Bulletin C-7, "Trail Boss Program," January 30, 1991, defines the Trail Boss Program, outlines GSA actions to implement it, and provides guidelines for agency participation. The objective of the Trail Boss Program is to help the Government modernize its major information systems through sound and timely acquisitions. Trail Boss is an alternative approach for effectively managing the acquisition and implementation of major information processing resources. Under the program, a single acquisition manager, the "Trail Boss," has authority and responsibility to build and manage an effective acquisition support team by integrating programmatic, technical, and contracting functions. The program emphasizes the importance of individuals, cooperation, and accomplishment rather than process and procedure. The Trail Boss Program is comprised of three sections:

o Trail Boss I, which highlights moving from acquisition to implementation;

o Trail Boss II, which provides guidance on the implementation of major information systems; and

o Trail Boss III, which provides in-depth training in the acquisition process of major information systems.

DISA sent two employees to training in Trail Boss I and planned to send two more to training in Trail Boss III during FY 1993. Since no one had completed all three courses, DISA had not been able to fully incorporate the Trail Boss concepts. However, because the Trail Boss Program is not a mandatory requirement for Federal agencies and since DISA had made efforts to incorporate Trail Boss in its program, we determined no further audit work was needed.

**Computer Accommodation Program.** DISA established an effective program for providing handicapped personnel with computers and appointed a program manager. The Computer Accommodation Program was originally created by DoD to assist offices in procuring adaptive equipment for handicapped employees.

**Regulatory Guidance.** The Americans with Disabilities Act of 1991 requires employers to make reasonable accommodations so that people with disabilities can perform the essential functions of their jobs. FIRMR Bulletin C-8, "Information Accessibility for Employees with Disabilities," January 30, 1991, states that agencies shall provide information resource accessibility to individuals with disabilities and that agencies shall be aware that an accommodation program is essential to enable handicapped employees to

perform as productive employees. FIRMR Bulletin C-10, "Telecommunications Accessibility for Hearing and Speech Impaired Individuals," January 30, 1991, provides guidelines for acquiring products and services that provide telecommunications accessibility for hearing and speech impaired individuals for communication with and within Federal agencies. The bulletin also provides general information regarding responsibilities for accommodating the needs of those with hearing and speech impairments. Accommodations are also provided for individuals with visual, mobility, or dexterity impairments. DoD Directive 1440.1, "The DoD Civilian Equal Employment Opportunity Program," May 21, 1987, requires DoD Components to develop procedures and implement a program for handicapped employees in computer support, staffing initiatives, training and development programs, and upward mobility programs designed to increase the representation of handicapped individuals. DISA recognizes handicapped needs in chapter 3 of the DISA "Acquisition How To Guide," October 1, 1990.

**DISA's Computer Accommodation Program.** DoD Computer Accommodation Program personnel assisted DISA in procuring information resources adapted for use by disabled employees. Since FY 1990, DISA utilized the DoD Computer Accommodation Program 13 times to acquire adaptive equipment for 85 DISA employees. Disabled employees within the DISA have been allowed to function productively due to the procurement of equipment, such as large print keyboard labels, a screen reader, and a hand scanner for personal computers that can scan and speak virtually any typeset material.

**Corporate Information Management Initiative.** The thrust of the DoD Corporate Information Management Initiative (the Initiative) is on using modern information technology to improve efficiency and reduce the costs of business processes. The OSD established the Center for Information Management (the Center) within DISA to provide guidance and assistance to DoD Components in areas such as information analysis, business process improvement, software reuse, data engineering, and open standards. Primarily because so few elements of the Initiative were completed or well-defined, we were unable to reach a firm conclusion on DISA's progress in implementation.

The Chief Information Officer was responsible for encouraging and guiding other DISA directorates in implementing the various aspects of the Initiative. In that regard, we examined Chief Information Officer efforts in: complying with the Technical Reference Model (technical specifications established by the Center), acquiring and using Computer-Aided Software Engineering tools, developing and using standardized data (DoD Data Dictionary), and reusing previously developed software. The Chief Information Officer's technical reports and draft policies incorporated or referenced components of the Technical Reference Model. A copy of the Data Dictionary Repository system had been installed, though it was not fully operational. Computer Aided Software Engineering tools were being used to perform process modeling within the Chief Information Officer divisions. We could not identify specific Chief Information Officer efforts to advance the reuse of software by other DISA directorates.

# Appendix F. Summary of Potential Benefits Resulting From Audit

| Recommendation Reference | Description of Benefit | Type of Benefit |
|---|---|---|
| A.1.a. | Internal Control. Improves understanding of the Chief Information Officer's role. | Nonmonetary. |
| A.1.b. | Internal Control. Requires use of consistent and appropriate procedures for acquisition of Federal Information Processing resources. | Nonmonetary. |
| A.2.a. | Internal Control and Compliance with Regulations. Brings DISA's life-cycle management guidance in conformance with DoD requirements and establishes DISA procedures for life-cycle management review and approval. | Nonmonetary. |
| A.2.b. | Internal Control and Compliance with Regulations. Establishes and requires appropriate life-cycle management practices by DISA components. | Nonmonetary. |
| A.2.c. | Program Results. Provides DISA's managers with an accurate information resource inventory. | Nonmonetary. |
| A.2.d. | Internal Control and Program Results. Establishes a process to verify the continued accuracy of DISA's information resource inventory data. | Nonmonetary. |
| A.2.e. | Program Results. Directs effective use of limited IRM reviews. | Nonmonetary. |
| A.2.f. | Internal Control. Provides the Chief Information Officer a basis for delegating procurement authority to DECCO. | Nonmonetary. |

## Appendix F. Summary of Potential Benefits Resulting From Audit

| Recommendation Reference | Description of Benefit | Type of Benefit |
|---|---|---|
| A.2.g. | Internal Control. Improves Chief Information Officer's system of internal management controls. | Nonmonetary. |
| A.3. | Internal Control. Provides Chief Information Officer with ability to monitor compliance with delegations from the GSA. | Nonmonetary. |
| B.1. | Compliance with Regulations. Verifies DISA's directorates are in compliance with DISA policy. | Nonmonetary. |
| B.2. | Internal Control and Compliance with Regulations. Establishes a mechanism to verify that DISA's AISs are in compliance with Federal, DoD, and DISA security requirements and procedures. | Nonmonetary. |
| B.3. | Program Results. Provides data to effectively manage AIS Security Program. | Nonmonetary. |
| B.4. | Program Results. Establishes and requires minimum training and experience for AIS security officers. | Nonmonetary. |

# Appendix G. Organizations Visited or Contacted

## Office of the Secretary of Defense

Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), Arlington, VA
Assistant Secretary of Defense (Health Affairs)
  Defense Medical Systems Support Center, Falls Church, VA

## Defense Agency

Defense Information Systems Agency, Arlington, VA
  Defense Commercial Communications Office, Scott Air Force Base, IL
  Defense Information Technology Services Organization, Denver, CO
  Defense Systems Support Organization, Arlington, VA
    Site R, Fort Ritchie, MD
  Joint Interoperability and Engineering Organization, Arlington, VA
    Joint Interoperability Test Center, Fort Huachuca, AZ
  Telecommunications Management Service Organization, Scott Air Force Base, IL

## Non-Defense Federal Agencies

Information Management Technology Division, General Accounting Office, Washington, DC
Information Resources Management Service, General Services Administration, Washington, DC

## Contractor

Advanced Technology Corporation, Arlington, VA

# Appendix H. Report Distribution

## Office of the Secretary of Defense

Comptroller of the Department of Defense
Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
Assistant to the Secretary of Defense for Public Affairs

## Department of the Army

Auditor General, Army Audit Agency

## Department of the Navy

Auditor General, Naval Audit Service

## Department of the Air Force

Auditor General, Air Force Audit Agency

## Defense Agencies

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

## Non-Defense Federal Organizations

General Services Administration
Office of Management and Budget
U.S. General Accounting Office, National Security and International Affairs Division, Technical Information Center

## Non-Defense Federal Organizations (cont'd)

Chairman and Ranking Minority Member of Each of the Following Congressional Committees and Subcommittees:

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Governmental Affairs
Senate Subcommittee on Oversight of Governmental Management, Committee on Governmental Affairs
Senate Subcommittee on Regulation and Governmental Information, Committee on Governmental Affairs
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Subcommittee on Oversight and Investigations, Committee on Armed Services
House Subcommittee on Readiness, Committee on Armed Services
House Committee on Government Operations
House Subcommittee on Information, Justice, Transportation and Agriculture, Committee on Government Operations
House Subcommittee on Legislation and National Security, Committee on Government Operations

# Part IV - Management Comments

# Defense Information Systems Agency Comments

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

IN REPLY REFER TO: AGA

FEB 2

MEMORANDUM FOR INSPECTOR GENERAL, DEPARTMENT OF DEFENSE
ATTN: Director, Readiness and Operational Support Directorate

SUBJECT: Draft Audit Report on Information Resources Management at the Defense Information Systems Agency (Project No. 2RE-0049)

Reference: DoDIG Memo, subject as above, 30 Nov 93

1. As requested by the referenced memorandum, the Defense Information Systems Agency (DISA) has reviewed the subject report, and our comments on Findings A and B are provided at Enclosure 1.

2. If you have questions on our response, the point of contact for this action is Ms. Sandra Leicht, Audit Liaison, DSN 222-5326 or commercial (703) 692-5326.

FOR THE DIRECTOR:

1 Enclosure a/s

RICHARD T. RACE
Inspector General

*Quality Information for a Strong Defense*

INTEROFFICE MEMORANDUM

TO: Inspector General (AG)

THRU: Deputy Director, Operations, Customer Relations and Services (FA) for 1/28/94

FROM: Chief Information Officer (IA)

DATE: 28 January 1994

SUBJECT: Draft Audit Report on Information Resources Management at the Defense Information Systems Agency (Project No. 2RE-0049)

Reference: IOM, AG, subject as above, 3 Dec 93

Preparer: MM Walther/IR/696-1915

1. In response to the reference, my office has reviewed the subject draft audit report. We generally agree with the findings and the intent of the recommendations. The recommendations should prove to be helpful as we continually strive to improve the effectiveness and efficiency with which we manage our information resources in accordance with Federal and DoD requirements and guidelines.

2. Enclosed are comments that address each finding and recommendation. Our comments describe corrective actions and milestone dates for each recommendation.

3. My action officer for this review is Margaret Walther. She may be reached at (703) 696-1915.

1 Enclosure a/s

for SARAH JANE LEAGUE
Chief Information Officer

WHEN SEPARATED FROM ENCLOSURE,
THIS MEMORANDUM REQUIRES NO PROTECTION

Comments on the DODIG's Draft Audit Report on
Information Resources Management at the
Defense Information Systems Agency
Project No. 2RE-0049, 30 November 1993

1. Finding: A, Oversight of Information Resources Management. "Oversight of DISA IRM programs and functions needed improvement. This condition occurred because oversight roles had not been well defined, oversight mechanisms were incomplete or inaccurate, and the Chief Information Officer's internal controls did not identify effective oversight procedures. Accordingly, the Chief Information Officer could not insure that DISA's information resources were efficiently and effectively used and managed in accordance with DoD policy. Additionally, the Chief Information Officer's decision to delegate procurement authority to the Defense Commercial Communications Office was not supported, and noncompetitive procurements were not adequately justified."

Comments: We generally agree with the finding and the intent of the recommendations. Our comments on the recommendations follow.

a. Recommendation 1a: That the Director, Defense Information Systems Agency, "clarify the role of the Chief Information Officer as the Defense Information Systems Agency's senior information resources management official and specify the Chief Information Officer's oversight responsibilities as they pertain to all information resources managed by the Defense Information Systems Agency."

Comments: Concur. The Director's Policy Letter 93-3, "DISA and OMNCS Information Management Policy," was issued on 30 March 1993. This policy letter establishes the Defense Information Systems Agency (DISA) and Office of the Manager, National Communications System (OMNCS) framework for defining and managing DISA and OMNCS information resources and systems. The policy letter defines and clarifies the role of DISA's Chief Information Officer, as well as the responsibilities of other DISA organizational elements. Additionally, the Director has initiated an effort to develop an Agency-wide Concept of Operations (CONOPS), which will clearly define the responsibilities and relationships of all DISA organizations, including that of the Deputy Director, Operations, Customer Relations and Services (DDOCRS), to which the DISA Office of the Chief Information Officer (OCIO) is now subordinate. The DDOCRS CONOPS is also undergoing revision, and will specifically address the roles, responsibilities, and relationships of the OCIO. Estimated completion date is 31 March 1994.

b. Recommendation 1b: That the Director, Defense Information Systems Agency, "direct that all Defense Information Systems Agency contracting offices use consistent acquisition policy and

1

procedures to acquire internally used Federal Information Processing resources. Additionally, the acquisition policy and procedures used should fully comply with requirements in the Federal Information Resources Management Regulation parts 201-20 and 201-39."

Comments: Concur. The Principal Deputy Director, Defense Commercial Communications Office, issued Policy Letter (PL) No. 94-01, Authority to Acquire Federal Information Processing (FIP) Resources, on 23 November 1993. This policy letter sets forth the authority and responsibilities associated with FIP acquisitions and follows the general guidelines contained in Defense Communications Agency (DCA) Letter 88-001, thereby providing consistency between communications and FIP resource acquisitions. Additionally, PL 94-01 and DCAL 88-001 will be consolidated into a single DISA Information Technology Procurement Organization (DITPRO) document, directive upon all DISA contracting offices. Estimated completion date is 1 August 1994.

c. Recommendation 2a: That the Chief Information Officer, Defense Information Systems Agency, "revise the Defense Information Systems Agency's life-cycle management policy for automated information systems to comply with DoD life-cycle management requirements, to include milestone review and approval procedures."

Comments: Concur. The DISA Information Systems Programs Organization (DISPO) is a new DISA line function and is now assigned Agency responsibility for implementation of DoD Life Cycle Management (LCM) regulations for internal and external customer-related support, including automated information systems. Final implementing documents were prepared and forwarded to the Office of the Deputy Assistant Secretary of Defense (DASD) for C3I Acquisition on 14 December 1993. DISPO has also prepared a draft handbook which more specifically addresses DISA life cycle management requirements and responsibilities, including milestone review and approval procedures. Estimated completion date for the handbook is 30 April 1994.

d. Recommendation 2b: That the Chief Information Officer, Defense Information Systems Agency, "conduct periodic reviews to ensure that the Defense Information Systems Agency's life-cycle management practices and procedures for automated information systems comply with DoD life-cycle management requirements."

Comments: Concur. An August 1993 update of the DISA Acquisition How To Guide, published by DITPRO, details the procedure to delegate signature authority to selected DISA activities for acquisitions within specified dollar thresholds. In accordance with this delegation, the OCIO is responsible for periodic

reviews to ensure continued compliance. To accomplish these reviews, two additional positions were justified and approved, augmenting the one individual previously assigned to this function. One of the new positions has been filled and a selection will be made in February 1994 for an individual to fill the other position. After both of the new staff members have completed a training and familiarization period, the OCIO will begin on-site inspections of DISA contracting offices, DISA activities supported by non-DISA contracting offices, and DISA activities that have been delegated signature authority. To assist with the inspections, the OCIO will prepare an activity self-inspection guide and an inspection schedule. Estimated completion date is 31 March 1994.

e. Recommendation 2c: That the Chief Information Officer, Defense Information Systems Agency, "require that Defense Information Systems Agency directorates update and maintain the Federal Information Processing inventory in the Automation Resources Management System data base."

Comments: Concur. The Office of the Chief Information Officer (OCIO) prepared a memorandum for distribution to DISA components, requiring an aggressive effort to enhance DISA-wide participation in the Defense Automation Resources Management Program (DARMP). The memorandum was signed by the DISA Chief of Staff on 11 January 1994. The DARMP provides consistent procedures, standards, policies, definitions, and requirements governing the redistribution, sharing, and inventory of FIP resources. The memorandum requires that each DISA directorate designate, in writing, an Automation Resources Management System (ARMS) focal point to update and maintain the activity's FIP inventory. All designation responses are due by 31 January 1994. Recommended actions have been completed; however, the OCIO will continue to monitor and oversee the DISA directorates' progress in updating FIP inventories.

f. Recommendation 2d. That the Chief Information Officer, Defense Information Systems Agency, "conduct periodic Automation Resources Management System inventory reconciliations."

Comments: Concur. The OCIO, the Center for Agency Services (CAS), the Joint Interoperability & Engineering Organization (JIEO), and the newly formed Logistics Office are currently working a team project to streamline the entire DISA inventory and redistribution process. A series of meetings have identified critical flaws in the property accountability and inventory arena. The Logistics Office began a Functional Process Improvement (FPI) effort to correct the process, holding the initial meeting on 12 January 1994. This effort will define the roles and responsibilities of the ARMS focal points and Property Accountability Officers. The FPI effort will also define the inventory and redistribution process, including inventory

reconciliation, resolving the inventory reconciliation concern. Estimated completion date is 31 July 1994.

g. Recommendation 2e: That the Chief Information Officer, Defense Information Systems Agency, "direct the Manager of the Information Resources Management Review Program to review information resource programs and activities that have substantial mission impact, resources, or potential vulnerabilities."

Comments: Concur. In consultation with the Office of Management and Budget (OMB), the General Services Agency (GSA) has reevaluated the Federal IRM Review Program. GSA is making changes to the program that will emphasize the importance of agency responsibilities under Section 3506 of the Paperwork Reduction Act, reduce the reporting burden, and help agencies more effectively use their internal IRM review resources. The IRM Review Program within DISA is staffed by one individual. Agency focus on reporting to DoD will be on compliance with Section 3506 and on the results of planned self-assessments, using the "Secretary of Defense Guide for Assessing Component Information Management Activities." This guide addresses seventeen specific basic information management areas. The guidance to comply with the new process is being developed and will include collaboration with the DISA Internal Management Control Program. Estimated completion date is 30 April 1994.

h. Recommendation 2f: That the Chief Information Officer, Defense Information Systems Agency, "conduct an 'Information Resources/Procurement Management Review' at the Defense Commercial Communications Office to determine compliance with Federal and DoD information resource development, acquisition, and reporting requirements."

Comments: Concur. The Office of the Deputy Assistant Secretary of Defense (DASD) for C3I Acquisition conducted an Information Resources/Procurement Management Review (IR/PMR) of the DECCO during the period 25-29 October 1993. Personnel from the DISA Office of the Chief Information Officer participated in this IR/PMR as members of the review team. DECCO management was given a detailed briefing of the findings at the conclusion of the review. Action completed.

i. Recommendation 2g: That the Chief Information Officer, Defense Information Systems Agency, "reevaluate the vulnerability of each Chief Information Officer division, develop specific control techniques that achieve related control objectives, and develop and maintain internal management control documentation."

Comments: Concur. As a result of an Agency reorganization, the Office of the Chief Information Officer was placed under the newly established Deputy Director, Operations, Customer Relations

and Services (DDOCRS). During the formation of this new organization, internal management controls are being implemented as a major consideration. Risk assessments accomplished by the new organization will address the concerns expressed in the draft audit report. Vulnerabilities, control objectives, and control techniques, which will achieve the related objectives, will be developed. Estimated completion date is 30 September 1994.

j. Recommendation 3: That "the Chief Information Officer, with the assistance of the Director, Acquisition Management Organization, establish a process to monitor and track contract actions relative to Delegations of Procurement Authority."

Comments: Concur. The Contract Policy Division, in coordination with the Office of the Chief Information Officer, is currently developing a process to monitor and track contract actions relative to Delegations of Procurement Authority issued to the DITPRO, which is the new DISA organization into which the previous Acquisition Management Office has been assimilated. The estimated completion date is 1 April 1994.

2. Finding B, Automated Information Systems Security. "DISA had not endorsed 25 of 45 automated information systems as being adequately secure, did not have an effective security review program for its systems, and did not adequately staff security positions or provide security training. This occurred because the DISA did not adequately implement its security program for automated information systems. As a result, systems did not comply with Federal and DoD security directives and guidance, and there was no assurance that the Agency's systems were reasonably protected."

Comments: Concur.

a. Recommendation 1: That the Chief Information Officer, Defense Information Systems Agency, "develop a plan, in conjunction with appropriate Agency officials, to bring the Defense Information Systems Agency into compliance with the Computer Security Act of 1987, DoD Directive 5200.28, 'Security Requirements for Automated Information Systems,' and DISA Instruction 630-230-19, 'Security Requirements for Automated Information Systems.' a. Implement and monitor the plan. b. Report periodically to the Director, Defense Information Systems Agency, on the plan's implementation and any unresolved automated information system security issues."

Comments: Concur. The Information Systems Security Division of the OCIO will prepare a plan to be coordinated with appropriate managers. The plan will include the process, responsibilities and realistic milestones for implementation and monitoring by the Office of the Chief Information Officer. The plan will also include a requirement for periodic briefings to the Director,

DISA, regarding the status of the plan and the program. Estimated completion date is 31 March 1994.

b. Recommendation 2: That the Chief Information Officer, Defense Information Systems Agency, "conduct periodic automated information system security reviews in compliance with DoD Directive 5200.28, 'Security Requirements for Automated Information Systems,' and Defense Information Systems Agency Instruction 630-230-19, 'Security Requirements for Automated Information Systems,' August 1991."

Comments: Concur. The OCIO will conduct oversight and compliance reviews of DISA organization automated information systems security programs on an accelerated basis, as funding limitations permit. A review of DISA-Pacific was conducted in June 1993. A schedule of additional reviews will be published upon receipt of FY 1994 funding. Estimated completion date is 28 February 1994.

c. Recommendation 3: That the Chief Information Officer, Defense Information Systems Agency, "identify security data required for effective oversight of the Defense Information Systems Agency's Automated Information System Security Program and revise Defense Information Systems Agency Instruction 630-230-19, 'Security Requirements for Automated Information Systems,' August 1991, to require submission of that data to the Chief Information Officer."

Comments: Concur. The OCIO has rewritten DISA Instruction 630-230-19, "Security Requirements for Automated Information Systems (AIS)," and is currently circulating a draft version to all DISA organizations for comment. The instruction identifies required security data and requires that this data be submitted to the Office of the Chief Information Officer. Estimated completion date is 1 October 1994.

d. Recommendation 4: That the Chief Information Officer, Defense Information Systems Agency, "establish minimum experience and training qualifications for Automated Information System security personnel at the Defense Information Systems Agency and revise Instruction 630-230-19, 'Security Requirements for Automated Information Systems,' August 1991, to require that minimum qualifications are met."

Comments: Concur. The revised DISA Instruction 630-230-19 will identify minimum experience and training qualifications for Automated Information Systems personnel. Estimated completion date is 1 October 1994.

6

# Audit Team Members

| | |
|---|---|
| William F. Thomas | Director, Readiness and Operational Support Directorate |
| Mary Lu Ugone | Audit Program Director |
| James W. Hutchinson | Audit Program Manager |
| Karim Malek | Senior Auditor |
| Judith A. Curry | Auditor |
| Lisa E. Novis | Auditor |
| Suzette L. Luecke | Auditor |
| Mark Ives | Auditor |
| Charlene K. Grondine | Auditor |
| Susan J. Lippolis | Auditor |
| Rhonda L. Ragsdale | Auditor |
| Lance A. Norrington | Auditor |
| Nancy C. Cipolla | Editor |
| Frank Ponti | Statistician |
| Paula D. Hazlewood | Administrative Support |