DoD 5200.28-M

ADP SECURITY MANUAL

TECHNIQUES AND PROCEDURES
FOR
IMPLEMENTING, DEACTIVATING,
TESTING, AND EVALUATING
SECURE RESOURCE-SHARING ADP SYSTEMS

DEPARTMENT OF DEFENSE

JANUARY 1973

Administrative Reissuance Incorporating Change 1, June 1979

THE UNDER SECRETARY OF DEFENSE
WASHINGTON, D.C. 20301

24 MAY 1979
DoD 5200.28-M
DUSD(PR)

POLICY

FOREWORD

This publication, DoD 5200.28-M, "ADP Security Manual--Techniques and Procedures for Implementing, Deactivating, Testing, and Evaluating Secure Resource-Sharing ADP Systems," is issued under the authority of and in accordance with DoD Directive 5200.28, "Security Requirements for Automatic Data Processing (ADP) Systems." This manual is effective immediately and is applicable to all Department of Defense Departments and Agencies, the Organization of the Joint Chiefs of Staff, and the Unified and Specified Commands which process, use, store or generate classified information in resource-sharing ADP systems. This manual implements DoD Directives and Instructions and takes precedence over conflicting instructions. It establishes uniform guidelines for techniques and procedures to be used when implementing, deactivating, testing, or evaluating secure resource-sharing ADP systems and, when applicable, the components of such systems, without the necessity of further formal issuance by any DoD Component. The Heads of DoD Components may, however, augment this manual to meet their needs by prescribing more detailed guidelines and instructions provided they are consistent with this manual and DoD Directive 5200.28. One copy of each supplemental instruction issued by a Component shall be forwarded, immediately following publication, to the Deputy Under Secretary of Defense for Policy Review. This copy shall be appropriately marked to indicate the part(s) of the manual being augmented. Recommendations for revisions to this publication should be addressed through appropriate channels to the Deputy Under Secretary of Defense for Policy Review, Attention: Director for Security Plans and Programs.

Daniel J. Murphy
Admiral, USN (Ret)
Deputy

First amendment (June 25, 1979)

CONTENTS
SECTION I
PART 1
INTRODUCTION

PART 2
DEFINITIONS

SECTION II
PERSONNEL SECURITY
PART 1
CLEARANCE AND ACCESS CONTROLS

SECTION III
PHYSICAL, COMMUNICATIONS, AND EMANATIONS SECURITY
PART 1
PHYSICAL SECURITY OF AREAS

PART 2
PHYSICAL SECURITY OF EQUIPMENT

PART 3
COMMUNICATIONS SECURITY

PART 4
EMANATIONS SECURITY

SECTION IV
HARDWARE/SOFTWARE FEATURES
PART 1
GENERAL

PART 2
HARDWARE

PART 3
SOFTWARE

SECTION V
AUDIT LOG OR FILE

SECTION VI
BASIC SAFEGUARDS

SECTION VII
ERASE AND DECLASSIFICATION PROCEDURES
PART 1
INTRODUCTION

PART 2
ERASE PROCEDURES

PART 3
DISPOSITION APPROVAL

SECTION VIII
SPECIFICATIONS FOR MAGNETIC TAPE ERASE EQUIPMENT

SECTION IX
SECURITY TESTING AND EVALUATIONS (ST&E)
PART 1
GENERAL

PART 2
PROCEDURES

SECTION I

GENERAL PROVISIONS

PART 1

INTRODUCTION

1-100. Objective

The security of the United States depends in part upon the proper safeguarding of classified data processed, stored, and used in or classified information produced by ADP Systems. Safeguards applied to ADP Systems include all hardware/software functions, characteristics, and features; operational procedures, accountability procedures, and access controls at the central computer facility and remote computer and terminal facilities; and the management constraints physical structures and devices needed to provide an acceptable level of protection for classified material (data or information) contained in the computer system.

1-100.1. The objective of this Manual is to provide guidelines and establish techniques and procedures that can be used to:

1-100.1.1. Implement secure resource-sharing ADP Systems so that with reasonable dependability, deliberate or inadvertent access to classified material by unauthorized personnel or the unauthorized manipulation of the computer and its associated peripheral devices, which could lead to the compromise of classified information, can be prevented.

1-100.1.2. Develop, acquire, and establish methodologies, techniques, standards, and procedures for the design, analysis, testing, evaluation, and approval of the security features for resource-sharing ADP Systems;

1-100.1.3. Establish methodologies, techniques, and procedures for the physical protection of ADP Systems and components; and,

1-100.1.4. Prescribe standards criteria, and specifications for deactivating secure ADP Systems and the sanitization of system components for disposition or utilization in unsecured environments.

1-100.2. The potential scans by which a computer system can be adequately secured are virtually unlimited. The safeguards adapted must be consistent with available technology, the frequency of processing, the classification of the data handled or the information to be produced, the environment in which the ADP system operates, the degrees of risk that can be tolerated and other factors that may be unique to the installation involved. Rigid adherence to all techniques, methodologies, and requirements discussed in this Manual could adversely impact upon the present and future use of the system under today's rapidly changing ADP technology. This technology is dynamic and the methods chosen to secure a particular system must accommodate new developments without degrading the level of protection.

1-100.3. The techniques, methodologies, and procedures in this manual, however, represent an approved method of securing a remotely accessed resource-sharing computer system in a multilevel security mode as prescribed by DoD Directive 5200.28, "Security Requirements for Automatic Data Processing (ADF) Systems," December l8, 1972. It is understood that all of the techniques described in this Manual may not be economically justified after a cost versus risk evaluation. Therefore, selected subsets of the techniques included in this manual, with appropriate trade-offs, may be used to gain the level of security required for classification category, etc., to be secured. In addition, techniques not necessarily included in this Manual may be used so long as such methods provide the degree of security specified in DoD Directive 5200.28.

1-100.4. The techniques and procedures described in this Manual shall not be applied to ADP systems that cannot be retrofitted without excessive and unjustifiable costs or that can be dedicated and adequately secured for classified operations with reasonable administrative, personnel, physical and communication security controls.

1-101. Authority and Scope

1-101.1. This manual, authorized by the Secretary of Defense under the authority of the National Security Act of 1947, as amended, and E.O. 12065, is established as a DoD Manual published by the Deputy Under Secretary of Defense for Policy Review under the authority of DoD Directive 5200.1, dated November 29, 1978, DoD Regulation 5200.1-R, December 29, 1978, DoD Directive 5130.2, dated June 16, 1977, and DoD Directive 5200.28, dated December 18, 1972.

1-101.2. This Manual is applicable to the Office of the Secretary of Defense, all Department of Defense Departments and Agencies, the Organization of the Joint

Chiefs of Staff, and the Unified and Specified Commands, which process, use, or store classified data or produce classified information in resource-sharing ADP systems.

1-101.3. This Manual implements DoD Directives and Instructions and the security policies established by the Deputy Under Secretary of Defense for Policy Review and takes precedence over conflicting instructions. It establishes uniform guidelines for the techniques and procedures to be used when implementing, deactivating, testing, and evaluating secure resource-sharing ADP systems.

1-101.4. Recommendations for the clarification, revision, or amendment of this Manual should be addressed through channels to the Deputy Under Secretary of Defense for Policy Review, Attention: Director for Security Plans and Programs.

1-102. Responsibilities

1-102.1. The Deputy Under Secretary of Defense for Policy Review is designated to fulfill the responsibilities, in section 5.1., DoD Directive 5200.29, "Security Requirements for Automatic Data Processing (ADP) Systems," December 18, 1972, and to:

1-102.1.1. Approve all specialized security testing and evaluation (ST&E) tools and equipment validated for the joint usage of more than one Department of Defense Component or contractor;

1-102.1.2. Advise, assist, and assess progress of Department of Defense Components in the development and implementation of effective security testing and evaluation (ST&E) programs; and

1-102.1.3. Monitor administration of Component's ST&E programs.

1-102.2. Component's Designated Approving Authorities, or their designees for this purpose, in addition to the responsibilities assigned in paragraphs 5.3.1., 5.3.2., and 5.3.3., DoD Directive 5200.28, will ensure:

1-102.2.1. Issuance of instructions that fully explain the security requirements and operating procedures of each ADP System approved for the handling of classified material and the proper clearance and indoctrination, in applicable security requirements and responsibilities, of all personnel who install, operate, maintain, or use such systems.

1-102.2.2. Operation of each ADP System under the controls prescribed for the category(ies) of classified material contained in the system.

1-102.2.3. Where appropriate, the appointment of terminal area security officer(s) who will be responsible for performing applicable security functions at approved terminal areas that are an integral part of an ADP System that contains classified material.

1-102.2.4. Maintenance of documentation on operating systems (O/S) and all modifications thereto, and its retention for a sufficient period of time to enable tracing of security-related defects to their point of origin or inclusion in the system.

1-102.2.5. Supervision, monitoring, and testing, as appropriate, of changes in an approved ADP System that could affect the security features of the system, so that a secure system is maintained.

1-102.2.6. Establishment of procedures to discover recover, handle, and dispose of classified material improperly disclosed through system malfunction or personnel action.

1-102.2.7. Proper disposition and correction of security deficiencies in all approved ADP Systems and the effective use and disposition of system housekeeping or audit records, records of security violations or security-related system malfunctions, and records of tests of the security features of an ADP System.

1-102.2.8. Conduct of competent system ST&E, timely review of system ST&E reports, and correction of deficiencies needed to support conditional or final approval or disapproval of an ADP System for the processing of classified information.

1-102.2.9. Establishment, where appropriate, of a central ST&E coordination point for the maintenance of records of selected techniques, procedures, standards, and tests used in the testing and evaluation of security features of ADP Systems that may be suitable for validation and use by other Department of Defense Components.

1-102.2.10. Justification of information requirements under the provisions of DoD Directive 5000.19.

1-102.2.11. Notification to the Deputy Under Secretary of Defense for Policy Review of major ST&E plans, problems, and accomplishment, as appropriate.

1-103. Arrangement

This Manual is divided into sections, parts, and paragraphs. Each section is designated by subject and Roman numeral (e.g., I, II, III, etc.), and covers a separate aspect of implementing, deactivating, testing, and evaluating secure resource-sharing ADP System used to handle classified material. Each part is designated by title and Arabic numeral (e.g., 1., 2., 3., etc.), and contains a breakdown of the subjects covered by the section into related divisions. The paragraphs are further division of the parts. They are so numbered that the first digit indicates the section, the second digit, the part and the last two digits, the paragraph (e.g., 1-103. designates Section 1, Part 1, paragraph 3; 2-314. designates Section II, Part 3, paragraph 14). The Manual is designed to permit subsequent insertions of additional loose-leaf parts and paragraphs within the appropriate section without major reprint of the entire publication.

1-104. Amendments

This Manual will be amended from time to time and, unless otherwise specified in any amendment, the amendment will be effective upon publication.

1-105. Component Procedures

Components may augment this Manual to meet their needs by prescribing more detailed guidelines and instructions for their internal systems provided these instructions are consistent with this Manual and DoD Directive 5200.28. The application of these provisions will be guided by the twofold objective of establishing reasonable uniformity and maintaining maximum cost effective security consistent with the accomplishment by each Component of its assigned mission. One copy of each supplemental instruction issued by a Component shall be forwarded to the Deputy Under Secretary of Defense for Policy Review, Attention: Director for Security Plans and Programs immediately following publication. This copy shall be appropriately marked to indicate the part(s) of this Manual being augmented.

SECTION I

PART 2

DEFINITIONS

1-200. Access.

The ability and the means to approach, communicate with (input to or receive output from), or otherwise make use of any material or component in an ADP system. Personnel only receiving computer output products from the ADP system and not inputting to or otherwise interacting with the system (i.e., no "hands on" or other direct input or inquiry capability) are not considered to have ADP system access and are accordingly not subject to the personnel security requirements of this Manual and DoD Directive 5200.28. Such output products, however, shall either be reviewed prior to dissemination or otherwise determined to be properly identified as to content and classification (see paragraph 4.3.5.2., DoD Directive 5200.28).

1-201. Automatic Data Processing (ADP) System

An assembly of computer equipment, facilities, personnel, software, and procedures configured for the purpose of classifying, sorting, calculating, computing, summarizing, storing, and retrieving data and information with a minimum of human intervention. An ADP System as defined for purposes of this Manual is the totality of automatic data processing equipment (ADPE) and includes:

1-201.1. General and Special purpose computers (e.g., digital, analog, or hybrid computer equipment);

1-201.2. Commercially available components, those produced as a result of research and development, and the equivalent systems created from them, regardless of size, capacity, or price, which are utilized in the creation, collection, storage, processing, communication display, and dissemination of classified information;

1-201.3. Auxiliary or accessorial equipment, such as data communications terminals, source data automation recording equipment (e.g., optical character recognition equipment, paper tape typewriters, magnetic tape cartridge typewriters, and other data acquisition devices), data output equipment (e.g., digital platters and

computer output microfilmers), etc., to be used in support of digital, analog, or hybrid computer equipment, cable-connected, wire-connected, or self-standing;

1-201.4. Electrical accounting machines (EAM) used in conjunction with or independently of digital, analog, or hybrid computers; and

1-201.5. Computer equipment that supports or is integral to a weapons system.

1-202. ADP System Security

Includes all hardware/software functions, characteristics, and features; operational procedures, accountability procedures, and access controls at the central computer facility, remote computer and terminal facilities; and, the management constraints, physical structures, and devices; personnel and communication controls needed to provide an acceptable level of protection for classified material to be contained (see 1-208.) in the computer system.

1-203. Arrest

The discovery of user activity not necessary to the normal processing of data that might lead to a violation of system security and force termination of the activity.

1-204. Breach

The successful and repeatable defeat of security controls with or without an arrest (see 1-203.), which if carried to consummation, could result in a penetration (see 1-222.) of the system. Examples of breaches are:

1-204.1. Operation of user code in master mode;

1-204.2. Unauthorized acquisition of I.D. password or file access passwords; and

1-204.3. Accession to a file without using prescribed operating system mechanisms.

1-205. Briefing

Explanation by a test team of the techniques, procedures, and requirements for the testing and evaluation of a specific system.

1-206. Central Computer Facility

One or more computers with their peripheral and storage units, central processing units, and communications equipment in a single controlled area. This does not include remote computer facilities, peripheral devices, or terminals that are located outside the single controlled area even though they are connected to the Central Computer Facility by approved communication links.

1-207. Compartmented Intelligence

Includes only that intelligence material having special controls indicating restrictive handling for which system of compartmentation or handling are formally established.

1-208. Contained

"Contained" refers to a state of being within limits, as within system bounds, regardless of purpose or functions, and includes any state of storage, use, or processing.

1-209. Controlled Security Mode

1-209.1. An ADP system is operating in the controlled security mode when at least some users with access to the system have neither a security clearance nor a need-to-know for all classified material then contained in the ADP system. However, the separation and control of users and classified material on the basis, respectively, of security clearance and security classification are not essentially under operating system control as in the multilevel security mode.

1-209.2. This mode presents an alternative to encourage ingenuity in meeting the security requirements of this Directive in a manner less restrictive than the dedicated and system high security modes, but at a level of risk lower than that generally associated with the true multilevel security mode. This is accomplished by the implementation of explicit augmenting measures that reduce or remove a substantial measure of system software vulnerabilities together with specific limitation of the personnel security clearance levels of users permitted concurrent access to the system.

1-209.2.1. Examples of measures that augment or enhance the system by reducing or removing system software vulnerabilities and associated risk include the

employment of hardware or firmware (paragraph 1-215., below) that is alterable only at the Central Computer Facility for critical system security functions; employment of hardware/operating systems or system architectures that manifest reduced system software vulnerabilities and risk; interconnection of remote terminals via one-way hardware or firmware information communication wherein substantive information can only be transmitted in one direction (some circuits require two-way communication for certain control information in order to properly receive substantive information--these may be considered one-way circuits when it is determined that only control information can be transmitted in two directions); assignment of terminal security officers in remote terminal areas not protected as required for the highest classification category, most restrictive type(s) of material then being handled by the system where the terminal security officer has a security clearance for that highest level; system splitting via hardware or firmware alterable only at the Central Computer Facility; and/or limitation on user capabilities, such as restriction to fixed query access or the prohibition of user assembler and machine language programming.

1-209.2.2. Consideration shall also be given to limiting the number of personnel security clearance levels of users permitted concurrent access to the system to no more than three adjacent levels, including uncleared. For example, access shall be granted to uncleared users as well as users with Confidential and Secret security clearances or to users with Secret and Top Secret security clearances and formal access authorizations for additionally restrictive types of classified material. Certain such additionally restrictive types of classified material may place other limitations or requirements on the foregoing. See paragraph 1-225., below.

1-210. Debriefing

The test team oral exit report of its evaluation of the security features of the ADP system.

1-211. Dedicated Security Mode

An ADP system is operating in the dedicated security mode when the central computer facility and all of its connected peripheral devices and remote terminals are exclusively used and controlled by specific users or groups of users who have a security clearance and need-to-know for the processing of a particular category(ies) and type(s) of classified material.

1-212. Escort(s)

Escort(s) are duly designated personnel who have appropriate clearances and access authorizations for the material contained in the system and are sufficiently knowledgeable to understand the security implications of and to control the activities and access of the individual being escorted. (Such action is essential to the protection of classified material contained in the system and to the maintenance of the reliability of the security features (hardware or software) of the system.)

1-213. Evaluator(s)

Personnel specifically designated to participate in the test team review, analysis, testing, and evaluation of the security features of an ADP system.

1-214. Evaluation

The evaluator's report to the Designated Approving Authority describing the investigative and test procedures used in the analysis of the ADP system security features with a description and results of tests used to support or refute specific system weaknesses that would permit the acquisition of identifiable classified material from secure or protected data files.

1-215. Firmware

A method of organizing the ADP system's control hardware in a microprogrammed structure rather than as wired circuitry such that the method falls in neither the software nor the hardware subsystems. Microprograms are composed of microinstructions, normally implemented in read-only control storage, to directly control the sequencing of computer circuits at the detailed level of the single machine instruction. For the purposes of this Manual (see paragraph 1-209., above), the firmware or microprogramming handling security and related control functions shall be alterable only within the Central Computer Facility and only under conditions that are controlled by specifically designated personnel. It shall not be alterable by users or by software. Particular care and evaluation are accordingly required where writable control storage is employed in the microprogram control storage.

1-216. Intelligence

Intelligence is the product resulting from the collection, evaluation, analysis, integration, and interpretation of all information concerning one or more aspects of foreign countries or areas, which is immediately or potentially significant to the development and execution of plans, policies, and operations.

1-217. Investigation

The review and analysis of system security features (e.g., the investigation of system control programs using flow charts, assembly listings, and related documentation to determine the security provided by the operating system).

1-218. Material

"Material" refers to data processed, stored, or used in, and information produced by, an ADP system regardless of form or medium (e.g., programs, reports, data sets or files, records, and data elements).

1-219. Multilevel Security Mode

An operation under an operating system (supervisor or executive program) that permits various categories and types of classified materials to be concurrently stored and processed in an ADP system and permits selective access to such material concurrently by uncleared personnel (users) and users having differing security clearances and need-to-know. Separation of personnel and materiel on the basis of security clearance and need-to-know in accordingly accomplished by the operating system and associated system software. In a remotely accessed resource-sharing system, the material can be selectively accessed and manipulated from variously controlled terminals by personnel having different security clearances and access approvals. This mode of operation can accomodate the concurrent processing and storage of:

1-219.1. Two or more levels of classified data, or

1-219.2. One or more levels of classified data with unclassified data depending upon the constraints placed on the systems by the Designated Approving Authority (section 5.3., DoD Directive 5200.28).

1-220. Operating System (O/S)

An integrated collection of service routines for supervising the sequencing and processing of programs by a computer. Operating systems control the allocation of resources to users and their programs and play a central role in assuring the secure operation of a computer system. Operating systems may perform debugging, input-output, accounting, resource allocation, compilation, storage assignment tasks, and other system related functions (Synonymous with Monitor, Executive, Control Program, and Supervisor).

1-221. Orientation

The formal and informal presentations and discussions with the authority responsible for the ADP system that supplements the information in the initial security testing and evaluation (ST&E) request and provides the system evaluators an introduction to the operating environment, the techniques used to provide system security, the identity and location of documentation describing the implementation of system security measures (e.g., O/S modifications, etc.), and the techniques available to demonstrate the affectiveness of such measures in meeting requirements of DoD Directive 5200.28.

1-222. Penetration

The successful and repeatable extraction and identification of recognizable information from a protected data file or data set without any attendant arrests.

1-223. Resource-Sharing Computer System

A computer system that uses its resources, including input/output (I/O) devices, storage, central processor (arithmetic and logic units), control units, and software processing capabilities, to enable one or more users to manipulate data and process

co-resident programs in an apparently simultaneous manner. The term includes systems with one or more of the capabilities commonly referred to as time-sharing, multi-programming, multi-accessing, multi-processing, or concurrent processing.

1-224. Remotely Accessed Resource-Sharing Computer System

A computer system that includes one or more central processing units, peripheral devices, remote terminals, and communications equipment or interconnection links, which allocates its resources to one or more users, and that can be entered from terminals located outside the central computer facility.

1-225. Special Access Programs

Any programs imposing need-to-know or related security requirements or constraints that are beyond those normally provided for the protection of information classified in one of the three security classification designations (i.e., Confidential, Secret, or Top Secret) by DoD 5200.1-R. Such a program includes, but is not limited to, special clearance, adjudicative, or investigative requirements, special designation of officials authorized to determine need-to-know, or special lists or briefings of persons determined to have a need-to-know. SIOP-ESI is an example of a DoD Special Access Program. Other sources of additional access control or other pertinent security requirements, not generally applicable to the same security classification category within the Department of Defense, include:

1-225.1. The Atomic Energy Act of 1954;

1-225.2. Procedures based on international treaty requirements; and

1-225.3. Programs for the collection of foreign intelligence or under the jurisdiction of the National Foreign Intelligence Board or the U.S. Communications Security Board.

1-226. ST&E Tools and Equipment

Specialized techniques, procedures, criteria, standards, programs or equipment accepted by qualified security testing and evaluating (ST&E) personnel for uniform or standard use in testing and evaluating the secure features of ADP systems.

1-227. System High Security Mode

An ADP system is operating in the system high security mode when central computer facility and all of its connected peripheral devices and remote terminals are protected in accordance with the requirements for the highest classification category and type(s) of material then contained in the system. All personnel having ADP system access shall have a security clearance, but not necessarily a need-to-know for all ,material then contained in the system. In this mode, the design and operation of the ADP system must accordingly provide for the control of concurrently available classified material in the system on the basis of need-to-know.

1-228. Validation

That portion of the development of specialized ST&E, procedures, tools, and equipment needed to establish acceptance for joint usage by one or more DoD Components or their contractors. Such action will include, as necessary, final development, evaluation, and testing, leading to acceptance by senior ST&E staff specialists of the three Military Departments or a Defense Agency, and approval for joint usage by the Deputy Under Secretary of Defense for Policy Review.

1-229. Verification

The successful testing and documentation of actual on-line system penetration or attempts to penetrate the system in support or in contradiction of assumptions developed during system review and analysis that are to be included in the evaluation report.

SECTION II

PERSONNEL SECURITY

PART 1

CLEARANCE AND ACCESS CONTROLS

2-100. General

Personnel who develop, test (debug), maintain, or use programs that are classified or that will be used to access or develop classified material shall have a personnel security clearance and an access authorization (need-to-know), as appropriate for the highest classified and most restrictive category of classified material that they will access under system constraints. (Users without a security clearance but permitted concurrent system access shall be limited to Federal Government employees and military personnel).

2-101. Central Computer Facility

2-101.1. Unescorted entry to the Central Computer Facility or access to any of its ADP System components (hardware or software) shall be controlled and limited to personnel who are cleared for access to the highest classified and most restricted category of classified material contained in the ADP System, and whose need-to-know has been ascertained by the responsible ADP System security officer.

2-101.2. When the ADP system contains compartmented intelligence or SIOP-ESI, access shall be limited to personnel who, in addition to the above, have a TOP SECRET clearance and an access authorization, as appropriate, for the type(s) of material contained in the system. Except as specified in subsection 2-103., below, other persons whose access to the area is required on a one-time or infrequent basis and who will not have access to classified material or to the system's hardware or software, may be admitted to the area when accompanied by an escort (see 1-212.) who will be responsible for the visitor's activities while in the area.

2-102. Operation and Operating System (O/S) Programming Personnel

Personnel operating the system and controlling access to its entry points or those who design, develop, install, modify, service, or maintain the security features of the

software in the operating system (OIS) that controls user program access to the system (I/O, storage or use) or the key or combination by which the system is protected, shall be cleared and have access authorization as appropriate for the highest classified and most restrictive category of material contained in the system and shall be indoctrinated in appropriate security procedures for the particular ADP System and facility before assuming their duties. (Temporary or permanent modification of the O/S shall be tested by designated personnel to assure that the security features of the ADP system are effective. Audit trail records (see 5-100.) of these transactions shall be maintained.)

2-103. Maintenance Personnel

Personnel requiring access to any part or component of the ADP System (central or remote) that could affect or modify the secure operations of the system or permit access to classified data or information, shall have a security clearance and access authorization for the highest classified and most restrictive category of classified material contained in the system. Should it become necessary for uncleared maintenance personnel to have access to the ADP system, they shall be accompanied by an escort (see 1-212.) designated for that purpose.

SECTION III

PHYSICAL, COMMUNICATIONS, AND EMANATIONS SECURITY

PART 1

PHYSICAL SECURITY OF AREAS

3-100. General

Physical security considerations are essential elements in the planning, design, installation, utilization, and evaluation of all ADP Systems, facilities, and installations.

3-101. Central Computer Facility

3-101.1. Physical security requirements for the Central Computer Facility area will be commensurate with the highest classified and most restrictive category of information being handled in the ADP System.

3-101.2. If two or more computer systems are located in the same controlled area, the equipment comprising each system may be located so that direct personnel access, if appropriate, will be limited to a specific system.

3-102. Remote Terminal Areas

3-102.1. While the physical and personnel security requirements for the Central Computer Facility area are based upon the overall requirement of the total ADP System, remote terminal area requirements will be based upon the highest classified and most restrictive category and type of material that will be accessed through the terminal under system constraints.

3-102.2. Each remote terminal will be individually identified to ensure required security control and protection, with identification as a feature of hardware in combination with the operating system.

3-102.3. When a peripheral device or remote terminal, whether or not approved for the handling of classified material, is to be used by personnel of a Component that is not responsible for the overall operation and control of the ADP System. Such

security measures for the device or terminal and its area will be prescribed by the authority responsible for the security of the overall ADP System. Such security measures will be agreed to and implemented before the user's peripheral device or remote terminal may be connected to the ADP System.

3-102.4. When one or more DoD Components' ADP Systems become a part of a larger ADP network, the approval and the authority to authorize temporary exceptions to security measures for the Components ADP System in the network will require the concurrence and approval of both the DoD Component operating the ADIP System and the DoD Component having overall responsibility for the security of the network (see 3-301.).

3-103. Disconnect Procedures

3-103.1. Each remote terminal that is not controlled and protected as required for material accessible through it will be disconnected from the ADP System when the system contains classified information.

3-103.2. Disconnect procedures, when required to protect classified materiel contained in the ADP System, will be used to disconnect remote I/O terminals and peripheral devices from the system by a hardware or software method authorized by the Designated Approving Authority.

3-104. Supplemental Requirements

When compartmented intelligence or SIOP-ESI is to be handled in the ADF System, the supplemental physical security control required by sections 4.12. and 4.13. of DoD Directive 5200.28, will apply to the central computer facility area, and all areas having remote terminals connected to the system.

3-105. Adjustment of Area Controls

3-105.1. When appropriate, provision will be made to permit adjustment of area controls to the level of protection required for the category or type of material actually being handled in the computer peripheral devices, and terminals, except that the Central Computer Facility and those components approved for the storage and processing of classified material, will not be downgraded below the level required to protect secure communications equipment, to maintain the reliability and security of

the ADP System, and to protect essential hardware or software components of the ADP System.

3-105.2. If the minimum measures for the Central Computer Facility, or ADP System are suspended or discontinued for any reason, the security features of the system will be re-evaluated, as would any new system or component before again being approved for the processing of classified material.

SECTION III

PART 2

PHYSICAL SECURITY OF EQUIPMENT

3-200. General

While procedural or specialized techniques to be applied by Components, have, in the past, been largely left to their discretion, it is contemplated that as specialized techniques are developed and tested they will be published either in this Manual or its associated newsletter.

3-201. Equipment Application

Countermeasures to physical security hazards such as fire, natural disaster, sabotage, and environmental problems (e.g., power failures) are also being prepared for coordination, approval, and publication in this section of the Manual.

SECTION III

PART 3

COMMUNICATIONS SECURITY

3-300. Communication Links

Transmission and communication lines and links that provide secure communication between components of or to an ADP System will be secured in a manner appropriate for the material designated for transmission through such lines or links under the provisions of DoD Directive C-5200.5, DoD Directive 5200.1, and DoD Regulation 5200.1-R. Telecommunications facilities supporting ADP Systems will meet the security criteria used for Defense communications systems under DoD Directive 4630.1.

3-301. Interface with Communications Networks

The DoD Component that operates an ADP System that requires only communication support from telecommunications networks such as AUTODIN will determine the security requirements for of classified material in its ADP System. The security measures to be agreed to and implemented before connection with the communication network are limited to those needed to insure the development, interface, and integration of securer reliable survivable, and cost-effective transmission and communication lines and links that are needed to meet the communication requirements of the telecommunications network supporting the ADP System.

3-302. Storage and Forward Message Switches

Information in this section will be added following further coordination and approval.

3-303. Multiplexers

Information in this section will be added following further coordination and approval.

SECTION III

PART 4

EMANATIONS SECURITY

3-400. Emanations Control

Measures to control compromising emanations are subject to approval under the provisions of DoD Directive S-5200.19, by the cognizant authority of the Component approving the security features of the ADP system.

SECTION IV

HARDWARE/SOFTWARE FEATURES

PART 1

GENERAL

4-100. Application

A combination of hardware and software features are essential to provide protection for material stored or processed in the secure resource-sharing ADP System. While all of the following features may not be available in the current hardware or software combination thereof, they shall be provided at the earliest date that the state-of-the-art permits. The available hardware/software features outlined below should operate unabridged whenever classified material is contained in the resource-sharing ADP System and measures shall be implemented to provide special controls over the access to or modification of such features. Where possible and practicable, such features should contain two or more independent controls that would have to malfunction simultaneously for a breach of system security to occur.

SECTION IV

PART 2

HARDWARE

4-200. Hardware Features

4-200.1. The execution sate of a processor should include one or more variables, i.e., "protection state variables," which determine the interpretation of instructions executed by the processor. For example, a Processor might have a master mode/user mode protection state variable, in which certain instructions are illegal except in master mode. Modification of the protection state variables shall be so constrained by the operating system and hardware, that a user cannot access information for which he has no authorization.

4-200.2. The ability of a processor to access locations in memory (hereinafter to include primary and auxiliary memory) should be controlled (e.g., in user mode, a memory access control register might allow access only to memory locations allocated to the user by the O/S).

4-200.3. The operation of certain instructions should depend on the protection state of the processor. For example, instructions that perform input or output operations would execute only when in master mode. Any attempt to execute an instruction that is not authorized should result in a hardware interrupt that will permit the O/S to interrupt and/or abort the program containing the illegal instruction.

4-200.4. All possible operation codes, with all possible tags or modifiers, whether legal or not, should produce known responses by the computer.

4-200.5. All registers should be capable of protecting their contents by error detection or redundancy checks. These include those that set protection state variables, control input or output operations, execute instructions, or that are otherwise fundamental to the secure operation of the hardware.

4-200.6. Any register that can be loaded by the operating system should also be storable, so as to permit the O/S to check its current contents against its presumed contents. (The term "register" as used in 4-200.5. and 4-200.6., refers primarily to index or general purpose registers rather than an isolated address of a single storage location within the computer.)

4-200.7. Error detection should be performed on each fetch cycle of an instruction and its operant (e.g., parity check and address bounds check).

4-200.8. Error detection (e.g., parity checks) and memory bounds checking should be performed on transfers of data between memory and storage devices or terminals.

4-200.9. Automatic programmed interrupt should function to control system and operator malfunction.

4-200.10. The identity of remote terminals for input or output should be a feature of hardware in combination with the operating system.

4-200.11. Read, write, and execute access rights of the user should be verified on each fetch cycle of an instruction and its operant.

SECTION IV

PART 3

SOFTWARE

4-300. General

The user and master modes of ADP Systems operation shall be separated so that a program operating in a user mode is prevented from performing control functions. As much of the operating system (O/S) as possible should run in the user mode (as opposed to the master mode) and each part of the O/S should have only as much freedom of the computer as it needs to do its job.

4-301. O/S Controls

The O/S shall contain controls that provide the user with all material to which he is authorized access, but no more. If such controls are not feasible, output material shall be generated only within the Central Computer Facility under the cognizance of the ADP System security officer. As a minimum, the O/S must control:

4-301.1. All transfers of material between memory and on-line storage devices; between the Central Computer Facility equipment and any remote device; or between on-line storage devices; and

4-301.2. All operations associated with allocating ADP System resources (e.g., memory, peripheral devices, etc.) memory protection, system interrupt, and shifting between user and master protection modes; and

4-301.3. Access to programs and utilities that are authorized to perform the various categories of maintenance (e.g., as operations that affect authorized additions, deletions, or changes to data) on the operating system, including any of its elements and files. Such controls shall insure that access is limited to personnel authorized to perform particular categories of maintenance; and

4-301.4. All other programs (user programs) so that access to material is made via an access control and identification system that associates the user and his terminal, in the ADP System with the material being accessed.

4-302. Test and Debugging Programs

User application programs, and systems programs that do not violate the security or integrity of the ADP System may be debugged during system operation, provided that such activity is limited to the user mode. All other system software development, experimentation, testing, and debugging shall be performed on a system temporarily dedicated for these purposes.

4-303. Clear System Procedures

Procedures shall be available for clearing from the system, or making inaccessible, all classified material during operations without the required protection.

4-304. Shutdown and Restart

The O/S must provide for security safeguards to cover unscheduled system shutdown (aborts) and subsequent restart, as well as for scheduled system shutdown and operational start-up.

4-305. Other Fundamental Features

The following features of the operating system (O/S) are also considered fundamental to the secure operation of an ADP System. Unauthorized attempts to change, circumvent, or otherwise violate these features should be detectable and reported within a known time by the operating system causing an abort or suspension of the responsible user activity. In addition, the incident shall be recorded in the audit log, and the ADP System security officer notified.

4-305.1. Memory/Storage Protection - The operating system shall protect the security of the ADP System by controlling:

4-305.1.1. Resource allocation (including primary and auxiliary memory);

4-305.1.2. Memory access outside of assigned areas; and

4-305.1.3. The execution of master (supervisory) mode instructions that could adversely affect the security of the O/S.

4-305.2. Memory Residue - The O/S shall ensure that classified material or critical elements of the system do not remain as accessible residue in memory or on on-line storage devices.

4-305.3. Access Controls - Access to material stored within the ADP system shall be controlled by the ADP System security officer, as required by cognizant authority, or by automatic processes operating under separate and specific controls within the O/S established through hardware, software, and procedural safeguards approved by the ADP System security officer.

4-305.4. Security Labels - All classified material accessible by or within the ADF System shall be identified as to its security classification and access or dissemination limitations, and all output of the ADP System shall be appropriately marked.

4-305.5. Terminal Identification - Manual and administrative procedures and/or appropriate hardware/software measures shall be established to assure that the terminal from which personnel are attempting to access classified material has been protected and is authorized such access. Where a terminal identifier is used, for this purpose, it shall be maintained in a protected file.

4-305.6. User Identification - Where needed to assure control of access and individual accountability, each user or specific group of users shall be identified to the ADP System by appropriate administrative or hardware/software measures. Such identification measurers must be in sufficient detail to enable the ADP System to provide the user only that material that he is authorized.

SECTION V

AUDIT LOG OR FILE

5-100. Application

An audit log or file (manual, machine, or a combination of both) shall be maintained as a history of the use of the ADP System to permit a regular security review of system activity. (For example, the log should record security related transactions, including each access to a classified file and the nature of the access, e.g., logins, production of accountable classified outputs, and creation of now classified files. Each classified file successfully accessed regardless of the number of individual references during each "job" or "interactive session" should also be recorded in the audit log. Much of the material in this log may also be required to assure that the system preserves information entrusted to it.)

SECTION VI

BASIC SAFEGUARDS

6-100. Application

Procedures and basic safeguards prescribed in DoD Directive 5200.1. and DoD Regulation 5200.1-R for the transmission, processing, handling, storage, and disposal of classified material apply to the material removed from the custody of the system. Further, when located outside of the Central Computer Facility or its approved remote terminal areas all disk packs, tapes, etc., used to store classified material shall be protected and stored as appropriate for the classification of the highest category of material ever recorded thereon until declassified (see section VII).

SECTION VII

ERASE AND DECLASSIFICATION PROCEDURES

PART 1

INTRODUCTION

7-100. General

The following procedures and specifications result from extensive research, investigation, and practice. They are adequate to the extent of such research and investigation, but, do not necessarily represent the ultimate status to be reached in this aspect of computer security. It is, therefore, anticipated that they will be improved through continued testing, evaluation, and usage by DoD Components.

7-101. During Operations

During normal operations in a controlled environment each memory location used for the storage of classified data shall be overwritten when it in no longer required, before reutilization, or before the content of the location may be read to preclude the unauthorized disclosure of classified data. Hardware/software techniques may be used to accomplish this task. When any of the memory units or storage media are removed from the controlled environment, the procedures in Section VII, Part 2, below, shall apply.

SECTION VII

PART 2

ERASE PROCEDURES

7-200. General

7-200.1. Safeguarding classified information in a computer or computer system requires special precautions because of the types of storage media and devices (magnetic drums, disks, disk packs, and tapes) used to store, record, or manipulate data that must be protected by appropriate classification and security controls until procedures below are carried out.

7-200.2. Declassification - The eventual temporary or outright release of the storage device or a system including storage media should be anticipated. Procedures to be used to release or deploy the storage media outside the controlled environment are set forth in the following sections.

7-201. Magnetic Tapes

Tapes used to store magnetically recorded digital data may be declassified by erasing with bulk tape degaussers that have been tested and approved by a laboratory of a Department of Defense Component or a commercial testing laboratory, where such tests may be certified, by adhering to test methods and performance criteria in technical specifications promulgated in Section VIII. Elements of DoD Components may, where necessary, develop procurement specifications for their use, provided the test methods and performance criteria comply, as a minimum, with the specifications in Section VIII.

7-202. Magnetic Disks, Disk Packs, Drums, and other Similar Rigid Magnetic Storage Devices

The equipment shall be checked immediately prior to beginning the overwrite procedure to insure that malfunctions do not occur that will prevent the classified information from being effectively overwritten. Further, when the capability exists, as an integral part of the storage subsystem, an AC/DC erase will be applied to all data tracks before the tracks are overwritten and the overwrite verified. Thereafter, all

storage locations will be overwritten a minimum of three times, once with the binary digit "1," once with the binary digit "0," and once with a single numeric, alphabetic, or special character. Such alpha-numeric or other unclassified data shall be left on the device. The current used in overwriting must be equal to that used in recording the information, but of a strength that will not damage or impair the equipment.

7-203. Inoperative Magnetic Disks, Disk Packs, Drums, and Similar Rigid Storage Devices

If the storage device has failed in such a manner that it cannot be overwritten the device may be declassified by exposing the recording surface(s) to a permanent magnet having a field strength at the recording surface of at least 1,500 OERSTED. Care must be taken to insure that entire surface is wiped at least three times, by a non-uniform motion of the magnet. Care must be taken to assure that all tracks are covered by the center of the magnet. A thin sheet of clear plastic (a 1-5 mil sheet) should be used to prevent damage to the recording surface(s).

7-204. Internal Memory

Internal memory (e.g., core) may be declassified by alternately setting each addressable memory location alternately to all "ones" and all "zeros" for 1000 cycles until the state is changed at least 999 times. Detailed memory erase or clearing programs or routines should be prepared by qualified ADP programmers and approved by the ADP Systems security officer.

7-205. Magnetic Storage Media Used to Store Analog, Video, or Similar Non-Digital Information

Magnetic tape used to record analog, video, or similar types of non-digital information may be declassified by degaussing as in 7-201., above. Rigid magnetic storage surfaces may be declassified as in 7-202., above, except that the unclassified overwriting signal must be analog instead of binary with the latter recording left intact on the device. In the case of a failure of the degauseer or overwriting methods, a permanent magnet may be used as in 7-203., above, for rigid recording surfaces.

SECTION VII

PART 3

DISPOSITION APPROVAL

7-300. General

With the specific approval in each case of the Designated Approving Authority, or designee for this purpose, within the DoD Component that is responsible for the security features of the ADP system, storage media treated as above in Part 2, may be handled as unclassified and released as necessary.

7-301. Records

A record of the above operations shall be maintained for a period of 2 years after disposition of the device or equipment.

7-302. Specific Guidance

7-302.1. Guidance for eradication of magnetic media not covered above may be obtained by submission of all pertinent details to the Deputy Under Secretary of Defense for Policy Review, Attention: Director for Security Plans and Programs, for consideration on a case-by-case basis.

7-302.2. In the absence of eradication by approved equipment or procedures, or at the direction of the Designated Approving Authority, or designee, magnetic information storage media shall be safeguarded in the manner prescribed for the highest classification ever recorded thereon until it is destroyed.

SECTION VIII

SPECIFICATIONS FOR MAGNETIC TAPE ERASE EQUIPMENT

8-300. Magnetic Tape Degausser Specifications

This specification covers any equipment to be used for automatic bulk degaussing of recorded magnetic tape. It describes in general the desired configuration and sets forth desired electrical and magnetic performance.

8-301. Requirements

8-301.1. General

8-301.1.1. Reel Size. The equipment shall be designed to degauss magnetic tape in widths from 1 to 2 inches, wound on reels from 3 to 15 inches in diameter, with the provision for conversion to either 5/16-inch hubs or computer reel hub dimensions. It will be permissible to turn over 2-inch reels for degaussing.

8-301.1.2. Installation. The equipment shall be designed such that either rackmounting or bench top operation can be accommodated with minimum modification.

8-301.1.3. Operation. Operation shall be automatic once the reel is loaded and the degaussing cycle is initiated, except for 2-inch wide tape that may be cycled twice. The degaussing operation shall not require more than two minutes per reel.

8-301.1.4. Degaussing Safeguard. A method of monitoring the relative current in the degaussing coils shall be provided.

8-301.1.5. Safeguard Tape Unwinding. For vertically mounted degaussers, a method of reversing the direction of reel rotation while cycling shall be provided. This reversal of reel direction must not interrupt the degausaing cycle. This safeguard prevents the unwinding of tape while cycling.

8-301.2. Detailed Requirements

8-301.2.1. Electrical Power. The equipment must meet all requirements over the following parameter ranges:

8-301.2.1.1. Input Voltage Range - 95 to 135 VAC, single phase, three-wire system.

8-301.2.1.2. Line Frequency Range - 48 to 62 cycles per second.

8-301.2.1.3. Power - The current drain shall be less than 20 amperes for any of the foregoing conditions of line frequency and voltage.

8-301.3. Mechanical

8-301.3.1. Cabinet. The equipment shall be designed for mounting in a standard 19-inch rack and shall have minimum height and weight according to the design requirements.

8-301.3.2. Finish. Surfaces shall be adequately protected against corrosion within the environments detailed under section 8-301.4., below.

8-301.4. Environmental Performance. The equipment shall perform to specification when operated in the environments listed in the following paragraphs:

8-301.4.1. Altitude. Non-operating: sea level to 50,000 feet
Operating: sea level to 10,000 feet

8-301.4.2. Relative Humidity. Operating and non-operating: 5 to 100 percent, no condensation. However, the equipment shall survive condensation after being dried out.

8-301.4.3. Temperature. Non-operating: -40°C to 71°C
Operating: 0°C to +55°C

8-301.4.4. Vibration and Shock. Non-operating. The equipment shall survive specified test methods that are intended to simulate shock and vibration levels expected in commercial shipping and handling.

8-301.5. Performance

8-301.5.1. Degausssing Level. The residual signal level after minimum of 90 db below saturated signal degaussing shall be a level for tape widths of 1 inch or less.

8-301.5.2. Duty Cycle. Design shall be such that continuous operation, i.e., a duty cycle of 100 percent may be used. Under conditions of continuous operation, the temperature rise at the reel face of the equipment shall not exceed 35°F above ambient.

8-302. Test Procedure

8-302.1. Equipment

8-302.1.1. Recorder reproducer with full-track 1/4-inch heads.

8-302.1.2. Audio oscillator.

8-302.1.3. Wave analyzer with 20-ops bandwidth.

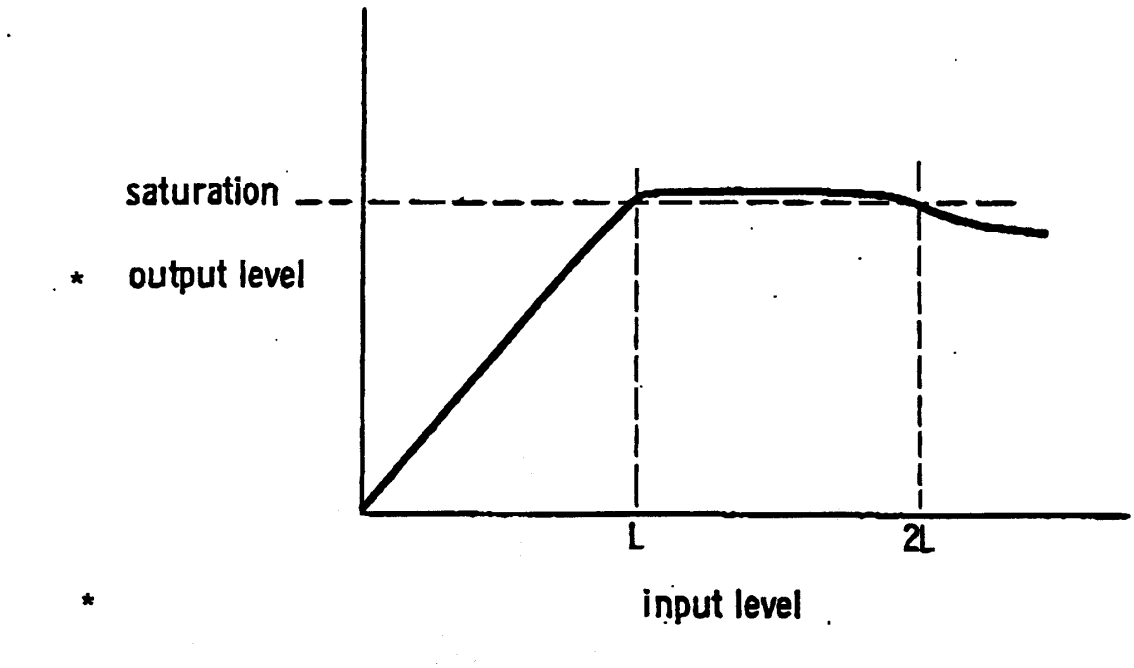
8-302.1.4. Oscilloscope.

8-302.2. Procedure

8-302.2.1. Record. Record tapes with a 400-ops signal at 7' ips with the record level set for saturation. Measure the playback signal level using the wave analyzer on the 20-ops bandwidth position and the recorder playback gain set at maximum. This is the reproduce reference level.

NOTE: The saturation point shall be defined by the tape transfer curve as the output level for which it levels L and 2L produce the same output (see figure number 1).

Figure 1



8-302.2.2. Degaussing. Degauss the tapes.

NOTE: To evaluate the ability to degauss wider tape widths two, three, and four 1/4-inch reels can be taped together for the degaussing procedure. To simulate the larger diameter reels a special 15-inch X 1/4-inch reel would have to be used. This can be constructed by interchanging a standard 1/4-inch hub and 15-inch flanges.

8-302.2.3. Playback. Playback the degaussed tapes with the playback gain set at maximum. Tune the wave analyzer (20-ops bandwidth) to measure any residual signal level.

NOTE: Clean and degauss tape recorder threading path before each pass.

SECTION IX

SECURITY TESTING AND EVALUATION (ST&E)

PART 1

GENERAL

9-100. Purpose

9-100.1. To develop and acquire methodologies, techniques, and standards for the analysis, testing, and evaluation of the security features of ADP Systems.

9-100.2. To assist in the analysis, testing, and evaluation of the security features of ADP Systems by developing facts (for the Designated Approving Authority) concerning the effectiveness of measures used to secure the ADP System in accordance with section 6. of DoD Directive 5200.28 and the provisions of this Manual. (See sections II, III, and IV.)

9-100.3. To minimize duplication and overlapping of effort, improve the effectiveness and economy of security operations, and provide for the approval and joint usage of ST&E tools and equipment.

SECTION IX

PART 2

PROCEDURES

9-200. Procedures

The procedures and other portions of this section will be published following additional testing and coordination.