

P
olicy and

O
versight



Intelligence Support Directorate

Management of Multilevel Security
Applications for DoD Systems

Report Number PO 97-024

June 12, 1997

Office of the Inspector General
Department of Defense

Additional Copies

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

Suggestions for Audits

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

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

Defense Hotline

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

Acronyms

AIS	Automated Information System
DAA	Designated Approving Authority
DISA	Defense Information Systems Agency
MLS	Multilevel Security
MROC	Multicommand Required Operational Capability



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



June 12, 1997

**MEMORANDUM FOR ASSISTANT SECRETARY OF DEFENSE (COMMAND,
CONTROL, COMMUNICATIONS AND INTELLIGENCE)**

**SUBJECT: Audit Report on Management of Multilevel Security Applications for DoD
Systems (Report No. 97-024)**

We are providing this audit report for your review and comment. We considered management comments on a draft of this report in preparing the final report.

DoD Directive 7605.3 requires that all recommendations be resolved promptly. Therefore, we request that the Office of the Assistant Secretary provide additional comments on Recommendations A.2., B.1., and B.2. in response to this final report. We request that management provide comments by August 11, 1997.

We appreciate the courtesies extended to the audit staff. Questions on the audit should be directed to Mr. Charles Santoni, Program Director, at (703) 604-8887 (DSN 664-8887) or Mr. Lloyd O'Daniel, Project Manager, at (703) 604-9562 (DSN 664-9562). See Appendix I for the report distribution. The audit team members are listed inside the back cover.

A handwritten signature in black ink, appearing to read "Russell A. Rau".

Russell A. Rau
Assistant Inspector General
Policy and Oversight

Table of Contents

Executive Summary	i
Part I - Audit Results	
Audit Background	2
Audit Objectives	4
Finding A. System Security Requirements	5
Finding B. Management of Multilevel Security Initiatives	13
Part II - Additional Information	
Appendix A. Scope and Methodology	18
Scope	18
Prior Audits and Other Reviews	18
Appendix B. Systems Descriptions	19
Appendix C. Federal and DoD Security Policies	22
Appendix D. DoD 5200.28-STD Classes of Systems	23
Appendix E. Multilevel Security Guards	24
Appendix F. DoD Multilevel Security Program Office Planned Implementations	26
Appendix G. Service, Joint Staff, and Unified Command Requirements for Equipment	27
Appendix H. Summary of Potential Benefits Resulting From Audit	30
Appendix I. Report Distribution	31
Part III - Management Comments	
Assistant Secretary of Defense (Command, Control, Communications and Intelligence) Comments	34

Office of the Inspector General, DoD

Report No. 97-024
Project No. 6OS-0046

June 12, 1997

Management of Multilevel Security Applications for DoD Systems

Executive Summary

Introduction. To reduce duplications in automated information systems, DoD is migrating from a largely unintegrated collection of systems operating at a variety of classification levels to an integrated network. To migrate to a cohesive, integrated network of systems, DoD needs multilevel security technology that allows secure interoperability between systems operating at different levels (classification levels or non-hierarchical compartments).

Audit Objectives. The audit objective was to evaluate DoD policies, regulations, directives, and instructions for developing and incorporating multilevel security applications in its systems.

Audit Results. We identified two conditions warranting management action.

- o DoD is establishing requirements for multilevel security in automated information systems acquisitions without fully identifying system operational and security requirements. As a result, DoD is acquiring automated information systems that may not have adequate or cost-effective security (Finding A).

- o DoD activities are developing and incorporating multilevel security technology into automated information systems with limited coordination and oversight. As a result, the opportunity exists for duplication, unnecessary expenditures, and increased security risks (Finding B).

Implementing the recommendations in this report will improve the incorporation of adequate security in automated information systems and improve the coordination of multilevel security initiatives throughout DoD. Appendix H summarizes the potential benefits of the audit.

Summary of Recommendations. We recommend that the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) establish security policies and procedures unique to automated information systems, develop a sensitivity labeling standard for automated information systems data storage and processing and policy to implement it throughout DoD, and require an interim review of the Integrated Maintenance Data System's operational and security requirements. We also recommend that policies and procedures be established that require coordination of all DoD multilevel security initiatives with the DoD Multilevel Security Program Office and that the DoD Multilevel Security Program Office be provided adequate authority and resources to coordinate DoD multilevel security initiatives.

Management Comments. The Assistant Secretary stated that a new directive for security requirements for automated information systems will be available October 1997, a Secret and Below Interoperability Memorandum that requires the use of the DoD Security Certification and Accreditation Process for Information Technology was signed March 1997, a labeling policy is being coordinated and should be released soon,

and the Integrated Maintenance Data System is scheduled for review during the fourth quarter of FY 1997. The Assistant Secretary also stated that initiatives are in place to provide coordination and oversight of the management of multilevel security initiatives and agreed that the DoD Multilevel Security Program Office needs an appropriate level of resources to accomplish its responsibilities.

Audit Response. The management comments were only partially responsive to the recommendations. We request that the Assistant Secretary provide a date indicating when a labeling policy will be issued. We also request that the Assistant Secretary reconsider its position on our recommendation to require all DoD multilevel security initiatives to be coordinated with the DoD Multilevel Security Program Office. Further, we request that management address what actions will be taken to provide the DoD Multilevel Security Program Office the resources it needs to accomplish its responsibilities and implementation dates for proposed actions. We request that the Assistant Secretary provide additional comments addressing these issues by August 11, 1997.

Part I - Audit Results

Audit Background

Introduction. The DoD has become increasingly dependent on automated information systems (AISs)¹. According to General Accounting Office Report No. GAO/AIMD-96-84, "Computer Attacks at the Department of Defense Pose Increasing Risks," May 1996, DoD currently has more than 2.1 million computers; 10,000 local networks; 100 long-distance networks; 200 command centers; and 16 central computer processing facilities or megacenters with more than 2 million users.

The Defense Information Infrastructure is the web of communications networks, computers, softwares, databases, applications, data, security services, and other capabilities in DoD. Today, AISs are becoming increasingly integrated into complex computer networks (such as the Internet). DoD is attempting to migrate from a largely unintegrated collection of systems operating at a variety of classification levels to an integrated network to reduce duplications in DoD AISs. An integrated network will give DoD commanders real-time access to information stored on several AISs to obtain a complete battlefield picture. To integrate DoD systems into a cohesive network, DoD needs multilevel security (MLS).

MLS Mode Defined. DoD Directive 5200.28, "Security Requirements for Automated Information Systems," March 21, 1988, defines a MLS mode as "A mode of operation that allows two or more classification levels of information to be processed simultaneously within the same system when not all users have a clearance or formal access approval for all data handled by the AIS." However, MLS mode is not possible with current technology. The "DoD Goal Security Architecture," volume six of the "Technical Architecture for Information Management,"² states that "no current information systems satisfy the long-held desire by users to operate simultaneously under several different security policies on a single device."

Current MLS technology, however, does provide some characteristics of MLS mode. MLS technology allows information to pass between systems of different levels. These levels can be classification levels (such as unclassified, secret, and top secret) or non-hierarchical security compartments (such as proprietary, privacy, mission-sensitive, and compartments within classification levels). Examples of MLS technology are MLS guards³ and compartmented mode workstations⁴.

¹An AIS is an assembly of computer hardware, software, and/or firmware configured to collect, create, communicate, compute, disseminate, process, sort, and/or control data or information.

²The "Technical Architecture for Information Management" provides guidance on all functional area applications developed by or for the Government.

³An MLS guard provides a bridge between systems operating at different security levels by automating the existing manual procedures. The guard can perform functions such as format checking, context checking, dirty word checking, sanitizing, label checking, and data integrity checking.

⁴Compartmented mode workstations are the predominate type of MLS workstation. An MLS workstation allows a user to access systems operating at different security levels from a single

MLS Problem Identified. The Strategic Air Command (now the U.S. Strategic Command) first identified and validated a requirement for MLS in October 1982. In July 1989, Joint Staff Requirements Submission JS 2-89, "Multilevel Security in Command, Control, Communications, and Intelligence Systems," validated the requirement for MLS as a critical operational capability that DoD command, control, communications, and intelligence systems lack.

In the summer of 1989, a panel of Service/Agency MLS representatives, chaired by the Joint Staff, was established to coordinate MLS issues and define the DoD MLS program. The panel tasked the Defense Communications Agency (currently the Defense Information Systems Agency [DISA]) to develop the "Multicommand Required Operational Capability for Multilevel Security in Command, Control, Communications, and Intelligence Systems," the Target Architecture and Implementation Strategy, and a program plan for the Joint MLS Technology Insertion Program (now the DoD MLS Program Office). On February 11, 1991, the Joint Staff validated the Multicommand Required Operational Capability (MROC) document that resulted in the creation of the DoD MLS Program Office. The Office of the Director for Command, Control, Communication and Computers (J-6) is writing a Joint Mission Statement for MLS that will replace the MROC. The draft document designates the same responsibilities for the DoD MLS Program Office as in the original MROC.

Security in AISs. DoD is migrating toward an integrated network with many connections to the Internet. In General Accounting Office Report No. GAO/AIMD-96-84, DISA estimated that DoD may have had 250,000 intrusions on its AISs last year. Although classified information is on separate networks, MLS technology is increasingly allowing the flow of information between unclassified and classified networks. As a result, all systems must have adequate security. DoD Components must properly install, use, and monitor MLS technology to prevent the flow of classified information to unclassified systems and unauthorized access to classified systems. No specific guidance exists on developing and installing MLS technology.

MLS Requirements. In addition to a need to pass information among different levels (classified levels or non-hierarchical compartments) of DoD networks, information needs to pass to networks of other Federal agencies, industry, academia, and U.S. allies.

Principal MLS Activities. DoD has three principal MLS activities. The DoD MLS Program Office in DISA is the designated focal point for DoD MLS initiatives. The Multilevel Information Systems Security Initiative is a National Security Agency initiative with the primary objective of providing a set of secure computer products, including MLS technology, to support network security and interoperability for the Defense Information Infrastructure. The third activity is the DoD MLS Working Group, a DoD forum where representatives from the Services, unified commands, Defense agencies, and contractors meet to exchange information on MLS-related topics.

terminal. It also permits the simultaneous display of different classification levels of information in different windows on the computer and allows authorized users to move information between the two windows.

Audit Results

MLS in DoD AISs. Since 1982, many DoD Components have started MLS initiatives to support operational requirements. DoD Components and contractors have developed more than 70 MLS guards. Twelve AISs in development have stated requirements for MLS. Finding A discusses the incorporation of MLS into new AISs. Finding B discusses the management of past and present DoD MLS initiatives.

Audit Objectives

The audit objective was to evaluate DoD policies, regulations, directives, and instructions for developing and incorporating MLS applications in its systems. See Appendix A for the audit scope.

Finding A. System Security Requirements

DoD is establishing requirements for MLS in AIS acquisitions without fully identifying operational and security requirements. The security requirements are not fully defined because DoD security policies and procedures for AISs are outdated and fragmented. As a result, DoD is acquiring AISs that may not have adequate or cost-effective security.

AIS Infrastructure

The DoD AIS infrastructure consists largely of dedicated, closed systems where all users have security clearances at the highest security classification of the data in the AIS (system-high mode). DoD is migrating from these isolated stand-alone systems into large integrated networks, incorporating distributed processing and client server designs. An integrated network may contain data at different classification levels or sensitive but unclassified data that becomes classified when aggregated. According to DoD guidance, AISs where all users will not have clearances, authorizations, or formal access approval for information handled by the AIS require MLS mode.

Acquisition Policy

The primary DoD acquisition policy document is DoD Directive 5000.1, "Defense Acquisition." Directive 5000.1 states that the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) is the Department's Acquisition Executive for AISs and establishes acquisition policies and procedures unique to AISs. DoD Directive 5000.1 does not address security for AISs. DoD Regulation 5000.2-R, "Mandatory Procedures for Major Defense Acquisition Programs and Major Automated Information System Acquisition Programs," provides the following guidance on information system security.

Information System Security requirements shall be included as a part of program and systems design activities to preserve integrity, availability, and confidentiality of critical program technology and information. Systems security requirements shall be established and maintained throughout the acquisition life-cycle for all ACAT [Acquisition Category] IA programs and others applicable. All AISs shall meet security requirements in accordance with DoDD 5200.28 and

Finding A. System Security Requirements

be accredited by the Designated Approving Authority^[5] prior to processing classified or sensitive unclassified data.

DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)," is the primary security policy for AISs processing classified, sensitive unclassified, and unclassified data. The Directive states that "The DAA must . . . have authority to evaluate the overall mission requirements of the AIS, and to provide definitive directions to AIS developers or owners relative to the risk in the security posture of the AIS."

The role of the DAA is explained in the National Computer Security Center Publication, NCSC-TG-029, "Introduction to Certification and Accreditation." In July 1996, NCSC-TG-031, "Certification and Accreditation Process Handbook for Certifiers," established additional guidance. Both documents emphasize that planning for accreditation should be implemented at the beginning of the system life-cycle to ensure that security protection mechanisms and safeguards are designed and integrated into the system to preclude expensive retrofits and redesign of the systems and that adequate resources are provided for certification and accreditation. The activities of the DAA are driven by the system's security requirements. In turn, the system's security requirements are driven by the system's mission, operational concept, the sensitivity of data to be processed, the user's clearances and authorizations, and the threat environment.

DoD Acquisition of AISs

We reviewed AIS acquisition programs to determine the adequacy of DoD policies and procedures for incorporating MLS into AIS acquisitions. The "Report on Information Technology Resources"⁶ included six AISs under development that included MLS requirements. The Office of the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) provided us a list of six additional AISs with MLS requirements. See Appendix B for the systems' descriptions. From these 12 programs, we judgmentally selected and reviewed four AISs. Three of these four program offices have dropped the requirement for MLS and the remaining program office has not determined how it will achieve MLS.

Reserve Component Automated System. The program office awarded the Reserve Component Automated System contract in 1991 with an MLS requirement. The program office planned to field the system hardware by 1994 and the software by 1996. Schedule slippages and insufficient funding resulted in the establishment of an Assessment Team to identify problem areas and to

⁵The Designated Approving Authority (DAA) is the official with the authority to formally accept the system and assume responsibility for operating a system at an acceptable level of risk.

⁶The Report on Information Technology Resources Exhibit 43 presents resources for all major, non-major, and all other AIS initiatives by corporate information management functional area.

Finding A. System Security Requirements

develop corrective actions. The Team found that the system's requirements were not clearly defined. The Team also found that MLS implementation was the primary cost driver in the program and concluded that the program should delete the MLS requirement. As a result, the program office removed the MLS requirement.

Joint Component Automated Logistics System. The Army will field the Joint Component Automated Logistics System to more than 260 locations with approximately 200,000 users. The program office awarded the contract in 1991 with MLS requirements. In September 1996, the program office determined that MLS was not achievable. The program office had not determined how classified information will be processed. As of October 1996, a DAA had not been appointed.

Sustaining Base Information System. The original concept for the Sustaining Base Information System encompassed 3,700 business functions and a requirement for MLS to protect sensitive unclassified information that becomes classified when aggregated. Congressional direction and budget cuts reduced the program to the eight business functions already in development. The program no longer has a requirement for MLS.

Integrated Maintenance Data System. In July 1996, the program office awarded the Integrated Maintenance Data System contract as a system development contract with undefined MLS requirements. Contract terms require delivery of a core system within 2 years. The core system will provide the basic system architecture and initial capability from which the full set of requirements, including MLS, are developed. The program office plans to field the core system with an operating system that may not support future MLS requirements. At the time of our review, the program had not appointed a DAA.

System Requirements for MLS. Three of the program offices dropped their requirements for MLS because MLS was either not needed after functional requirements were fully determined or because MLS was not technically feasible. The DAAs were not involved in developing the original system requirements. In addition, existing security guidance mandated a MLS mode for these systems.

Current acquisition and security policies do not require the DAA to help determine the AIS security requirements. Acquisition policies state only that the DAA must accredit the AIS before the AIS can process classified or sensitive unclassified data. Security policy states that the DAA is responsible for the overall security of the AIS. We believe that if DAAs had been appointed early enough to be involved in the concept and design development phases of the systems we reviewed, the program offices would have been better able to determine their systems' operational and security requirements.

Finding A. System Security Requirements

Security guidance requires a MLS mode for all AISs that process information where all users do not have clearances for, or authorized access to, all data. However, the technical community understands and the "DoD Goal Security Architecture" states that current technology does not support a MLS mode. Existing technology can be successfully incorporated into a system design to allow some MLS capability.

The user, program manager, and DAA need to determine the most cost-effective use of available MLS technologies based on the operational needs and security requirements. The most cost-effective system security is designed into the system from the beginning. When security is added after a system has been designed, the system's cost can increase from 10 to 40 percent or in some cases even more because the system must repeat the design and testing processes.

Security Policies and Procedures

Numerous Federal and DoD policies address security. A chart depicting the various Federal and DoD security policies is in Appendix C. General Accounting Office Report No. GAO/AIMD-96-84 states that "The military services and Defense agencies have issued a number of information security policies, but they are dated, inconsistent, and incomplete."

DoD Directive 5200.28. DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)," is the primary policy for safeguarding classified, sensitive unclassified, and unclassified information processed in AISs. Enclosure four, "Procedure for Determining Minimum AIS Computer-Based Security Requirements," contains criteria for determining system security mode-of-operation based on the sensitivity of information in the AIS and the security clearances of its users. Using this criteria, DoD Directive 5200.28 dictates that an AIS must operate in the MLS mode if all AIS users will not have clearances, authorization, or formal access approval for all information handled by the AIS.

DoD Standard 5200.28-STD. The "Computer Security Requirements Scale," in DoD Directive 5200.28, specifies that the system must meet technical security criteria and evaluation methodologies criteria in DoD 5200.28-STD, "Department of Defense Trusted Computer System Evaluation Criteria." The criteria are divided into security classes, which represent the measured degree of confidence in a system to protect sensitive information. See Appendix D for descriptions of the security classes. The Directive states that a MLS mode requires a B1 or higher security class. DoD 5200.28-STD requires that B1 and higher security classes have the ability to not only preserve the integrity of sensitivity labels but also to use labels to enforce a set of mandatory access control rules. Sensitivity labeling is the machine-readable information attached to the data that represents the classification of the data. Mandatory access control is the means of restricting access to data based on the sensitivity (as represented by the label) of the information and the formal authorization and clearance of a user. DoD does not have a sensitivity labeling standard for

Finding A. System Security Requirements

processing and storing data in AISs. Without a DoD standard, each program expends resources to develop proprietary labeling. Proprietary sensitivity labels do not cause a problem in stand-alone, closed systems. However, because DoD is migrating to an integrated network of systems, the absence of a standard sensitivity labeling policy will create interoperability problems.

Sensitivity Labeling. The Information Security Labeling Subgroup, Information Security Standardization Working Group, at DISA held its initial Information Security Labeling workshop in September 1996. The working group's tasks are to research and collect information on labeling from the community, develop labeling standards, and submit draft labeling standards for coordination. At present, the group has insufficient resources to accomplish its tasks.

Security Classes. DoD Directive 5200.28 states that if security features (as defined in DoD 5200.28-STD) for B1 or higher security classes are required, the requirement shall be met by acquiring trusted products listed on the National Security Agency's evaluated products list or products with security features that meet the security class. This statement suggests that combining trusted computer products or products that meet the same security class results in the same security class for the entire system. Combining components certified at the same security class does not result in the combined entity being certifiable at that security class. Each product is evaluated independently. The manner in which products are integrated and configured into a system directly effect the system's resulting security class. Poor integration or configuration management can greatly diminish the security class of the products and the system as a whole. However, program offices are still contracting for security classes instead of defining the security attributes that their systems' operational functions require.

The National Security Agency realizes that the criteria in DoD 5200.28-STD is no longer applicable to today's integrated networked systems. The National Security Agency will no longer certify components at trusted levels or classes but will develop a minimum essential requirements document that will provide the contractors a better understanding of DoD security requirements.

Security Certification and Accreditation Process. The DAA is responsible for the overall security of the AIS and must accredit the AIS before it begins processing classified or sensitive unclassified information. The National Computer Security Center provides guidance on certification and accreditation and the role of the DAA. It emphasizes the need to plan for accreditation from the beginning of the system's life-cycle, thereby requiring the DAA to be involved in the system's requirements determination process.

DoD is aware of the inadequacies of the accreditation process. In August 1992, the Office of the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) tasked DISA, in coordination with the Services and Defense agencies, to develop a standard process for certification and accreditation. A standard process would minimize the risks associated with nonstandard security implementations across the shared Defense Information Infrastructure. The group evaluated 10 processes, but found none suitable for

Finding A. System Security Requirements

use DoD-wide. DISA drafted the Defense Information Technology Security Certification and Accreditation Process Document, which provides a common framework to certify and accredit all DoD systems within the network infrastructures they employ and to maintain the security of these systems throughout their life-cycle.

The Defense Information Technology Security Certification and Accreditation Process has four phases. The first phase, "Definition," defines the certification and accreditation level of effort, identifies the DAA, and documents the security requirements necessary for certification and accreditation. The objective of the first phase is to establish a binding System Security and Authorization Agreement on the level of security required before the system development begins or changes are made to a system. The program manager, the DAA, and the user representative use the agreement to resolve schedule, budget, security, availability, functionality, and performance issues. The other phases are "Verification," "Validation," and "Post Accreditation." DISA does not have the authority to ensure the adoption of the process throughout DoD. DoD needs to establish policy for a standard accreditation process that involves the DAA in the development of the system's functional requirements and design. This process should include a requirement for a document that represents an agreement between the users, the program manager, and the DAA that resolves all issues concerning system security before contract award.

Conclusion

To provide better access to real-time information and to reduce the duplication and high cost of maintaining legacy systems, the Defense Information Infrastructure is migrating to an integrated network of systems. With that connectivity come much greater security risks. To manage the risk of large interconnected systems, security must be a priority. DoD dependence on information systems and infrastructures has grown. This growing dependence heightens concern about the vulnerability of electronic threats to the Defense Information Infrastructure. Attacks would seriously affect the ability of DoD to implement its assigned missions and functions. Current DoD security policies and procedures are not sufficient for acquisition of today's AISs. Because of outdated security policies and the lack of responsible security authority involvement in the requirements determination, program offices are contracting for security requirements that may not be cost-effective or feasible.

Security policies direct programs to require a MLS mode if the AIS will process more than one classification of data and all users will not have the authorization or clearances for all data. To develop the most cost-effective and efficient system design, the program manager, the user, and the DAA need to accurately and jointly determine the system's operational and security functional requirements. Present policies do not require the involvement of the DAA in the security requirements determination process. Without the involvement of the DAA, the system's security may not be cost-effective or creditable and vulnerability to threats may be increased.

Policies and procedures unique to AISs need to be developed to enable DoD to acquire cost-effective, secure AISs. The Defense Information Technology Security Certification and Accreditation Process Document standardizes the accreditation process and requires that the users, program manager, and DAA determine the operational and security requirements, as well as the system design. Policy must be established to require the DoD community to implement this process. Also, DoD needs to issue security policies that reflect the environment to which DoD is migrating.

The operational functions, the applicable security policies, and the security technology available to secure a system should determine the system's design. The system's security policies depend on the system's operational functions, the classification of the data involved, and the clearances of the personnel who will need access to the data.

Recommendations, Management Comments and Audit Response

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

1. Establish security policies and procedures unique to automated information systems. These policies and procedures should:

a. Reflect the current and future automated information system technologies and environment.

b. Require the user representatives, the program manager, and the designated approving authority to develop the system's operational and security functional requirements and prepare a document of agreement that resolves all system security issues.

c. Establish a standard security certification and accreditation process.

2. Develop a sensitivity labeling standard for automated information system data storage and processing and establish policy to implement it throughout DoD.

3. Require an interim review of the Integrated Maintenance Data System's operational and security requirements.

Management Comments. The Assistant Secretary agreed with the finding and recommendations and stated that a new directive for security requirements for automated information systems will be available in October 1997. He also indicated that in March 1997 he signed a "Secret and Below Interoperability Memorandum" that requires the use of the DoD Security Certification and

Finding A. System Security Requirements

Accreditation Process for Information Technology. Further, the Assistant Secretary stated that a labeling policy is being coordinated and should be released soon and that the Integrated Maintenance Data System is scheduled for review during the fourth quarter of fiscal year 1997.

Audit Response. We consider the management comments responsive. However, the Assistant Secretary did not indicate the estimated date by which a labeling policy will be issued. We ask that the Assistant Secretary provide that date in response to the final report.

Finding B. Management of Multilevel Security Initiatives

DoD activities are developing and incorporating MLS technology into AISs with limited coordination and oversight. Because DoD does not have a MLS focal point with adequate authority and resources to coordinate DoD MLS initiatives, the opportunity exists for duplication, unnecessary expenditures, and increased security risks.

MLS Initiatives

Since DoD identified MLS as a needed capability, various DoD Components and contractors have developed numerous MLS technologies. These initiatives include the development of guards. Since 1982, the Services, unified commands, agencies, and contractors have developed at least 70 guards that address unique MLS problems. A list of DoD and commercial MLS guards are in Appendix E. An Assistant Secretary of Defense (Command, Control, Communications and Intelligence) memorandum, "Service Multilevel Security (MLS) Projects," August 12, 1992, states that the DoD MLS Program Office identified more than 100 MLS projects that were initiated to meet Service requirements. The number of current MLS initiatives is unknown. The DoD MLS Program Office is surveying all DoD Components to determine the number and types of MLS technologies in use or in development within DoD.

As DoD migrates toward an integrated network of AISs at various classifications levels, the demand for MLS technology will grow. The August 12, 1992, memorandum emphasized the need for coordination of all DoD MLS initiatives, in particular Service initiatives. DoD does not have the necessary resources to pursue multiple independent MLS solutions. Coordination is necessary to take advantage of technology advances and ensure that new projects do not duplicate other efforts. The Assistant Secretary of Defense (Command, Control, Communications and Intelligence) tasked the DoD MLS Program Office to coordinate MLS projects so that DoD could use previous lessons learned and avoid wasteful duplication of effort. Unfortunately, the DoD MLS Program Office could not provide the needed coordination because of inadequate resources and authority.

DoD MLS Program Office

The MROC established the DoD MLS Program Office to expedite the development and fielding of MLS capabilities. According to the MROC, the DoD MLS Program Office is responsible for:

Finding B. Management of Multilevel Security Initiatives

- o Planning and coordinating DOD MLS projects and initiatives.
- o Developing and evaluating generic MLS technology, including architectures and standards, methodology and guidance, individual components, and system configurations. This work will be accomplished by DOD departments and agencies and at designated test-beds.
- o Engineering assistance to aid operational facilities (i.e., assist requirements documentation, define operational scenarios, evaluate products and approaches, and refine system solutions).

The DoD MLS Program Office focuses on the integration of near-term MLS products, whether developed by the Multilevel Information Systems Security Initiative or industry, to meet warfighter operational requirements for the unified commands. The DoD MLS Program Office conducted engineering studies at the unified commands from 1992 through 1994 to identify DoD MLS operational requirements. Based on the results of those studies, the DoD MLS Program Office fielded selected MLS guards and workstations in the theaters.

Authority and Resources to Coordinate MLS Initiatives. The DoD MLS Program Office has not coordinated all DoD MLS initiatives because of inadequate authority and resources. No DoD guidance requires DoD Components to coordinate the installation and development of MLS technology with the DoD MLS Program Office. As a result, the DoD MLS Program Office is unable to fulfill its responsibilities to plan and coordinate DoD MLS projects and initiatives.

The DoD MLS Program has consistently had inadequate resources since its inception. The DoD MLS Program Office has depended on funds from DISA and other agencies, as well as fee-for-service taskings. From FYs 1990 through 1996, the DoD MLS Program Office received less than \$12 million to develop and install MLS applications. In Program Decision Memorandum II, DISA allocated \$30.3 million for FYs 1997 through 2001 to integrate MLS capabilities into the Global Command and Control System. In FY 1997, the DoD MLS Program Office will receive \$6.2 million of the funds to work on its projects. The DoD MLS Program Office also has limited staff. As of January 8, 1997, the DoD MLS Program Office had a staff of four people (two permanently assigned and two temporarily assigned).

Identified MLS Requirements. In February 1996, the Joint Chiefs of Staff, Director of Command, Control, Communications and Computers (J6), surveyed the Services and unified commands for their requirements for MLS technology. The submission resulted in approximately 500 MLS requirements. Appendix F lists the DoD MLS Program Office's plan to satisfy MLS requirements for FYs 1997 and 1998. Appendix G lists the MLS equipment to fulfill the activities' requirements for which MLS technology is available. Most necessary resources are currently not available.

Benefits of a DoD MLS Focal Point

The DoD MLS Program Office, the designated focal point for MLS, was unable to coordinate MLS initiatives because of inadequate authority and resources. Since DoD does not have the needed resources to pursue multiple independent MLS solutions, coordination of MLS developmental efforts is essential. Therefore, a DoD MLS focal point that can coordinate MLS initiatives is necessary. Because of the lack of resources for coordinating MLS initiatives, DoD cannot monitor MLS initiatives and cannot develop policy, standards, and guidance for MLS or a strategy to take advantage of emerging MLS technology. Coordination of DoD MLS initiatives would minimize excessive expenditures and duplicative efforts by allowing DoD to use existing technology and benefit from lessons learned. A focal point would also provide the necessary guidance and engineering assistance to promote proper use of MLS technology. Without adequate guidance, DoD Components may not properly install, use, and monitor MLS technology, thereby increasing security risks in DoD AISs. The coordination of MLS initiatives could result in technological, developmental, and financial advantages to DoD.

Recommendations, Management Comments and Audit Reponse

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

1. Establish policies and procedures that require the coordination of all DoD multilevel security initiatives with the DoD Multilevel Security Program Office.

2. Provide the DoD Multilevel Security Program Office with sufficient resources to adequately perform the following responsibilities outlined in the "Multicommand Required Operational Capability for Multilevel Security in Command, Control, Communications, and Intelligence Systems":

a. Plan and coordinate DoD multilevel security projects and initiatives.

b. Develop and evaluate generic multilevel security technology, including architectures and standards, methodology and guidance, individual components, and system configurations.

c. Provide engineering assistance to aid organizations in implementing multilevel security technology.

Finding B. Management of Multilevel Security Initiatives

Management Comments. The Assistant Secretary stated that initiatives are in place to provide coordination and oversight of the management of MLS initiatives. The MLS Working Group serves as the focal point with the Services and Agencies for the development of Departmental policy and guidance governing the implementation and management of the integration and interoperability of users and systems operating at various classification levels. The Assistant Secretary agreed that an appropriate level of resources needs to be applied to the MLS Program Office.

Audit Response. The management comments are partially responsive to the recommendations. At present, no DoD directive requires DoD organizations to coordinate MLS initiatives with the DoD MLS Program Office, the designated focal point for DoD MLS initiatives. As a result, the DoD MLS Program Office cannot oversee and provide guidance for the implementation of MLS. While the MLS Working Group serves a positive purpose, it does not have the authority or the resources to assume the designated focal point responsibilities assigned to the DoD MLS Program Office in the MROC. Therefore, we do not agree that sufficient initiatives are in place or that the MLS Working Group is the appropriate vehicle for providing coordination and oversight of the management of MLS initiatives. We request that the Assistant Secretary reconsider his position on Recommendation B.1. and provide additional comments in response to the final report. The response should indicate actions to be taken to implement the recommendation and estimated completion dates.

Although the Assistant Secretary agreed with Recommendation B.2., the management comments did not indicate what actions would be taken to provide the DoD MLS Program Office the resources needed to adequately perform the responsibilities outlined in the recommendation. We request that the Assistant Secretary address the actions to be taken and provide estimated completion dates in response to the final report.

Part II - Additional Information

Appendix A. Scope and Methodology

Scope

Management of MLS Initiatives. We reviewed the DoD policies and guidance for developing and incorporating MLS applications in DoD AISs. We interviewed DoD personnel who establish security guidance for AISs. We also interviewed personnel at DoD Components that implement MLS in AISs. We did not use computer-processed data or statistical sampling procedures to conduct this audit.

Audit Period, Standards, and Locations. This economy and efficiency audit was performed from April through November 1996, in accordance with auditing standards issued by the Comptroller General of the United States, as implemented by the Inspector General, DoD.

Organizations and Individuals Visited or Contacted. We visited or contacted organizations and individuals within the DoD and the Institute for Defense Analysis. Further details are available on request.

Prior Audits and Other Reviews

No prior audit work on MLS has been conducted within the last 5 years.

Appendix B. Systems Descriptions

Army

Joint Computer-aided Acquisition and Logistics Support. The Joint Computer-aided Acquisition and Logistics Support system provides an infrastructure capable of integrating digitized technical data that will meet the Services/Defense Logistics Agency initial goal of automating technical manual processes and functions. The estimated program costs and life-cycle costs for Joint Computer-aided Acquisition and Logistics Support are \$641.2 million and \$2.2 billion, respectively.

Reserve Component Automation System. The Reserve Component Automation System is an automated information management system that will assist Reservists with day-to-day office administration and mobilization planning and execution applications. The Reserve Component Automation System uses commercial off-the-shelf and Government off-the-shelf hardware and software where possible.

Sustaining Base Information System. The Sustaining Base Information System was to modernize 20 business software applications and the associated infrastructure to support the sustaining base needs of the Army. The implementation of Sustaining Base Information System will begin the transition of Army sustaining base information processing to an open system environment. The estimated program costs and life-cycle costs for Sustaining Base Information System are \$590 million and \$1.4 billion, respectively.

Air Force

Global Decision Support System. The Global Decision Support System is the Air Mobility Command's primary command and control system to manage and monitor the execution of strategic airlift and air refueling missions. The redesigned Global Decision Support System replaces the legacy unclassified Global Decision Support System and the Secret Tanker Airlift Mobility Information System. From FYs 1984 through 1995, approximately \$178 million was spent on the Global Decision Support System.

Integrated Maintenance Data System. The Integrated Maintenance Data System will provide Air Force decisionmakers with information on operational readiness. The system will integrate multiple and diverse maintenance

Appendix B. Systems Descriptions

information systems into a single open system client/server network to provide a single data repository for the Air Force. The Air Force has recently awarded a \$65.9 million contract for software development.

DISA

Commodity Command Standard System. The Commodity Command Standard System is the Army's legacy wholesale logistics system that supports the operations of the Army's national inventory control and maintenance points. It is the world's largest integrated business system with more than 300 separate subsystems and 1,600 separate programs.

Defense Message System. DISA established the Defense Message System program to develop an integrated, common user, organizational, and individual messaging and directory services system for DoD. The system will process electronic messages for all classifications levels, compartments, and handling instructions. The system will replace the resource-intensive Automatic Digital Network and messaging systems throughout DoD.

Global Combat Support System. The Global Combat Support System is an integration and interoperability initiative that will provide the information technology capabilities required to move and sustain joint forces in the DoD.

Global Command and Control System. The Global Command and Control System is a DoD-wide command and control system that will provide complete tactical information to the warfighter. The system replaces the World Wide Military Command and Control System.

Information Systems Security. The goal of the Defense Information Infrastructure Information Systems Security initiative is to deploy state-of-the-art telecommunications and information system security technologies configured to support movement of multilevel classifications of information horizontally and vertically within DoD without regard to organizational boundaries or physical location. The estimated program costs and life-cycle costs are each \$441.8 million.

Office of the Secretary of Defense

The High Performance Computing Modernization Program will strategically locate, rapidly deploy, sustain, and upgrade the computing environments and

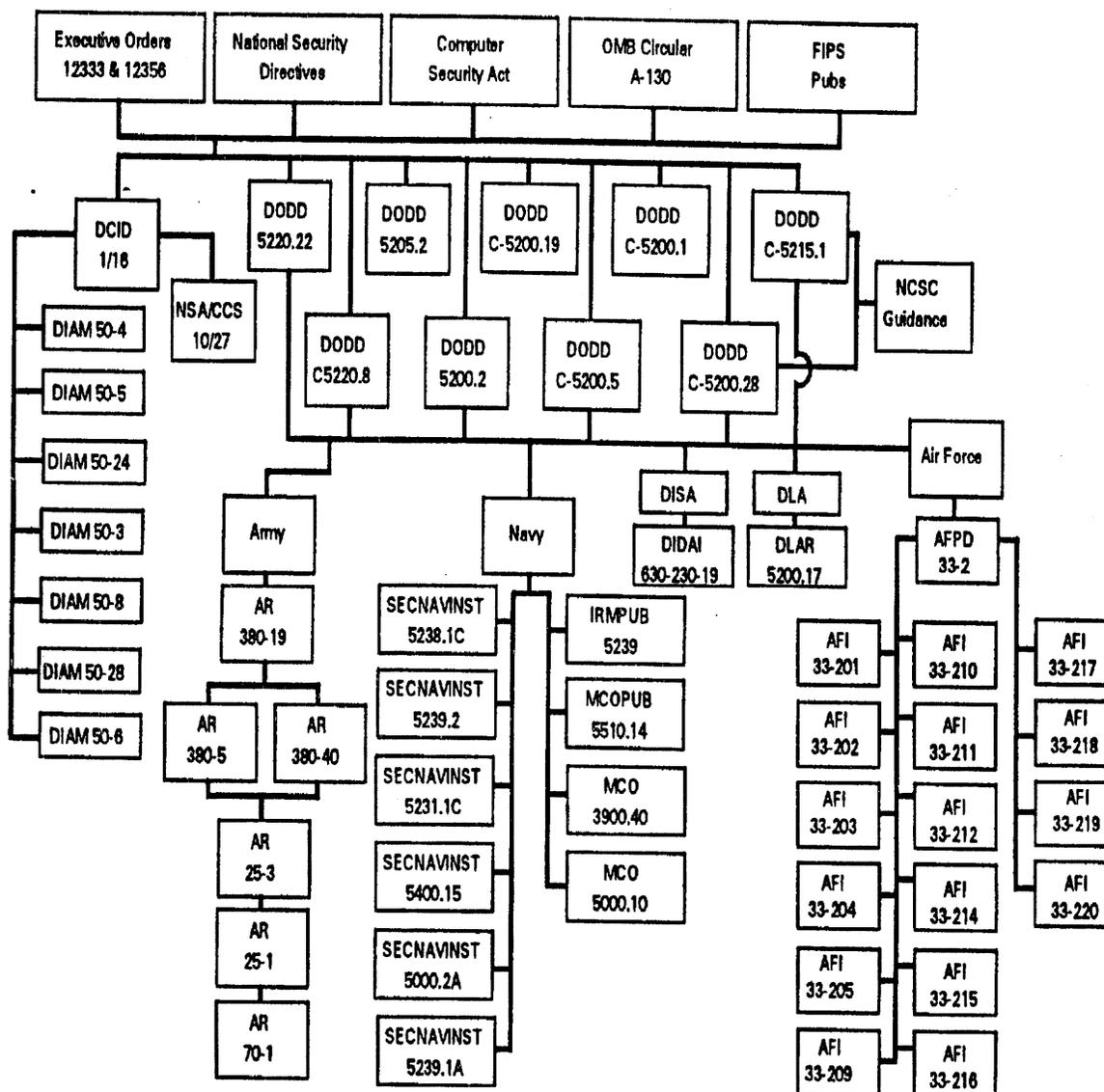
networks for the DoD laboratories and test facilities. The estimated program costs and life-cycle costs for High Performance Computing Modernization Program are \$522 million and \$5.4 billion, respectively.

Joint Staff

The Joint Staff Automated for the Nineties system will satisfy mandatory headquarters office automation support requirements. The estimated program costs and life-cycle costs for Joint Staff Automated for the Nineties are \$47.5 million and \$84.4 million, respectively.

Appendix C. Federal and DoD Security Policies

The DISA Cerfication Branch developed this chart to depict the numerous Federal and DoD policies in existence.



Appendix D. DoD 5200.28-STD Classes of Systems

Class D: Minimal Protection. This class is reserved for those systems that have been evaluated but failed to meet the requirements for a higher evaluation class.

Class C1: Discretionary Security Protection. This class nominally satisfies the discretionary security requirements by providing separation of users and data. The Class C1 environment is expected to be one of cooperating users processing data at the same level(s) of sensitivity.

Class C2: Controlled Access Protection. This class enforces a more finely grained discretionary access control than C1 systems, making users individually accountable for their actions through login procedures, auditing of security-relevant events, and resource isolation.

Class B1: Labeled Security Protection. This system requires all features required for a Class C2 system. In addition, an informal statement of the security policy model, data labeling, and mandatory access control over named subjects must be present. The capability must exist for accurately labeling exported information.

Class B2: Structured Protection. This system is based on a clearly defined and documented formal security policy model that requires the discretionary and mandatory access control enforcement of Class B1 systems to be extended to all subjects and objects in the automated data processing system. In addition, covert channels are addressed and the system is relatively resistant to penetration.

Class B3: Security Domains. This class must satisfy the reference monitor requirements that it mediate all accesses of subjects to objects, be tamperproof, and be small enough to be subjected to analysis and tests. This system is highly resistant to penetration.

Class A1: Verified Design. This class is functionally equivalent to those in Class B3 in that no additional architectural features or policy requirements are added. The distinguishing feature of systems in this class is the analysis derived from formal design specification and verification techniques and the resulting high degree of assurance that the trusted computer base is correctly implemented.

Appendix E. Multilevel Security Guards

The following are is a list of MLS guards we identified that have been developed by DoD and contractors. The guards that we identified as sponsored, developed, or evaluated by DoD are asterisked "*."

Advanced Command and Control Architectural Testbed Guard
Air Force Mission Support System Guard*
All Source Analysis System Message Security Filter*
Army Information Security Guard*
Automatic Digital Network Security Communications Controller*
Boeing Mail Guard
Boeing MLS Local Area Network*
Collateral Filter*
Command and Control Guard*
Communications Front End*
Compartmented Mode Workstation Guard*
Defense Message System Firewall Plus*
Defense Message System Objective Guard*
Dual Desktop System
El Paso Intelligence Center Guard
Electronic Interface between the Strategic War Planning System and
Intelligence Data Handling System for the 90's Link Guard*
Firewall Guard*
GateGuard*
Gemini Trusted Network Processor*
Generic Trusted Intermediary*
Global Decision Support System Guard*
Global Transportation Network Guard*
GuardMail
Imagery Support Server Environment*
Intelligence Guard for Office of Naval Intelligence Replicator*
Joint Maritime Command Information System Information Flow
Improvement*
Joint Services Imagery Processing System Guard*
Knowledge-Based MLS*
Large Scale Integration Guard
Linked Ops-Intel Centers Europe/Intra-theater Intelligence Communications
Network Guard*
Logical Coprocessing Kernel Guard*
Logistics Data Network WorldWide Military Command and Control System
Automatic Data Processing Interface Terminal*
Message Flow Modulator*
Message Release Register*
MLS-100*

Modern Aids to Planning System/Command Automation System Guard*
National Aeronautics and Space Administration Restricted Access Processor
Guard*
Navy Modular Automatic Communications System-2 Guard*
Ocean Surveillance Information System Baseline Upgrade Sanitization*
One-Way Gateway*
One-Way Guard
One-Way Printer Port*
Periods Processing*
Prototype Secondary Information Dissemination System*
Radiant Mercury*
Recon Guard
Relocatable Army Processors for Intelligence Data-Europe Guard*
Secret-to-Unclassified Network Guard*
Secure Cooperate Processing Environment*
Secure Network Server*
Security Release Station
Security Release Terminal
Sensitive Compartmented Information Isolation Segment*
Simplex Links*
Standard Mail Guard*
Strategic Threat Analysis and Tracking System-3 Guard*
Stunt Box (also called Message Security Unit)*
Supreme Allied Commander, Atlantic Filter*
Tactical Exploitation of National Capabilities Guard*
Trusted Interlink Dissemination/Access Server
Trusted MLS Email Guard-100
Trusted MLS Email Guard-200
Trusted MLS Email Guard-200+
Trusted MLS Email Guard-2000
U.S. Air Force, Europe Guard*
U.S. Army, Europe Guard*
U.S. Forces Command Security Monitor*
Universal Guard*
VERDIX Secure Local Area Network
VERDIX Secure Local Area Network Exportable
WorldWide Military Command and Control System Information System
Workstation Guard*
WorldWide Military Command and Control System Guard*

Appendix F. DoD Multilevel Security Program Office Planned Implementations

This chart depicts the DoD MLS Program Office MLS implementation plan. The bold and italicized entries will be funded by the program office. The remaining projects are fee-for-service tasks. Entries to be determined (TBD) may be implemented in either FY 1997 or 1998, as funds become available.

<u>Unified Command</u>	<u>FY 1997</u>	<u>FY 1998</u>	<u>TBD</u>
U.S. Atlantic Command	GCCS Guard, Imagery Guard, MLS Server		<i>Upgrade OIW, Modify SMG to SNS</i>
U.S. Central Command	Imagery Guard	GCCS Guard, SNS	<i>Upgrade OIW</i>
U.S. European Command	GCCS Guard	Imagery Guard, MLS Server	<i>OIW, Modify SMG to SNS</i>
U.S. Forces Korea	SNS		<i>Upgrade OIW, GCCS Guard</i>
U.S. Pacific Command	GCCS Guard, <i>MLS Server*</i>		<i>Upgrade OIW, Modify SMG to SNS, Imagery Guard</i>
U.S. Southern Command	OIW, GCCS Guard, SNS, Imagery Guard, MLS Server		
U.S. Space Command	OIW, GCCS Guard	Imagery Guard	Modify SMG to SNS
U.S. Special Operations Command		Imagery Guard	<i>Upgrade OIW, Modify SMG to SNS</i>
U.S. Strategic Command	OIW, MLS Server	GCCS Guard, Imagery Guard	SNS
U.S. Transportation Command		OIW, SNS, Imagery Guard	<i>GCCS Guard</i>

*The MLS Server is jointly funded by the U.S Pacific Command and the DoD MLS Program Office.

Acronyms

GCCS	Global Command and Control System
OIW	Ops/Intel Workstation
SMG	Standard Mail Guard
SNS	Secure Network Server

Appendix G. Service, Joint Staff, and Unified Command Requirements for Equipment

The DoD MLS Program Office received 500 MLS requirements. The DoD MLS Program Office evaluated these requirements to determine which could be met using current technology. The following list is the equipment necessary to fulfill the selected requirements for the Joint Staff, Unified Commands, and Services. The estimated cost of the necessary equipment is \$32.8 million.

The following acronyms are used in this Appendix but were not used earlier in the report.

ACOM	Atlantic Command
CENTCOM	Central Command
CTAPS	Contingency Theater Automated Planning System
DADS	Division Air Defense System
DBMS	Data Base Management System
EUCOM	European Command
PACOM	Pacific Command
SOCOM	Special Operations Command
SOUTHCOM	Southern Command
SPACECOM	Space Command
STRATCOM	Strategic Command
TRANSCOM	Transportation Command

Appendix G. Service, Joint Staff, and Unified Command Requirements for Equipment

Equipment	Army	Navy	Air Force	Marine Corps	Joint Staff	ACOM
A. 1-Way Transfer COSPO Workstation			8		6	2
B. 2-Level Workstation			8		2	
C. Collaborative Virtual Work Space						
D. Command and Control Guard	1		4	2	1	1
E. Cryptographic solutions ¹	X		X		X	
F. Encryption solutions ¹						
G. GCCS Trusted Workstation	4	20	10	20	2	6
H. Imagery Guard		1	2	1	1	
I. Intercoalition Workstation						
J. MLS CTAPS (future)						
K. MLS DBMS			3	1	1	1
L. MLS DADS (future)						1
M. MLS Local Area Network		1 ²				
N. MLS Releasability Server						
O. Office Automation Trusted Workstation			26			2
P. OIW			4	2	2	
Q. Radiant Mercury		1				
R. SNS Mail Guard	4	3	4	2	2	2
S. SNS Mail Guard with backup					2	
T. Trusted Workstation	2			20		

¹The number of cryptographic and encryption solutions were not specified. An "X" indicates a requirement for solutions.

²The cost of the Navy's MLS LAN is not in the total estimated cost of necessary equipment.

Appendix G. Service, Joint Staff, and Unified Command Requirements for Equipment

	CENTCOM	EUCOM	PACOM	SOCOM	SOUTHCOM	SPACECOM	STRATCOM	TRANSCOM	
		1					2		A.
		2				2			B.
		1							C.
		2	1	2	2	2	1		D.
X	X	X	X				X		E.
						X			F.
4	30	16			14	9	6		G.
		1					1		H.
		2							I.
		1							J.
1	1	1	1				3		K.
									L.
1		1							M.
		1							N.
		2					100		O.
	1	1	4	2	6	12			P.
1		1							Q.
2	3	5	2	4	3	3	2		R.
									S.
		24	10	6			4		T.

Appendix H. Summary of Potential Benefits Resulting From Audit

Recommendation Reference	Description of Benefit	Amount and Type of Benefit
A.1.a.	Management Controls. Establishes security policies to ensure that AISs incorporate feasible security.	Nonmonetary.
A.1.b.	Management Controls. Establishes policies for AISs to better determine operational and security requirements and to resolve security issues before contract award.	Nonmonetary.
A.1.c.	Management Controls. Establishes policies to ensure all DoD AISs are accredited to a standard level of confidence.	Nonmonetary.
A.2.	Management Controls. Establishes policies to ensure interoperability of integrated networks.	Nonmonetary.
A.3.	Program Results. Will ensure that the program office has fully determined cost-effective and feasible user operational and security requirements.	Nonmonetary.
B.1.	Management Controls. Establishes policies and procedures for coordination of MLS initiatives.	Nonmonetary.
B.2.	Program Results. Assists the DoD MLS Program Office in fulfilling its duties.	Nonmonetary.

Appendix I. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense (Comptroller)

Deputy Chief Financial Officer

Deputy Comptroller (Program/Budget)

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

Assistant Secretary of Defense (Public Affairs)

Assistant to the Secretary of Defense for Intelligence Oversight

Director, Defense Logistics Studies Information Exchange

Joint Staff

Director, Joint Staff

Department of the Army

Auditor General, Department of the Army

Department of the Navy

Assistant Secretary of the Navy (Financial Management and Comptroller)

Auditor General, Department of the Navy

Department of the Air Force

Assistant Secretary of the Air Force (Financial Management and Comptroller)

Auditor General, Department of the Air Force

Other Defense Organizations

Director, Defense Information Systems Agency
Director, Defense Logistics Agency
Director, National Imagery and Mapping Agency
Inspector General, National Imagery and Mapping Agency
Director, National Security Agency
Inspector General, National Security Agency
Inspector General, Defense Intelligence Agency

Non-Defense Federal Organizations

Office of Management and Budget
Technical Information Center, National Security and International Affairs Division,
General Accounting Office

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

- Senate Committee on Appropriations
- Senate Subcommittee on Defense, Committee on Appropriations
- Senate Committee on Armed Services
- Senate Select Committee on Intelligence
- Senate Committee on Governmental Affairs
- House Committee on Appropriations
- House Subcommittee on National Security, Committee on Appropriations
- House Committee on Government Reform and Oversight
- House Subcommittee on Government Management, Information, and Technology,
Committee on Government Reform and Oversight
- House Subcommittee on National Security, International Affairs, and Criminal
Justice, Committee on Government Reform and Oversight
- House Committee on National Security
- House Permanent Select Committee on Intelligence

Part III - Management Comments

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



ASSISTANT SECRETARY OF DEFENSE

6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

May 19, 1997



MEMORANDUM FOR ASSISTANT INSPECTOR GENERAL POLICY AND OVERSIGHT

SUBJECT: Audit Report on Management of Multilevel Security
Applications for DoD Systems (Project No.60S-0046)

Your memorandum of February 11, 1997, requested comments on the subject draft document in preparation for the publication of the final report. The following are our comments to the proposed findings and recommendations.

Response to Finding A: Agree with the finding that "... multilevel security (MLS) requirements in automated information systems (AIS) acquisitions ... are not fully defined because DoD security policies and procedures for AISS are outdated and fragmented. ..." and with recommendations (Establish policies and procedures ..., Develop a sensitivity labeling standard ..., and ... review Integrated Maintenance Data System's ... security requirements).

In October 1996, I chartered the Information Assurance Group (IAG) to revise DoD Directive 5200.28, "Security Requirements for Automated Information Systems," noted in your report. A new directive will be available in October 1997. In March 1997, I signed the Secret and Below Interoperability (SABI) memorandum dated March 20, 1997. The SABI provides implementation guidelines for the sharing of information among users and interconnecting systems - networks at secret levels with users and systems - networks down to the unclassified level. SABI includes the use of a standard certification and accreditation process, "Department of Defense Security Certification and Accreditation Process for Information Technology, which is a DoD Instruction.

Also, I have a labeling policy that is being coordinated presently in formal Departmental review within the IAG and should be released shortly.

Response to Finding B: Initiatives are in place in consonance with the need to provide coordination and oversight regarding the management of multilevel Security initiatives and recommendations to "establish policies and procedures ... (for) the coordination of all DoD multilevel security initiatives ..." The MLS Working Group (WG) chartered under the IAG serves as the focal point with the Services and Agencies for the development of Departmental policy

and guidance governing the implementation and management of the integration and interoperability of users and systems - networks operating at various classification levels. The DISA, Information Program Management Office for Multilevel Security is the Vice-Chairperson overseeing the Department-wide MLS WG.

Lastly, the U.S. Air Force Integrated Maintenance Data System (IMDS) identified in your report is a program under the review by the Major Automated Information Systems Review Council that I chair. As such, the IMDS security plan is reviewed at program milestones throughout its development. IMDS will be scheduled for review during fourth quarter Fiscal Year 1997.

I agree with your findings that sufficient resources to adequately support the initiatives and responsibilities of the DoD MLS Program are fundamental to its success and support your recommendations that the appropriate level of resources be applied to the program.


Emmett Paige, Jr.

Audit Team Members

This report was prepared by the Intelligence Support Directorate, Office of the Assistant Inspector General for Policy and Oversight.

Charles M. Santoni
Lloyd O'Daniel
Lois J. Wozniak
Wilbur Broadus
Karen Bourgeois