

28 Feb 97

DEVELOPMENT OF POLICIES FOR ACCESS TO DATA AND OTHER ADP RESOURCES
(Supplementation is prohibited.)

A. REFERENCES.

1. DoD 5200.2-R, Personnel Security Program, Appendix K, ADP Position Categories for Designating Positions.
2. DLAR 5200.17, Security Requirements for Automated Information and Telecommunications Systems.
3. DRMS Directive 5210.4, Appointment of Functional Data Owners and System Resources Owners.

B. PURPOSE. This directive establishes guidelines and assigns responsibilities for compiling and publishing access policies.

C. APPLICABILITY AND SCOPE. This directive applies to all personnel who have been appointed as Functional Data Owners or System Resources Owners, or other personnel who are vested with the authority to approve access requests within an ADP environment. The policy statements and the responsibilities as presented in this directive are in consonance with the personnel requirements of the DoD 5200.2-R, Appendix K (reference A1), the security requirements of the DLAR 5200.17 (reference A2), and the directive for appointing data/resources owners (reference A3). The scope of coverage includes HQ DRMS, the directorates of Operations East and West, Europe, the International Sales Office (ISO), and all DRMOs.

D. DEFINITIONS.

1. AUTOMATED INFORMATION SYSTEM (AIS): An assembly of computer hardware, software, and/or firmware configured to collect, create, communicate, compute, disseminate, process, store, and/or control data or information. Networks are considered to be AIS also.
2. AUTOMATED INFORMATION SYSTEM SECURITY OFFICER (AISSO). The focal point for information concerning the secure design and development of an AIS. This individual, in coordination with the Data Owners/System Resource Owners, determines the security controls needed to protect the information being processed. The AISSO conducts the security requirements analysis for an AIS prior to development, supports the ISSO's testing and evaluation effort, and documents the results in the supporting documentation for AIS accreditation.
3. COMPARTMENT: An isolation of the operating system, user programs, and data files from one another to protect against unauthorized or concurrent access by other users or programs, and the breaking down of sensitive data into small isolated blocks for the purpose of reducing risk to the data.
4. DATA ACCESS POLICY: The statements by the data owners regarding who may have access to certain kinds of data and what level of privileges users are allowed to have.

5. DATA OWNER (also RESOURCES OWNER): The individual(s) responsible for approving access requests and making decisions about the protection and use of sensitive information and resources. Data owners and resources owners are the personnel responsible for the business functions supported by the AISs.

6. DESIGNATED APPROVING AUTHORITY (DAA): The agency/activity focal point with the authority to grant AIS accreditation and security software certification, and to accept whatever minimal or residual risk may be left after the implementation of security countermeasures.

7. INFORMATION SYSTEM SECURITY OFFICER (ISSO): The agency/activity focal point for computer security matters. In his/her operational capacity, the ISSO implements the provisions of DLAR 5200.17 and develops local security procedures for administering the activity computer security program. The ISSO oversees user account administration, manages the TASO program, and reports possible security violations.

8. INFORMATION SYSTEM SECURITY MANAGER (ISSM): The agency/activity focal point for advising the DAA on AIS security matters. In his/her operational capacity, the ISSM assists in establishing, implementing, and reviewing AIS security programs. The ISSM makes recommendations, maintains liaison and cooperation with other organizations, and assures compliance with security policies.

9. LEAST PRIVILEGE. A security requirement that states users shall have access to the information and functions to which they are entitled (e.g., need-to-know), and nothing more. Access requirements are to be defined in the data owner's policy.

10. NEED-TO-KNOW. The necessity for access to, knowledge of, or possession of specific information required to carry out official duties.

11. PRIVILEGE: A permission for a user to take various actions against data and other resources within the ADP environment.

12. POSITION SENSITIVITY: The term used to indicate that various ADP positions have specific criteria relative to performing different kinds of ADP duties. ADP positions are divided into three sensitivity categories (see enclosure 2).

13. SENSITIVE UNCLASSIFIED DATA: Any information the loss, misuse, or unauthorized access to or modification of which could adversely affect U.S. national interests, the conduct of Federal programs, or the privacy to which individuals are entitled under the privacy Act.

14. SYSTEM MONITOR: The focal point for establishing and managing user access accounts at the DRMOs. The System Monitors also have a variety of other duties to perform.

E. POLICY.

1. Access policies must be developed in accordance with enclosure (1), and must be published and distributed.

2. Access policies are the Functional Data Owner's and the System Resources owner's vehicle for setting forth rules of access. The rules comprise the owner's access requirements. The rules also support the Principle of Least Privilege.

3. Access policies identify the owners and provide information about the owners.
4. Access policies define users. User identification can be very specific, or can be broad in scope depending on the data owners' and resources owners' views for controlling user access. Identifying the defining users and user groups can be by any manner meaningful to the owners (example: job title or position; job function; location of users (from a general geographic area to a specific location); general reference to an organization, business, or activity; specific name of an organization, business, or activity; using combinations of different identification means).
5. Access policies identify position sensitivity requirements associated with the accesses (refer to enclosures 1 and 2).
6. Access policies list specific kinds of data or resources and identify whether the data or resource is designated as sensitive or nonsensitive (refer to enclosures 2 and 3). If the access policy addresses sensitive data, then the DLA Sensitivity Category is also designated (refer to enclosure 1, page 1-8).
7. Access policies declare privileges (refer to enclosure 4).
8. Access policies cite the systems, applications, or compartments where data or resources are located.
9. Access policies provide a matrix which summarizes users, user privileges, data elements, and data sensitivity (see enclosure 1, page 1-5).
10. Access policies are not compelled to take into account:
 - a. The ADP solutions implemented to meet processing requirements.
 - b. System and application processing exceptions.
 - c. Telecommunications and ADP technical considerations.
11. Owner's access rules are applicable in all instances and are universal regardless of where access to data or resources originates from. The processing within programs, applications, compartments, and systems cannot require or mandate changes to user accesses and privileges established by the owners.
12. Access policies must be updated or amended when new access rules are added and when current rules are revised or deleted. Changes may be published as revisions to the original access policy.
13. Upon publication and distribution of access policies (and any subsequent revisions), requests for access will no longer be automatically sent to the owners for approval. The step of initially sending all requests to owners will be eliminated. Requests will be sent to personnel responsible for establishing access capabilities (e.g., System Monitors, ISSOs). Requests will only be forwarded to owners for review when they fall outside the guidance of the policies. NOTE: In reference A3, the personnel responsible for establishing access capabilities are referred to as Access Account Administrators.
14. The owner retains the original access policy and the originals of any subsequent revisions. Copies of the original document (and any revisions) are forwarded to:
 - a. Management in the owner's chain of command.

- b. The organization responsible for establishing user access capabilities and privileges.
- c. The organization responsible for maintaining/operating the systems/applications.
- d. The agency/activity ISSM.

F. RESPONSIBILITIES.

1. Data owners and resources owners will:

- a. Compile access policies in accordance with enclosure 1, and follow guidance presented in enclosures 2, 3, and 4.
- b. Compose revisions when policy changes are made.
- c. Produce as many copies of access policies and revisions as are needed, and distribute copies to appropriate personnel and organizations (see paragraph E13.).
- d. Review requests for approval/disapproval when:
 - (1) The user does not fit a policy's defined users or user groups.
 - (2) The privileges requested exceed or fall outside the privileges declared for specific users and user groups.
 - (3) Position sensitivity does not match the policy's requirements.
 - (4) Requests for access to data/resources which do not appear to fit any of the policy's entries.

2. Automated Information System Security Officers (AISSOs) will assist the data owners/resources owners in the development of access policies.

3. System Monitors/ISSOs will:

- a. Review requests to assure accesses and privileges fall within the data owners and resources owners guidelines as portrayed in the published policies.
- b. Forward requests to the owners when the accesses/privileges/position sensitivity fall outside the framework or scope of the published access policies.
- c. Establish user capabilities for requests that fall within policy guidelines or when requests forwarded to the owners have been approved and returned by the owners.

G. EFFECTIVE DATE AND IMPLEMENTATION. This publication is effective and shall be implemented upon distribution.

H. INFORMATION REQUIREMENTS. (Reserved for future use.)

BY ORDER OF THE COMMANDER

4 Encl	/s/
1. Guidance for Development of Access Policy.	DOUGLAS W. YOUNG
2. DoD 5200.2-R, Appendix K, ADP Position Categories.	LCDR, SC, USNR
3. List of Sensitive Unclassified Data.	Executive Officer
4. Guidance for describing User Privileges.	

Coordination: All HQ DRMS Directors, East/West Operations Deputy Commander, Europe Region Commander.

GUIDANCE FOR DEVELOPMENT OF ACCESS POLICY

1. THE POLICY DOCUMENT. Policies are composed of a title page and two main sections. SECTION I is administrative information. SECTION II comprises the access rules and contains the details about privileges, users, and resources. SECTION II has two parts; the first part (ACCESS INFORMATION) is a detailed presentation of the access rules, and the second part (ACCESS MATRIX) summarizes the rules from the first part as a quick reference. The owner may include an introductory/overview write-up between the title page and SECTION I (see the example on page 1-2). Also, at the owner's discretion, definitions and/or references and/or enclosures may be added, and the owner may want to put examples and illustrations in the policy.

2. THE TITLE PAGE. A title page may be brief, such as the following example:

DATA ACCESS POLICY
FOR
AUTOMATED USERCODE REQUEST APPLICATION
(AURA)

3. THE INTRODUCTORY/OVERVIEW PAGE. The inclusion of an introductory/overview page and its contents are at the owner's discretion. The following is an example of what the page might consist of or look like:

INTRODUCTION:

The following Data Access Policy is established to provide guidelines and assignments for the responsibility of maintaining consonance with the security requirements of the DLAR 5200.17. User access will be permitted when a request provides justification showing the access is needed to perform work-related duties and assignments.

OVERVIEW:

The Automated Usercode Request Application (AURA) is designed to help people gain access to any of the computer systems in Defense Reutilization & Marketing Service (DRMS) quickly and conveniently. It reduces paper handling, improves security control, and makes it easier for the people who administer the computer systems to collect the information they need.

AURA is a centralized UNIX based application. It is used primarily by ADP Security (DRMS-IZ) and designated Terminal Area Security Officers (TASOs) to communicate access needs in an increasingly complex data processing environment. The system relies heavily on the UNIX mail facility to transmit request forms for individual computer systems.

1-2

4. THE SECTION I PAGE(S). The format for Section I is as follows:

SECTION I
ADMINISTRATIVE INFORMATION

PRIMARY OWNER: LOGON ID:
TELEPHONE NUMBER: OFFICE SYMBOL:
MAILING ADDRESS:
E-MAIL ADDRESS:
PRIMARY OWNER SIGNATURE: DATE:

ALTERNATE: LOGON ID:
TELEPHONE NUMBER: OFFICE SYMBOL:
MAILING ADDRESS:
E-MAIL ADDRESS:
ALTERNATE OWNER SIGNATURE: DATE:

NOTE: If more than one alternate has been appointed, the 'ALTERNATE' information is re-entered for as many alternates as there are.

1-3

5. THE SECTION II PAGES. The following illustrations on this page and page 1-5 show the format and provide examples of SECTION II entries. Guidance and instructions for composing SECTION II are on pages 1-6 through 1-8. Read the guidance before starting SECTION II.

SECTION II

ACCESS INFORMATION

A. SYSTEM/APPLICATION:

Automated Usercode Request Application (AURA)

B. DATA ELEMENTS/AGGREGATES/FORMS/FILES (OR OTHER RESOURCES) AND SENSITIVITY DESIGNATION (IF DATA):

DRMS Field Cost DBMS Options File

Sensitive (5)

Mode Panel - Input Screen Description (Add/Delete/Modify User Information)
nonsensitive

System Selection Panel (System Selection Screen Description)
nonsensitive

AURA Systems File (/USERS/CONTRDEV/AURA/RELEASE/SYSTEMS)
nonsensitive

AURA TASO File (/USERS/CONTRDEV/AURA/RELEASE/TASOS)
nonsensitive

C. AUTHORIZED USERS/USER GROUPS:

DLA Terminal Area Security Officers (TASOs)

DLA Information System Security Officers (ISSOs)

DRMS DBMS Data Owner

D. USER PRIVILEGES:

ISSOs and DBMS Data Owner--Create and Delete--Field Cost DBMS
 Options File
 TASOs--update--user data elements of the Field Cost DBMS
 Options File
 ISSOs and TASOs--update--Mode Panel
 ISSOs--alter--System Selection Panel
 TASOs--read only--System Selection Panel
 ISSOs--alter--AURA System File
 ISSOs--alter--AURA TASO File

E. USER POSITION SENSITIVITY LEVEL:

DLA ISSOs -- Critical Sensitive
 DLA TASOs -- Noncritical Sensitive
 DBMS Owners--Noncritical Sensitive

1-4
 SECTION II

ACCESS MATRIX

SYSTEM/APPLICATION/COMPARTMENT: AURA

DATA ELEMENTS/ AGGREGATES/ FORMS/FILES	DATA SENSITIVITY CATEGORY	USERS, USER GROUPS	USER PRIVILEGES
DRMS Field Cost DBMS File	5	DBMS Owners DLA ISSOs DLA TASOs	Create & Delete Create & Delete Update
Mode Panel	1	DLA ISSOs DLA TASOs	Update Update
System Selection Panel	1	DLA ISSOs DLA TASOs	Alter Read Only
AURA Systems File	1	DLA ISSOs	Alter
AURA TASO File			

--	--	--

NOTE: If the matrix references other sources (e.g., not data), then there is no reason to include the column titled DATA SENSITIVITY CATEGORY. Also, the first column heading would be RESOURCES rather than DATA ELEMENTS/AGGREGATES/FORMS/FILES.

1-5

INSTRUCTIONS FOR COMPOSING SECTION II

1. The list of DATA ELEMENTS/AGGREGATES/FORMS/FILES does not have to contain every element or item in a particular system or application. At a minimum, the list must consist of all system/application items that are sensitive. Enclosure 3 is a list of different kinds of sensitive unclassified data, but it is not a complete list of all data that is sensitive. In some instances, sensitivity determinations are made by the data owners. In most instances, resources sensitivity is determined by the resource owner, or by some other authority or administrative source.

2. If a data element is sensitive, then the DLA Sensitivity Category is also annotated in parentheses (see pages 1-4 and 1-5 for an example of annotating a sensitivity level, and see page 1-8 for the different categories of sensitive data). In those occasional instances where data is sensitive but does not fit into one of the DLA categories, N/C (No Code) should be entered. An example of this would be the Defense Nuclear Ordnance Item Reference Data. When dealing with other ADP resources (e.g., not data) that are considered sensitive, there is no Sensitivity Category. In this case, N/A (Not Applicable) would be entered in

parentheses next to the resource description. Examples of sensitive resources would be software such as NETMASTER and VRA.

3. The list of DATA ELEMENTS/AGGREGATES/FORMS/FILES (or RESOURCES) should contain nonsensitive items where the likelihood exists that someone will submit a request for access. An example of possible request for access to nonsensitive items would be the AURA Mode and System panels (see the examples at point B on page 1-4).

4. Items that can be excluded from the list of DATA ELEMENTS/AGGREGATES/FORMS/FILES are those things which are not sensitive and are not likely to be requested. As an example, if someone submitted a request for DAISY or IRIS access, it is probable the individual would not also request access to DRMO RICs, which are nonsensitive data elements. RICs are data returned when a successful interrogation is submitted. The DAISY or IRIS owner, knowing this, would probably not want to include that particular element in the list of DATA ELEMENTS/AGGREGATES/FORMS/FILES.

5. The list of AUTHORIZED USERS/USER GROUPS consists of entries depicting different users/user groups. The owner should enter users and user groups in fairly concise terms to assure there can be no misunderstanding about who the users are that the owner is referring to. As an example, the phrase 'DRMO Chiefs' is a very explicit group, but the term 'Managers' is vague (it would be best to say 'DRMS Zone Managers' if that is what the owner intends). Also, the owner can further expand the user definition for more clarification of the users or user groups. An example of this would be a statement such as 'DLA Trade Security Control personnel located at the Memphis International Sales Office'.

6. The owners may use various words to portray the privileges they will be granting to users. Words such as 'read', 'list', 'print', 'compile', 'create', 'execute', 'run', 'change', 'update', 'alter', and 'delete' are examples of some of the words that can be used. However, some terms have specific meaning within data processing, so a degree of care should be taken when choosing terms (refer to enclosure 4 for further guidance on terms describing privileges). Also, the advice of the AISSOs may be of considerable help in this area. It should be remembered this guidance applies to other ADP resources (locally developed programs, COTS software, other DP/T capabilities). It would not be proper to use terms such as 'compile' and 'execute' for denoting access privileges to different kinds of data.

7. The owners need to refer to enclosure 2 when considering requirements pertinent to positions. As a rule of thumb, any system/application item viewed as non-sensitive or non-critical and which has no other access restriction imposed by the data owner would not require other than an ADP-III position (Nonsensitive Position) for accessing the item. For access to sensitive items, position requirements would depend upon the AIS controls and procedures in place that provide appropriate protection.

Strong AIS security features mitigate risks and, in that case, there may not be a compelling need for a position sensitivity requirement higher than an ADP-II category for access to certain kinds of sensitive data. It is up to the owner to decide upon position requirements for access to various data and resources. However, it should also be realized there are some positions which the ADP-I designation is mandatory (e.g., Senior Vice Presidents). Owners do not have any leeway in changing the sensitivity category of those positions. As a note of clarification, the category criteria take into consideration a wide range of a

person's ADP involvement and responsibilities. Access to data is but one of many factors pertinent to making determinations about the appropriate sensitivity level of a position.

8. The ACCESS MATRIX (the second part of SECTION II) is a summary of the details in the first part of SECTION II (the ACCESS INFORMATION part). The matrix serves as a quick visual reference to the contents in the first part. The one item that does not have to be entered in the matrix is the position sensitivity category (a continuous repetition of the sensitivity category next to the user/user groups is not necessary).

9. In the event the owner wants to include data and/or resources of other systems/applications owned, then a new page of the five illustrated entries as shown on page 1-4 and a related access matrix as portrayed on page 1-5 would be composed to cover the other systems/applications. In this case, the access policy's title page would reflect the scope of policy coverage (the title page would include all systems/applications covered) and, if an INTRODUCTION/OVERVIEW page is present, the presentation would also reflect the other systems/applications of the access policy.

10. Sensitive category descriptions. DLA has defined seven categories of sensitive unclassified data and each category has been assigned a numeric code. Each category has various security requirements to be implemented for assuring appropriate protection is in place (there are seven requirements for sensitive data, but not all are required for every category). The different kinds of sensitive unclassified data listed in enclosure 3 fall into the various categories. NOTE: Data Sensitivity Category Code 1 is NONSENSITIVE and Category 9 I CLASSIFIED.

CATEGORY

CODE	TITLE	DESCRIPTION
2	PROPRIETARY	Information provided by non-Government sources on the condition that it not be released to other than non-Government sources. Examples include company proprietary data, contract bids, quality assurance evaluations, and pre-award survey information.
3	PRIVACY	Personal and private information as defined in the Privacy Act of 1974 or the FOIA.
4	PERSONAL GAIN	Information which could be changed by a person to provide him or herself benefits, such as performance ratings or education levels.
5	ACCOUNTING	Quantitative data which provides official accountability records, such as balances-on-hand, asset amounts, credits, and debits. Does not include similar data when used only for reference or research purposes.
6	ASSET LOSS	Data which contributes to the automated decision to transfer or pay out a tangible asset, including asset routing information (e.g., data involved in creating payments via check or electronic fund transfer, data leading to the shipment of material).
7	SECURITY	Data associated with the security CONTROL mechanisms (e.g., passwords) that control access to the system, contain audit records, and assure the integrity of the TCB and its extensions.
8	TRUSTED	Information that when received, is INFORMATION accepted as authentic (e.g., electronically prepared AUTODIN messages, electronic mail messages).

ADP POSITION CATEGORIES
AND
CRITERIA FOR DESIGNATING POSITIONS

OMB Circular A-71 (and Transmittal memo #1), July 1978 OMB Circular A-130, December 12, 1985, and FPM Letter 732, November 14, 1978 contain the criteria for designating positions under the existing categories used in the personnel security program for Federal civilian employees as well as the criteria for designating ADP and ADP related positions. This policy is outlined below:

ADP POSITION CATEGORIES

1. Critical-Sensitive Positions.

ADP-I positions. Those positions in which the incumbent is responsible for planning, direction, and implementation of a computer security program; major responsibility for the direction, planning and design of a computer system, including the hardware and software; or, can access a system during the operation or maintenance in such a way, and with a relatively high risk causing grave damage, or realize a significant personal gain.

2. Noncritical-Sensitive Positions.

ADP-II positions. Those positions in which the incumbent is responsible for the direction, planning, design, operation, or maintenance of a computer system, and whose work is technically reviewed by a higher authority of the ADP-I category to insure the integrity of the system.

3. Nonsensitive Positions.

ADP-III positions. All other positions involved in computer activities.

In establishing the categories of positions, other factors may enter into the determination, permitting placement in higher or lower categories based on the agency's judgment as to the unique characteristics of the system or the safeguards protecting the system.

CRITERIA FOR DESIGNATING POSITIONS

Three categories have been established for designating computer and computer-related positions - - ADP I, ADP-II, and ADP-III. Specific criteria for assigning positions to one of these categories is as follows:

<u>Category</u>	<u>Criteria</u>
ADP-I	<p>Responsibility for the development and administration of agency computer security programs, and also including direction and control of risk analysis and/or threat assessment.</p> <p>Significant involvement in life-critical or mission-critical systems.</p> <p>Responsibility for the preparation or approval of data for input into a system which does not necessarily involve personal access to the system, but with relatively high risk for effecting grave damage or realizing significant personal gain.</p> <p>Relatively high risk assignments associated with or directly involving the accounting, disbursement, or authorization for disbursement from systems of (1) dollar amounts of \$10 million per year or greater, or (2) lesser amounts if the activities of the individual are not subject to technical review by higher authority in the ADP-I category to insure the integrity of the system.</p> <p>Positions involving <u>major</u> responsibility for the direction, planning, design, testing, maintenance, operation, monitoring, and/or management of systems hardware and software.</p> <p>Other positions as designated by the agency</p>

head that involve relatively high risk for effecting grave damage or realizing significant personal gain.

2-2

<u>Category</u>	<u>Criteria</u>
ADP-II	<p>Responsibility for systems design, operation, testing, maintenance, and/or monitoring that is carried out under technical review of Higher authority in the ADP-I category, includes, but is not limited to:</p> <p>(1) access to and/or processing of proprietary data, information requiring protection under the Privacy Act of 1974, and Government-developed privileged information involving the award of contracts;</p> <p>(2) accounting, disbursement, or authorization for disbursement from systems of dollar amounts less than \$10 million per year. Other positions are designated by the agency head that involve a degree of access to a system that creates a significant potential for damage or personal gain less than that in ADP-I positions.</p>
ADP-III	<p>All other positions involved in Federal computer activities.</p>

EXAMPLES OF SENSITIVE UNCLASSIFIED DATA

1. Acquisition of supplies or equipment for the Military Services.
2. Status of spare parts, especially for major weapons systems.
3. Industrial manufacturers' capability to meet operational readiness.
4. Evaluation of shipping/scheduling by contractors.
5. Warehousing and shipment of materials.
6. Inventory management records.
7. Requisitions from services, to include trend history.
8. Emergency relocation and logistics planning.
9. Procurement, inventory, and distribution records of bulk fuels and petroleum products.
10. Reutilization and sales of surplus equipment purchased and managed by DoD.
11. Location, transportation, and disposal of hazardous waste materials.

12. Financial and accounting records.
13. Contractor Payment Notices (CPNs).
14. Shipment Performance Notices (SPNs).
15. Status of personnel selection process, Equal Opportunity complaints, and disciplinary actions.
16. Personnel payroll records.
17. Engineering drawing for DoD equipment.
18. Contracting and commercial proprietary data.
19. Contract technical and pricing data.
20. Research and development data.
21. Automated Information Systems (AISs) audit trail, logon, and password (or other authenticator) records.
22. Security countermeasures implemented for the protection of sensitive data.
23. Results of investigations of suspected fraud, waste, and abuse activities.
24. Results of criminal investigations and crime prevention surveys.
25. Records of suspensions and debarments.

3-1

Encl 4
DRMS-D 5210.5

GUIDANCE ON THE USE OF TERMS FOR DESCRIBING USER PRIVILEGES

1. Owners may use a wide variety of terms to describe privileges. However, some terms have specific meaning within ADP, and the owners should take this into consideration when assigning privileges.

2. Privileges are actually ADP capabilities controlled by and made possible through different means such as Commercial Off The Shelf (COTS) packages, components of an Operating System's platform of software, and Operating System code. In some instances, it may be advantageous for the owners to discuss privileges with the AISSO responsible for a particular AIS, or with other individuals who have ADP knowledge (e.g., systems analyst, programmers, and computer specialists).

3. The following paragraphs define and explain terms associated with privileges.

a. READ, READ ONLY (also; LOOK AT, VIEW, BROWSE). This is generally considered the least privilege that can be granted to a user. When dealing with nonsensitive unclassified data, and when the owners (or other authorities) have no other rules or restriction pertinent to access, anyone with a 'need-to-know' may be granted the read privilege. Normally, the intention is not to give the user any other capabilities along with read. However, the 'read' privileges implies 'execute' in an IBM MVS/ESA or MVS/XA environment protected by the Resources Access Control Facility (RACF). Therefore, a user given read capability to a particular library containing Job Control Language (JCL) jobs could run a JCL job stored in the library.

b. LIST (also; PRINT). In an ADP environment, listing data for viewing on a monitor or printing hard copy output is normally associated with the read privilege. When read is requested, an ADP list or print capability is almost always available and set up for the user when the read capability is established.

c. EXECUTE (also; RUN). This is used in conjunction with references to program object code and to JCL streams (or to other control languages or other 'executable' objects). To execute a program means to run the program. In other words, running an executable ADP object causes the object to do what it is designed and programmed to do. NOTE: The term 'object' is commonly used to denote programs, files, and other ADP resources; the term 'subject' refers to users and user surrogates.

d. COMPILE. In general, this refers to accessing program source code for the purpose of making changes and producing an 'executable' object code file. In many instances this infers performing steps such as 'compile', 'link', and 'go' which are prevalent in testing environments on IBM large-scale computers.

e. CREATE. This is not a widely used term describing ADP functions (it is used in RACF profiles to establish a user capability). In some instances it may be meaningful for the owner to use the term when the owner wishes to convey his/her authority for someone to establish new objects.

f. UPDATE (also; CHANGE). This is used to denote the privilege for allowing someone to change the value of a data element or the contents of a data field. Update implies read authority.

4-1

g. ALTER. This is the privilege which allows addition and deletion of file data fields or data base entries. Alter implies update or change capability. In IBM large-scale computer environments protected by RACF, alter also implies delete. In computers using RACF, a user with alter authority to a file or a library (a.k.a. Partitioned Data Set) could also delete the file or library.

h. ROOT. The root authority is a most powerful capability in minicomputer environments using UNIX Operating Systems. Root allows the total range of not only add/delete/change actions, but other ADP activities such as monitoring, suspending, and intercepting anything within the ADP environment. Root is commonly referred to as 'superuser' authority.

i. DELETE. Delete gives the authority for someone to remove ADP objects. This capability, along with root and alter, should be significantly restricted, and the owner should expect to receive substantial justification when these privileges are requested.

j. SPECIAL. This term has explicit meaning relating to privileges. It is a RACF profile entry and probably should not be used by an owner in an attempt to describe privileges.

k. AUDITOR. This term also has explicit meaning relating to privileges. It is a RACF profile entry and probably should not be used by an owner in an attempt to describe privileges.