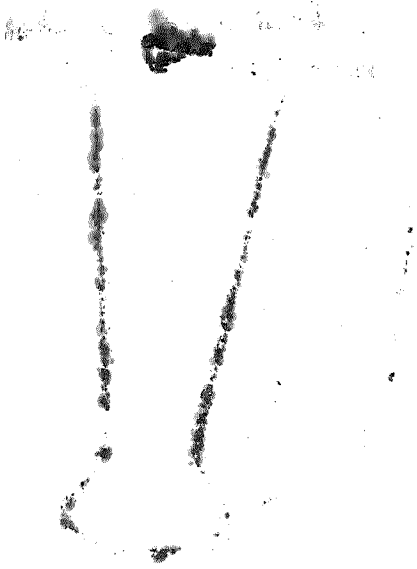


NOS MULTI-LEVEL SECURITY

GENERAL INTERNAL DESIGN

Revision C

Disclaimer:

This document is a working paper only. It is subject to change and does not necessarily represent any official intent on the part of Control Data Corporation.

Control Data Corporation

REVISION RECORD

REVISION	DESCRIPTION
A	(80/04/07) Original document approved, DCS Log ARH 3621.
B	(82/06/11) Revised for NOS V2.
C	(82/10/11) Revised to reflect current design requirements and provide additional detail.

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

1.0 INTRODUCTION.

"Multi-Level Security" has been defined by the U.S. Department of Defense in its ADP Security Manual [4] as:

> "A mode of operation under an operating system which provides a capability permitting various levels and categories or compartments of material to be concurrently stored and processed in an ADP system ... This mode of operation can accomodate the concurrent processing and storage of (a) two or more levels of classified data, or (b) one or more levels of classified data with unclassified data depending upon the constraints placed upon the system by the delegated Approving Authority."

This GID describes the initial implementation of the multi-level security concept on the NOS operating system. Some of the major design features of this phase of MLS implementation include:

* Provision of eight hierarchical access sensitivity levels for classification of data and other system resources.
* Provision of thirty-two security categories (compartments) for classification of permanent files.
* Mandatory access control and flow control policy enforcement.
* Separate passwords for interactive and batch use.
* Password encryption.
* User password expiration terms.
* Permanent file password expiration terms.
* Permanent file PERMIT expiration terms.
* Overwrite (clearing) of directly accessible mass storage files.
* Classified output labeling.
* Clearing of storage after job rollout.

1.1 APPLICABLE DOCUMENTS.

1. Multi-Level Security Overview and Requirements, by J.N. Nielsen, Arden Hills Programming Division, CDC, DCS Log ARH 2678; June, 1978.

2. NOS Multi-Level Security Solution DAP, by P.D. Farrell, Arden Hills Programming Division, CDC, CDS Log ARH 3317; August, 1979.

3. EST Expansion Solution DAP, by J.J. Eikum, Arden Hills Programming Division, CDC, DCS Log ARH 3682; January, 1980. Revised by R.A. Japs, Arden Hills Programming Division. CDC, May, 1982.

4. Department of Defense ADP Security Manual, DoD 5200.28-M, January, 1973.

5. EST Expansion GID by D.K. Eldred, Arden Hills Programming Division, May, 1982.

6. DoD Regulation 5200.1-R, "Information Security Program Regulation", The Deputy Secretary of Defense, October, 1980.

7. NHP Enhancements for NOS MLS, by P. D. Farrell, Arden Hills Programming Division, CDC, DCS Log ARH5167, July, 1982.

8. User Service Class Assignment GID, by B. M. Sliwinski, DCS Log ARH5211.

9. Validation Block Reorganization DAP, by P. D. Farrell, DCS log ARH5214.

1.2 DEPENDENCIES.

1.2.1 EQUIPMENT ACCESS LEVEL LIMITS.

Implmentation of equipment security access limits is dependent upon the EST Expansion project.

1.2.2 NETWORK HOST PRODUCTS.

MLS Feature modifications to the Network Configuration File (NCF), to Terminal-to-Application requests, and for login security are dependent upon implementation by Network Host Products, Sunnyvale Programming Division.

1.3 USER IMPACT.

The following items describe areas where the changes made by the Multi-level Security feature may affect current user programs and procedures. More detail on the affected areas are provided in the appropriate sections of this document.

1.3.1 FET FIELDS AND USAGE.

Multi-level security makes use of FET word FET+1, bit 39, and FET word FET+4, byte 1, both of which fields have been unused up to now on the NOS Operating system. Users should insure that their programs do not use these fields in a conflicting manner.

1.3.2 SEPARATE BATCH AND INTERACTIVE PASSWORDS.

With Multi-level Security, a site may require, if desired, separate batch and interactive passwords. Previously, one password was used for both batch and interactve use. This feature is not dependent on the security mode of the operating system.

1.3.3 USER PASSWORD EXPIRATION.

Installations may define expiration dates for user passwords. Users will find their passwords no longer valid on or after the expiration dates. The decision of whether or not to assign password expiration dates and the processing of expired user passwords will be the responsibility of the installation. This feature is independent of the security mode of the operating system.

1.3.4 PERMANENT FILE PASSWORD AND PERMIT EXPIRATION DATES.

Validated users will be able to specify expiration dates for permanent file passwords and for PERMIT's. This ability is independent of the security mode of the operating system.

1.3.5 VALIDATION TO WRITE UNLABELED TAPES.

Previously, any user validated to use magnetic tapes could read and write both labeled and unlabeled tapes. With Multi-level Security, however, regardless of the security mode of the operating system, a user must be explicitly validated to write unlabeled tapes.

1.3.6 VALIDATION FILE INCOMPATIBILITY.

This project, and others, are making a number of changes to the format of the validation file. Because of these, previous versions of the validation file are incompatible and any previous version must be returned to source and rebuilt.

2.0 OVERVIEW.

NOS Multi-Level Security is based upon two mechanisms for ensuring the privacy of a set of data, mechanisms in addition to the standard NOS privacy mechanisms. These are (1) hierarchical security access levels, and (2) security categories (often referred to as "compartments"). The access level and category(s) of a set of data are attributes of that data, determined and defined by the owner of the data in accordance with applicable security policy.

2.1 SECURITY ACCESS LEVELS.

Eight security access levels are available for the classification of data, ranging from 0, the lowest (unsecured or unclassified) level, to 7, the highest level. These levels are hierarchical, level "x" being defined as less sensitive than level "x+1". The creator, or owner, of a data file - permanent file, local file, or magnetic tape - may assign an access level to that file depending upon the owner's individual validations and upon operating system constraints. Alternatively, the owner may allow the file's access level to be assigned automatically by the operating system.

It should be noted that it is the responsibility of the owner of a set of data to determine the security access level appropriate for the data in accordance with the privacy and security policies applicable to the data contained within the file.

2.2 SECURITY ACCESS CATEGORIES.

In addition to the eight access levels, there are thirty-two categories available for the classification of data. The owner of a permanent mass storage data file may assign any or all of the thirty-two categories to that file, depending upon the owner's individual validations and upon operating system constraints.

Like security access levels, it should be noted that is also the responsibility of the owner of a permanent file to determine the security category(s) appropriate for the data in accordance with the privacy and security policies applicable to the data contained within the file.

Security categories are not hierarchical. The purpose is to allow separation of data into different compartments, regardless of the security access level of the file. For instance, within an access level corresponding to "TOP SECRET", files could be categorized as "MEDICAL", "PERSONNEL", "MILITARY", etc. This mechanism will allow users to access data only in authorized areas, determined by their validation.

2.3 OPERATING SYSTEM MODE.

There are defined two modes of operation of the NOS Operating System under Multi-Level security: the secured mode and the unsecured mode.

The unsecured mode is equivalent to the current mode of operation of the NOS Operating System. The file security permissions and the user security authorizations of the Multi-Level Security system are not enforced by the operating system when in the unsecured mode.

In the unsecured mode a user may assign security access levels and/or categories to files. The levels and categories will be maintained by the system but access validation will not be enforced by the operating system. This will allow applications to construct their own security systems independently of the operating system when the system is to operate as an unsecured system.

Unless specifically noted, this document refers only to the secured system; the unsecured system will remain unaffected.

3.0 SECURITY POLICY.

This section defines the security policy, or rules to be followed for access to secured objects, under the NOS Multi-Level Security system.

3.1 MANDATORY SECURITY.

In conjunction with the formal security access level and category designations associated with classified data (the "mandatory" classification designations), there is a corresponding set of formal clearances which users must have in order to access classified information. Compromise is is defined as "the disclosure of classified information to persons not authorized access thereto." A user may not obtain access to classified information if the user is not cleared to the classification level of the information.

A requirment of the above is that classification labels associated with sensitive data cannot be arbitrarily changed, since this could permit individuals who lack the appropriate clearance to access classified information. An additional requirement is that the system must control the flow of information so that data from a higher classification cannot be placed in a storage object of lower classification unless its "downgrading" has been authorized.

The term "Mandatory Security" has evolved in the computer security community to identify the access policy rules that deal with mandatory classification designations for sensitive information and individual clearances.

3.2 DISCRETIONARY SECURITY.

In addition to the formal requirements covered under Mandatory Security, DoD Regulation 5200.1-R [9] stresses the Need-to-Know principle. The regulation states that "no person may have access to classified information unless ... access is necessary for the performance of official duties."

The regulation further states that "No one has the right to have access to classified information soleley by virtue of rank or position." Thus, even though an individual has all the formal clearances for access to specific classified information, each individual's acces to information must be based on a demonstrated Need-to-Know basis. The requirement to release classified information only to those who have a legitimate Need-to-Know is satisfied when an individual who has authorized posession of the classified information (the permanent file owner in NOS) ascertains that "a determination of trustworthiness has been made ... for some other individual who has a Need-to-Know for that classified information. This requires that the permanent file owner must exercise

discretion in sharing classified information with other individuals or groups of individuals who already have the appropriate formal clearances. The term "Discretionary Security" has evolved in the computer security community to name the computer system's ability to control information on an individual basis. Note that this requirement is not discretionary in a "take it or leave it" sense. The Need-to-Know test must be explicitly satisfied before access can be granted to information.

Discretionary Security is satisfied in the NOS MLS system by the classical NOS Permanent File private, semi-private, and public file mechanism, with its PERMIT mechanism to additionally, explicitly grant or deny file access. In addition, Multi-Level Security adds password and PERMIT expiration dates.

Under NOS, Discretionary Security is applicable to both secured systems (systems enforcing Mandatory Security) and unsecured systems (non-MLS).

4.0 SYSTEM FUNCTIONS.

4.1 OPERATING SYSTEM MODE.

The security mode of the operating system is determined at deadstart time by IPRDECK entry. Once set, the operating system security mode is fixed and cannot be altered except by another level 0 deadstart.

The format of the OPSECM IPRDECK entry and the options available are described in Section A.3.1.2.

The default value of the operating system security mode is zero (unsecured). The distinction between the different modes where Multi-level security is enabled (1, 2, and 3) is solely to determine what options are available to the operator when changing the system access limits. (See Section 4.2). No other use of this value is made in the system.

4.2 OPERATING SYSTEM ACCESS LIMITS.

Control of access to the operating system when the system is in the secured mode (OPSECM IPRDECK entry equal to 1, 2, or 3) is accomplished by setting the highest and lowest security access levels that are allowed in the system. These levels are referred to as the system access limits. They define an inclusive range of access levels: no job may execute at an access level below the lower bound or above the upper bound. Similarly, no file or device may be accessed below the lower bound or above the upper bound.

The operating system access limits may be set by IPRDECK entry during deadstart or by console command during system operation if the security mode allows. See Section A.3.1.5 for the format of the SECURES,SY IPRDECK entry and console command.

The SECURES,SY IPRDECK entry will be accepted but will have no affect when the system is in the unsecured mode (OPSECM IPRDECK entry value equal to zero).

In order to prevent unauthorized modification of the system access limits during operation, console use of the SECURES command will require that the console be in security unlock status. See section 4.7.2 for a description of security unlock status.

4.3 ORIGIN TYPE ACCESS LIMITS.

In addition to the operating system access limits, access limits may be defined for each origin type. The system access limits are by definition the access limits for System origin. Unless redefined by deadstart IPRDECK entry or by console command, all origin type limits will be the same as the system access limits.

This feature will be useful for limiting, for instance, interactive jobs to a certain range of access levels while batch jobs are permitted a greater range of access levels.

Origin type access limits may be set by the SECURES,ot IPRDECK entry during deadstart or by the SECURES,ot console command during system operation. See Section A.3.1.5 for the format of the SECURES,ot IPRDECK entry and console command.

The access limits defined for an origin type other than System (which set the system access limits) must lie within the system access limits. If the system access limits are reset with the SECURES,SY command, all origin type limits will also be reset.

In order to prevent unauthorized modification of the job origin type access limits, console use of the SECURES,ot command will require the console to be in security unlock status.

4.4 EQUIPMENT ACCESS LEVEL LIMITS.

Access level limits may be assigned to individual equipment. The access level limits define the lowest and highest access levels of data that may be written to or read from that equipment.

Access level limits of equipments are set during deadstart using the ACCESS EQPDECK entry. Equipment access level limits apply to mass storage, unit record, and magnetic tape equipments. Limits entered for other types of equipment are ignored by the system. See section A.4.1.1 for the format of the ACCESS EQPDECK entry.

The default access level limits of all equipment will be zero, i.e. no secure data can be written to or read from that equipment.

Equipment access level limits of unit record equipment only may be set or changed during system operation using the SECUREQ console command. Use of this command requires the system to be in security unlock status. See Section A.3.2.3 for the format of the SECUREQ console command.

4.5 MASS STORAGE DEVICE ACCESS LEVEL LIMITS.

When a mass storage or ECS device is initialized, the access level limits of data permitted to reside on the device will be recorded in the MST in the device label. No files may be assigned to that device that have access levels outside the device access level limits. Existing files on the device may not have their access levels changed to levels outside the access level limits. See Section 6.7 for a description of device recovery.

4.5.1 DEADSTART INITIALIZATION.

When a device is initialized during deadstart processing, the equipment access level limits will be copied from the device EST entry to the device MST entry, then written with the MST entry to the device label.

4.5.2 ON-LINE INITIALIZATION.

Options will be added to set the device access level limits during on-line initialization. These will be entered from the K-display along with the other parameters specified by the operator. They must be within the equipment access level limits. See section 6.37 for a description of the new operator entries.

The default values of the device access level limits are the equipment access level limits in the device's EST entry.

4.6 CONSOLE SECURITY STATUS DISPLAY.

The operating system security status will appear on the left-screen header when the system is operating as a secured system and will include the lower and upper system access limits.

When the system is operating as an unsecured system (operating system security mode = zero), the security status display will be blank.

See Section A.4.6.1 for the format of the left screen header.

4.7 OPERATOR SECURITY.

It must be a basic assumption that in a security environment an individual who is allowed operational access to the system console has been properly cleared by the installation's security control authority for access to the highest level of data that will be processed by the system in that individual's presence.

For this reason, NOS Multi-Level Security makes no restriction upon common, normal operator functional controls of the system. The conflicting assumption, that the operator is not properly cleared for normal functional control of a secured system, is not within the purview of this document.

4.7.1 SECURITY ADMINISTRATOR.

Although the operator can be considered cleared for normal system control functions, there are certain system control functions which are more sensitive in a multi-level security system environment. These include the ability to change users' validations, to modify system security control parameters, or to directly interrogate or alter user programs or data.

In order to provide a higher, more sensitive level of access to system control, NOS Multi-Level Security will use the concept of Security Administrator Privilege, a validation privilege for the individual in the user validation file. This privilege will allow an installation to designate a certain individual or individuals as security administrator(s) in accordance with the installation security procedures. Those system control functions which require this privilege are described in various portions of this document.

4.7.2 SECURITY UNLOCK STATUS.

Many operator functions currently require the console to be UNLOCKed. This is to insure that they are not done accidently, due to their potential consequences. In a secured environment, this concept is being extended to restrict certain operator functions to someone with security administrator privileges. This includes functions such as changing and displaying memory, as well as new commands (SECURES, SECUREQ). See section 6.4.2 for the functions that will be restricted, and the format of the command used to set security unlock status at the console.

4.8 USER VALIDATION AND AUTHORIZATION.

All users must be validated for permission to access data and to use the system. The information necessary to establish a user's validation (the Capability List in some terminologies) is contained in the user validation file (VALIDUZ or the equivalent) and contains such security access information as the user's passwords, password expiration dates, permitted access levels and categories, and special privilege validations. See section 6.36 for a description of the MODVAL parameters used to set these values in the user's validation file entry.

4.8.1 USER PASSWORDS.

Each user will have two passwords defined in the validation file; one for batch and one for interactive access to the system. Interactive access is defined as any login to a NAM application (IAF, RBF, TAF, etc.). These passwords may be defined to be the same or not, as determined by each installation's requirements. All passwords will be encrypted; the display code value will not be stored in the validation file. When validating user entry of passwords, the entered value will first be encrypted, then compared with the validation file. The encryption algorithm will be of the trap-door function type to insure that even if the security of the encrypted value is compromised, the original password cannot be determined.

4.8.2 USER PASSWORD EXPIRATION.

When a user password is created or is changed, it will have an associated expiration date. On or after the expiration date the password will no longer be valid. The expiration date will normally be automatically assigned when the password is defined or is changed (MODVAL or PASSWOR) and its term will be controlled by installation option. The released value of the default expiration term will be infinite, i.e. no expiration. Password expiration will apply both in secured and unsecured systems.

Users may be validated to assign password expiration dates by means of optional parameters on the PASSWOR command. The password expiration date thus assigned will be constrained by an installation option maximum.

4.8.3 USER VALIDATED ACCESS LEVELS.

In each user's entry in the validation file there will be a list of the security access levels that the user may access on a secured system. Any, all, or none of the eight available levels may be validated for access by the user. The access levels permitted a user are defined using the MODVAL utility in the CREATE or UPDATE option modes.

4.8.4 USER VALIDATED ACCESS CATEGORIES.

In each user's entry in the validation file there will be a list of the access categories that a user may access on a secured system. The user may be validated to access any, all, or none of the thirty-two available access categories. The access categories validated for the user are defined using the MODVAL utility in the CREATE or UPDATE option modes.

4.8.5 SPECIAL PERMISSIONS.

Special permissions are privileges that may be individually granted to users in accordance with the installation's security policy. The default mode of all special permissions when the user's validation file entry is created is off (not granted).

In order to grant any of the special permissions, MODVAL entries will be provided which may be used in either the CREATE or UPDATE modes. The permissions added to the user validation file by NOS Multi-Level Security are described below:

* Security Administrator

  This permission is used to identify those users who have extended capabilities to access sensitive system control functions on a secured system. Various utilities such as MODVAL or SYSEDIT will require that the user have this privilege.

  When a new user validation file is created, this permission will automatically be granted to the SYSTEMX user number, user index 377777. This establishes an initial security administrator for the system. Thereafter, the security administrator (executing MODVAL under the SYSTEMX user number) may assign this privilege to another user or users. After this is done, under a new privileged user number, the security administrator privilege may by deleted from SYSTEMX.

  In order to prevent a system from being left with no user with security administrator privilege, a user may not delete this privilege from the user's own validation file entry: only a different user, also with security administrator privilege may delete the privilege from the first user.

* User May Change Passwords

  This permission currently exists on the NOS System as a validation option.

  This permission will be required on both secured and unsecured systems.

* User May Assign User Password Expiration Date.

  Permits the user to assign a user password expiration date using the XD or XT parameters on the PASSWOR control statement.

  This permission will be required on both secured and unsecured systems.

* User May Assign Permanent File Password Expiration

  Permits the user to assign a permanent file password or PERMIT expiration date using the XD or XT parameters on permanent file commands.

  This permission will be required on both secured and unsecured systems.

* User May Downgrade Job Access Level.

  Permits the user to downgrade (lower) the access level of a job using the SETJAL command and macro.

* User May Downgrade File Access Level.

  Permits the user to downgrade (lower) the access level of local or permanent files using the SETFAL or SETPFAL commands and macros.

* User May Write-Down.

  Permits the user to write to files which are at a lower access level than the access level of the user job. This permission is also required to define an existing local file that has an access level lower than that of the job as a direct access permanent file.

* User May Write Unlabeled Magnetic Tapes.

  Permits the user to write unlabeled magnetic tapes. This permission will not be required by System-Origin jobs.

  This permission will be required on both secured and unsecured systems.

* User May Execute On-Line Diagnostics.

  Permits the user to execute On-Line Diagnostics, and perform other Customer Engineer operations.

  This permission will be required on both secured and unsecured systems.

4.9 JOB ACCESS LEVELS.

Each executing job in a secured system has an associated access level. The job access level is dynamic and may change during the life of the job in the system.

4.9.1 JOB CARD ACCESS LEVEL LIMIT.

The maximum access level that a job may attain is defined by the AL (Access Limit) parameter on the job's JCE Card. If the value of this parameter at the time of job entry is greater than the access limits for the job origin type, or not valid for the user, the job will be aborted with a JOB CARD ERROR. On an unsecured system, this parameter will only be checked for being one of the eight defined access level names.

See Section A.4.4.1 for the format of the JOB card.

4.9.2 INTERACTIVE JOB ACCESS LEVEL LIMIT.

The access level limit of an interactive job is defined to be the access level limit of the user's communications line as defined in the Network Configuration file.

4.9.3 JOB VALID ACCESS LEVELS.

The following items determine which access levels are valid for a job. Whether each item restricts the valid levels at the upper or lower bound is also indicated.

1. The Origin Type Access Limits for the job's origin type. (upper/lower).

2. The access levels validated for the user in the validation file entry (upper/lower).

3. For jobs with a JOB card, the job access level limit from the AL parameter (upper). If no limit is specified on the JOB card, the default will be the lowest valid level as determined by the other criteria. This will limit the job to this single access level.

4. For interactive jobs, the line access limit for the terminal communications line (upper).

5. For jobs created from an existing local file (SUBMIT or ROUTE), the access level of that local file. (lower)

A job's valid access levels are those access levels which meet all of the criteria listed above. These levels are not necessarily a contiguous subset of the available levels.

A job's Access Level Limits are defined as the highest and lowest access levels that a job may attain in the system under the constraints listed above. These limits will not change during the life of a job. If the job's origin type limits are changed with the SECURES command, causing the job's access level limits to be out of that range, the job will be aborted with a security violation.

A job's valid access categories are those that are both valid for the user as defined by the validation file entry and valid for the system as defined by the SECCATS IPRDECK entry.

4.9.4 INITIAL JOB ACCESS LEVEL.

When a job is initially scheduled to a control point for execution, the job access level will be set to the job's lower access level limit.

4.9.5 USER CHANGE OF JOB ACCESS LEVEL.

During the course of job processing, a user may use the SETJAL command to raise or lower the job access level. The new job access level must by valid for the user and within the job access level limits. If these conditions are not met, the attempt will be processed as a security violation. Security violation processing is described in section 4.21.

Any user may use the SETJAL command to raise the job access level to a valid value, however validation is required to lower (downgrade) the job access level. The SEJAL command is described in Section A.3.3.4.

On an unsecured system, job access levels are not recognized and the SETJAL command will be ignored by the system.

4.9.6 SYSTEM ADVANCE OF JOB ACCESS LEVEL.

On a secured system, when a user process reads from a file which has a higher access level than the user's job (Read-down), the system will automatically advance the job's access level to the access level of the data (simple security condition rule). The job access level will then remain at the new level until it is changed (by another dynamic advance or by user SETJAL command).

This process will not take place on an unsecured system or if the user process has an SSJ= entry point or Subsystem ID.

There is no equivalent mechanism to dynamically lower the access level of a job; this can be done only with the SETJAL command.

4.10 FILE ACCESS LEVELS.

All files in a secured system have associated with them a security access level. Access to any file on the system is restricted to those files whose access levels are within the system access limits and whose access levels are valid for the user within the user's job access limits.

On an unsecured system, file access levels other than zero may exist and will be maintained by the system, but access validation will not be checked or enforced.

4.10.1 LOCAL FILES.

The access level of a local file will be set by the system to the access level of the job creating the file at the time that the file is created or assigned to the job. The optional AL parameter on the ASSIGN command may be used to create a file at an access level other than the access level of the job. The access level defined must be a valid access level for the user and job. The ASSIGN command is described in Section A.4.4.2.

On an unsecured system, a user is free to ASSIGN any access level desired (0 through 7) to a local file with no access level validation performed. If the access level requested is not within the range of 0-7, the request will be processed as an invalid request rather than a security violation.

4.10.1.1 USER CHANGE OF FILE ACCESS LEVEL.

During the course of job processing, the user may use the SETFAL (Set File Access Level) command or macro to raise or to lower the access level of a local file. This command may not be used for direct access permanent files. The SETFAL command is described in Section A.3.3.3.

The new access level of the file must be valid for the job (valid for the user and within the job access limits) and valid for the device on which the file resides (within the device access level limits).

Any user may use the SETFAL to raise the access level of a local file, however permission is required to lower the access level of a file.

An invalid attempt to change the access level of a file on a secured system using the SETFAL command will be processed as a security violation.

4.10.1.2 SYSTEM ADVANCE OF FILE ACCESS LEVEL.

When a user writes to a local file which has a lower access level than the level of the user's job, the system will raise the access level of the file to the access level of the job and the file access level will remain at the new access level (Security *-Property Rule). If the access level of the file's resident device will not permit the new access level, the write attempt will be processed as a security violation.

This process will not take place if the user has write-down privilege or if the job has an SSJ= entry point or Subsystem ID.

There is no corresponding mechanism to dynamically lower the access level of a file; this will be done only by use of the SETFAL command.

4.10.2 INDIRECT ACCESS PERMANENT FILES.

On both secured and unsecured systems, the security access level of an indirect access permanent file is the access level of the local file from which is it created using the SAVE or the REPLACE command. The security access categories of an indirect access permanent file will be set to the current access category set of the job when the file is SAVEd or REPLACEd.

On a REPLACE of an existing file or an APPEND, if the local file access level is greater than the permanent file access level, write-down privileges are required.

When an indirect access permanent file is assigned to a job with the GET or OLD command, the initial access level of the local copy of the permanent file is set to the access level of the permanent file. Thereafter, the local copy of the file will be treated as a local mass storage file. On a secured system the access level must be validated for the user and within the job access limits. Also, the permanent file access categories must be a subset of the current access category set of the job. The file will not be assigned and the request will be processed as a security violation if these conditions are not met. If the request was from an alternate user's catalog, however, the request will be processed as a File Not Found error condition.

The access levels and categories of an indirect access permanent file may be changed by the owner of the file using the SETPFAL and SETPFAC commands. On a secured system the new access level must be valid for the user, within the job access limits, and valid for the device on which the file resides. New access categories must be a subset of the current access category set of the job.

4.10.3 DIRECT ACCESS PERMANENT FILES.

On both secured and unsecured systems the security access level of a direct access permanent file is the access level of the user job creating the file. The security access categories will be set to the current access category set of the job when the file is DEFINEd.

If the file exists as a local file at the time it is DEFINEd, the permanent file access level will be set to the local file access level. If this level is lower than the job access level the user must be validated for write-down privilege.

4.12 SYSTEM MODIFICATION.

In order to prevent unauthorized modification of the operating system on a secured system, SYSEDIT will only be allowed from system origin jobs with security administrator privilege.

4.13 PERMANENT FILE PASSWORD EXPIRATION.

When a user creates or changes a permanent file password, the file password will have an expiration date associated with it, recorded in the file catalog entry. On or after that date the file password will no longer be valid for alternate user access and the file will accessible only by the owner of the file.

Normally the expiration date will be generated by the system using a default expiration term when the password is created or changed; however, if validated, the user may specify an expiration date or term on the permanent file command which creates or modifies the file password.

4.14 PERMANENT FILE PERMIT EXPIRATION.

A user may specify an expiration date or term for PERMITted user access using the XD or XT parameters on the permanent file PERMIT statement or macro. On or after the specified date, the permit will function as a NULL permit; that is, the designated user will no longer be able to access the file in any mode.

4.15 MEMORY STORAGE PROTECTION.

An IPRDECK option will be provided to cause central and extended memory to be cleared whenever it is released from a job. The result of selecting this option is that when a job rolls out or completes no residual data is left from the job in central or extended memory. See Section A.3.1.1 for the format of the IPRDECK entry.

4.16 MASS STORAGE OVERWRITE.

The OVWRITE utility and CIO function provides a means for the user to clear or declassify mass storage file space. In this context, to clear means to overwrite with zeroes, to declassify means to overwrite first with binary zeroes, then with binary ones, then with a pattern of alternating binary ones and zeroes.

Due to the mass storage allocation mechanism in NOS, this capability is not necessary; it is not possible for a job to read mass storage that has been released by any job (even by the same job).

The area of mass storage cleared by this operation includes only that space currently used by the file (up to the EOI sector). Space that has been released (for example by a REWIND followed by a write) is not accessible and cannot be cleared.

OVWRITE will be available on both secured and unsecured systems. The OVWRITE command is described in Section A.3.3.1.

4.17 PERMANENT FILE AND QUEUE UTILITIES.

Access levels will be added as selection criteria for all permanent file and queue utilities. Either a range or a single level may be selected. See sections 6.40 and 6.41 for descriptions of the new parameters on these utilities, and the restriction that will apply in a secure system to each utility.

4.18 PRINTED OUTPUT SECURITY.

BATCHIO will control the output of secure data when the system is in a secure mode by the following means:

1. Restricting output to unit record equipment with appropriate access levels.

2. Identifying the access level of printed output on the standard system banner page.

3. Holding output in the queue for special handling, if above an operator defined access level.

4.18.1 SECURED UNIT RECORD EQUIPMENT.

Equipment access levels apply to unit record equipment as well as other system equipment. The access level limits of a unit record device define the highest and lowest access levels of data which may be transmitted to or from the device.

The access level limits of unit record equipment is defined in the equipment EST entry and will be displayed on the console I-Display.

4.18.2 SECURE OUTPUT IDENTIFICATION.

Two methods are provided for the identifying secure printed output;

(1) display of file access level in the standard banner page header, and

(2) optional, additional classification identification preceding and/or within the output data as special headers and/or page headings and footings.

4.18.2.1 STANDARD BANNER PAGE HEADER.

An additional field of file access level identification will be included in the standard banner page header when the system is in secured mode. This line will not be included when the system is in unsecured mode. See Section A.4.7 for the banner page header format.

4.18.2.2 OPTIONAL ADDITIONAL IDENTIFICATION.

The SECHDR utility provides a means of identifying printed output with either or both of two identifier types printed with the output data. The first type consists of separate security identification banner pages printed before the first page of output data and after the last page of output data. The second type consists of page headings and footings printed at the top and bottom of each page of output.

In order to use the optional identifiers, the user must first pass the output data throught the SECHDR utility before routing the file to the output queue. See Section A.3.3.2 for a description of the SECHDR command.

4.18.3 OUTPUT QUEUE SPECIAL HANDLING LEVEL.

Installations may set an output queue special handling level on a secured system. A file which enters the output queue at an access level equal to or greater than the output queue special handling level will be held in the output queue until the operator releases the file for output.

The output queue special handling level may be set either by the OQSH IPRDECK entry or by the OQSH console command. A change in the output queue special handling level or to the access level limits of a unit record equipment will not affect a file currently being processed by BATCHIO. Raising the OQSH level will automatically release files that were previously prevented from printing.

The OQSH IPRDECK or console entry will be recognized when the system is in the unsecured mode but will have no affect. See Section A.3.1.3 for the format of the OQSH command.

Files held in the output queue due to the output queue special handling level can be explicitly released by the operator. See Section A.3.2.2 for the format of the RELEASE operator command.

4.19 ON-LINE DIAGNOSTICS.

Validation privileges (security validation word bit COLD) will be required to run any on-line diagnostics. This will be enforced by CVL. No other restrictions will be placed on running diagnostics on a secure system.

4.20 PRIVILEGED PROCESSES.

Programs loaded from the system library containing active SSJ= entry points and Subsystems, as identified by Subsystem ID, will have the following privileges:

1. Downgrading job access level.
2. Downgrading file access levels.
3. Writing-down.

These privileges will permit SSJ= jobs and subsystems to have job access levels and file access levels in accordance with the needs of their system functions without constraint by the validations of the user for whom they are executing.

4.21 SECURITY VIOLATION PROCESSING.

When a security violation is detected, the following steps will be performed by the detecting process and by the system:

1. Set the job error flag to SVET (detecting process).

2. Issue an Accounting Dayfile message describing the violation (detecting process).

3. Abort the job without EXIT or REPRIEVE processing and decrement the user security count in the validation file (1AJ). The current system does this already.

5.0 INTERFACE SPECIFICATIONS.

5.1 VALIDATION FILE ENTRY.

		5 4 3 2 1 9876543210987654321098765432109876543210987654321
ACCN	0	User number | User index
APSW*	1	Batch password | Expiration date
APRN	3	User proc file | SP | Reserved
ASHN	3	Shell program name | Control bits
APWI*	4	Terminal password | Expiration date
ASVW*	5	Val bits | Level bits | Category bits
APJN	6	Project number
APJ1	7	Project number
ACGN	10	Charge number
AHMT	11	Resource access controls
AHDS	12	Resource access controls
AAWC	13	Access control word
ATWD	14	Terminal control | Create date | Last mod date
	15	Reserved for installation
	16	Reserved for installation

*Indicates new or modified.

Note: The validation file format is being revised. See Reference 9.

5.1.1 WCPD_ASVW (5)

12/ User Validation bits:

Bit	Description
59	Security Administrator validation
58	May perform CE functions
57	May assign password expiration date
56	May assign PF password expiration date
55	May downgrade job access level
54	May downgrade file access level
53	May write-down
52	May write unlabeled tapes
51-48	Reserved for system

12/ Access level validation bits:

Bit	Description
47-44	4/ Reserved
43	Validated for level 7
42	Validated for level 6
41	Validated for level 5
40	Validated for level 4
39	Validated for level 3
38	Validated for level 2
37	Validated for level 1
36	Validated for level 0

36/ Access category validation bits:

Bit	Description
35-32	4/ Reserved
31-0	Bit 2**n set validates access to category n (n = 0,...,31)

5.2 PF CATALOG ENTRY.

		5 4 3 2 1 9876543210987654321098765432109876543210987654321
FCFN	0	File name ! User index
FCLF	2	File length ! !First track! First sec
FCRI	2	Permit random index ! Creation date and time
FCAC	3	Access count ! Modification date and time
FCCT	4	Cat.! Mode! ER ! DN ! Last access date time
FCKD	5	! Control mod date and time
FCRS	6	
FCPW*	7	File password ! Expiration date
FCAF	10	Alternate storage
FCAL*	11	Reserved ! Access level and categories
FCX1*	12	Reserved for CDC
FCX2*	13	Reserved for CDC
FCX3*	14	Reserved for CDC
FCX4*	15	Reserved for CDC
FCUC	16	User control word
FCIN	17	Installation word

* Indicates new, modified, or relocated.

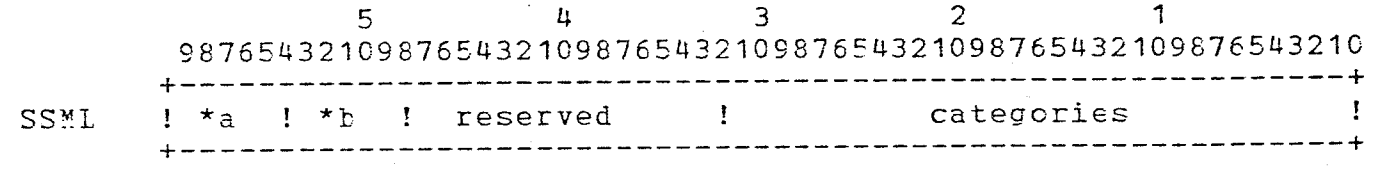
Word FCAL:

21/ Reserved
3/ File Access Level
4/ Reserved
32/ Bit 2**n set indicates file inclusion in category n
(n = 0,...,31).

5.3 CENTRAL MEMORY RESIDENT (CMR).

5.3.1.1 WORD SSML.

The operating system security mode, output queue special handling level and system access categories are contained in word SSML.



*a	6/Output queue special handling level.
*b	6/Operating system security mode.
categories	32/ System Access Categories.

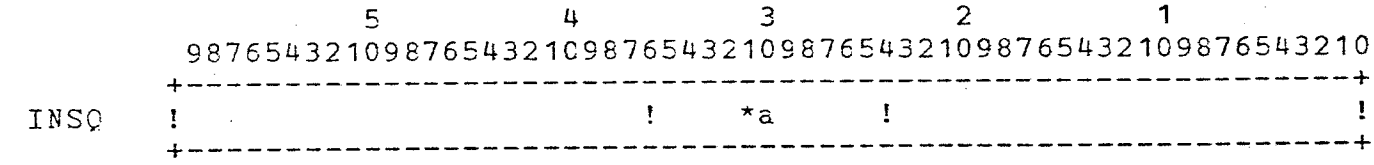
5.3.1.2 WORD SSTL.

The Security unlock and Memory Clearing bits will be added to word SSTL. The Unlock bit is moved.

Bit 58	Memory Clearing (0 = Enabled)
Bit 57	Security Unlock Status (1 = Unlocked)
Bit 56	Unlock Status (1 = Unlocked)
Bit 13	Reserved

5.3.2 QUEUE FILE TABLE (QFT).

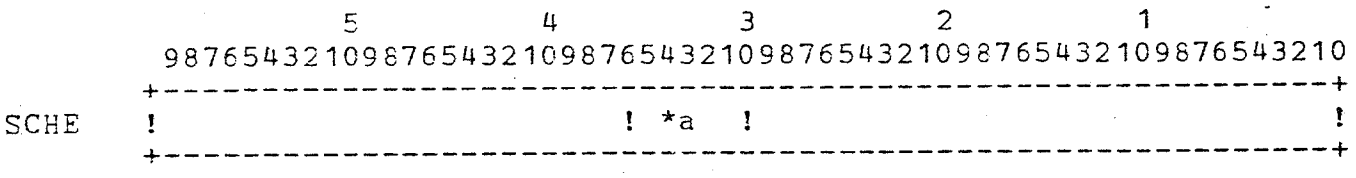
The security access level of a queued file are stored in word INSQ (2) of the QFT. For INPUT files, the job access level upper limit is also defined.



*a	5/ Reserved 1/ Release bit 3/ File Access level 3/ Job Access level Upper Limit (Input files only)

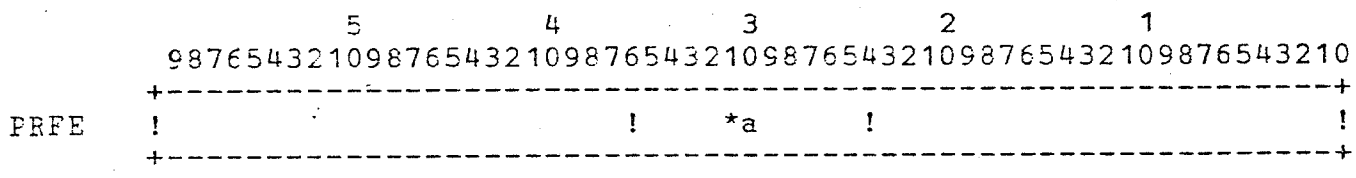
5.3.3 EXECUTING JOB TABLE (EJT).

Word SCHE(1) of the EJT entry will contain the job termination in progress flag. This flag is being moved from Control Point Area word ECJW.



*a 1/ Jcb in No Rerun status.
1/ Jcb termination in progress.
4/ Reserved.

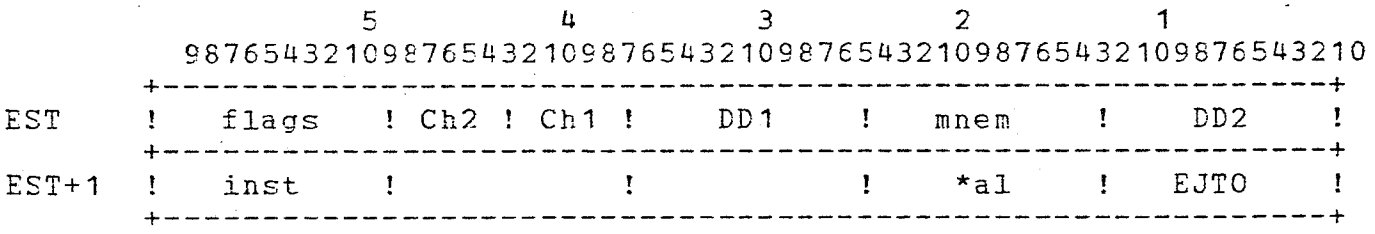
Word PRFE (2) of the EJT entry for each job in the system contains the Job Access Level Limits for each jcb in the system.



*a 6/ Reserved
3/ Jcb Access Level Lower Limit
3/ Job Access Level Upper Limit

5.3.4 EQUIPMENT STATUS TABLE (EST).

The following describes the format of the EST entry as defined by the EST expansion project GID (5) and shows the equipment access level limit field.



EST Word 0:

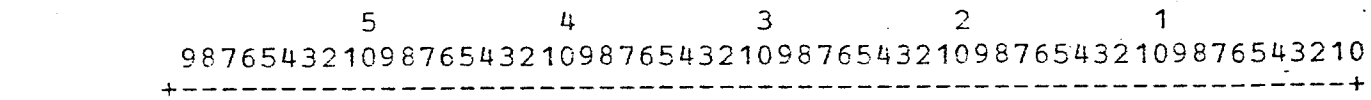
flags	12/	Device dependent flags.
Ch2	6/	Channel 2 assignment.
Ch1	6/	Channel 1 assignment.
DD1	12/	Device dependent.
mnem	1/ 11/	On-Off bit. Equipment mnemonic.
DD2	12/	Device dependent.

EST Word 1.:

inst	12/	Installation area.
*al	6/ 3/ 3/	Reserved. Access level lower limit. Access level upper limit.
EJTO	12/	EJT Ordinal.

5.3.5 MASS STORAGE TABLE (MST).

Word PFGL (4):



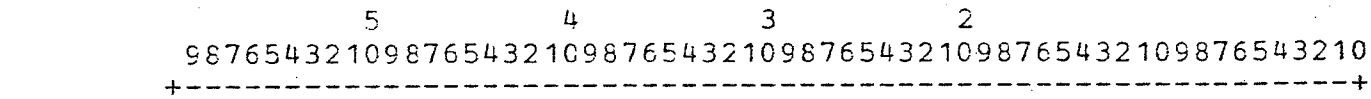
DN 6/ Device Number.

AL 3/ Device access level lower limit.
3/ Device access level upper limit.

UD 6/ Multi-Unit Drive Indices.

5.3.6 SERVICE CLASS CONTROL TABLE.

Each of the origin type words in the SCT will contain the origin type access level limits.

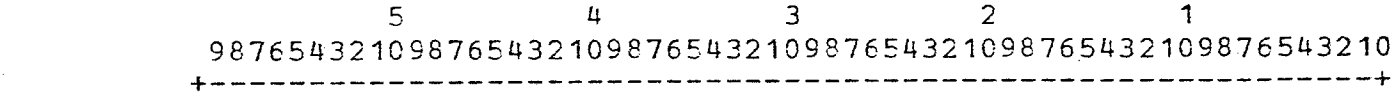


*a 3/ Origin type access level lower limit.
3/ Origin type access level upper limit.

This table is defined in the User Service Class Assignment GID (8).

5.4 FNT/FST ENTRY.

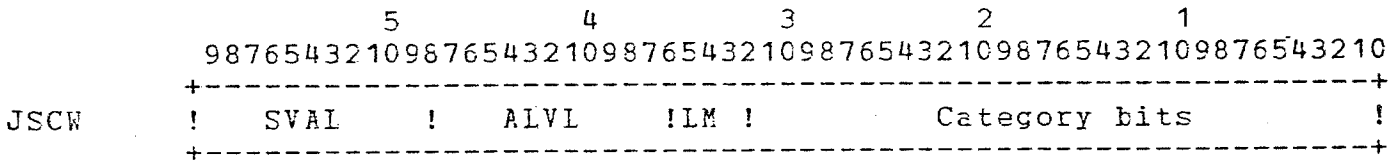
Word FUTL (2) of the FNT entry for each local file contains the file access level.



*a 3/ Reserved.
3/ File Access Level.

5.5 CONTROL POINT AREA.

5.5.1 WORD JSCW.



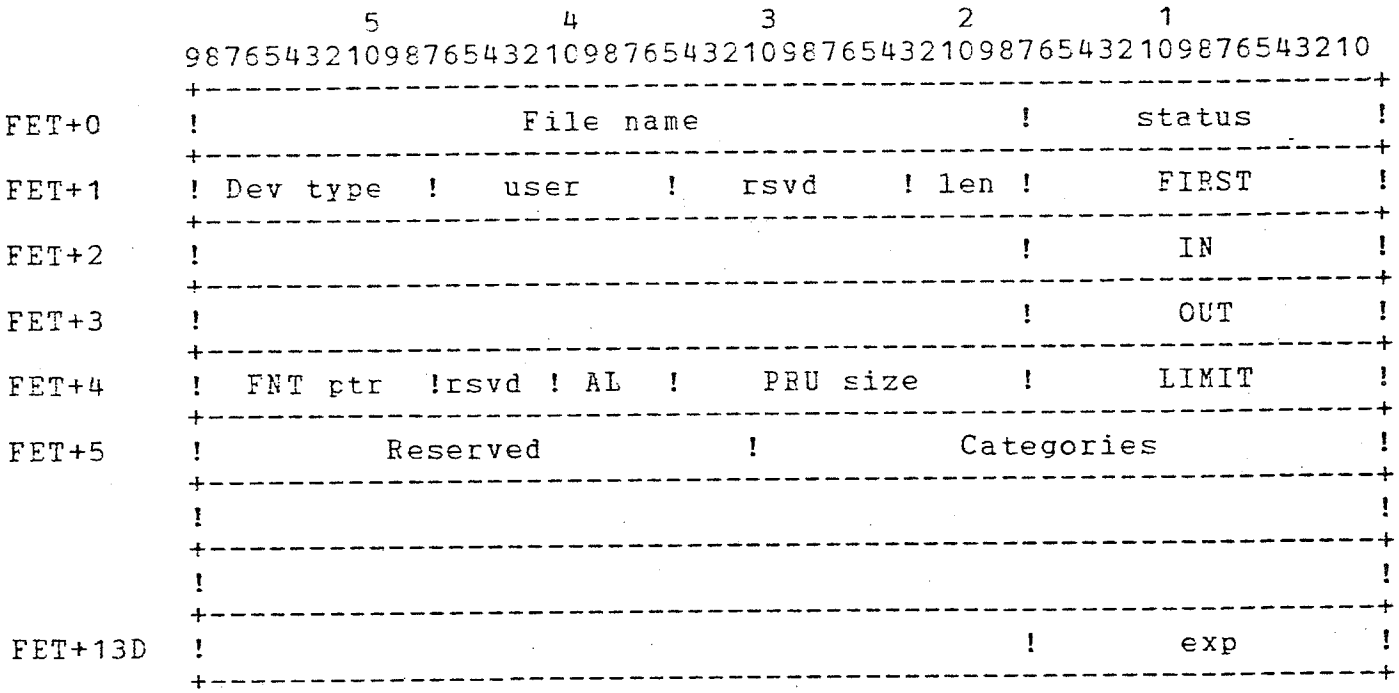
SVAL 12/ Security privilege validation bits

Bit	Description
59	Security administator.
58	On-Line diagnostics.
57	May assign user password expiration date.
56	May assign permanent file password expiration date.
55	May lower (downgrade) job access level.
54	May lower (downgrade) file access level.
53	May write to lower level (write-down).
52	May write unlabeled magnetic tapes.
51-48	Reserved.

ALVL 3/ Job Access Level.
1/ Reserved.
8/ Access Level Validation bits.

LM 3/ Job Access Level Limit.
1/ Reserved.

5.6 FILE ENVIRONMENT TABLE (FET).



Word FET+1:

user 12/ User processing bits:

Bit	Description
39	If set, file access level to be taken from or returned to file access level field in FET+4 depending upon function being processed.

Word FET+4:

AL 9/ Reserved
3/ File Access Level

Word FET+5:

Note: This description and use of FET+5 applies only to the SETPFAC PFM function.

Categories 32/ Category bits:
Bit 2**n set indicates request to set bit 2**n in the PF Catalog entry (n = 0,...,31).

Word FET+13D:

Note: This description and use of FET+13D applies only to PFM requests.

exp 18/ Password or PERMIT expiration date or term:

If bits 12-17 are zero, bits 0-11 contain the password expiration term in days to be added to the current date to calculate the password or PERMIT expiration date.

If bits 12-17 are nonzero, bits 0-17 contain the packed password expiration date.

5.7 QAC PARAMETER BLOCK.

5.7.1 SELECTION FLAGS - WORD 8.

* Selection flag bit 13 will be used as the access level selection flag. If this bit is set, QAC will use the access level field contents as selection criteria.

5.7.2 SELECTION CRITERIA - WORD 10D.

Security access level selection criteria are added to selection criteria word 10D.

Word Format:

```
                5         4         3         2         1
         9876543210987654321098765432109876543210987654321098765432 10
        +-----------------------------------------------------------+
addr+9  !      SLID       !      DLID       ! AL  !      ALID       !
        +-----------------------------------------------------------+
```

SLID 18/ Creation logical ID.

DLID 18/ Destination logical ID.

AL 3/ Access level lower bound.
3/ Access level upper bound.

ALID 18/ FWA of alternate ID list.

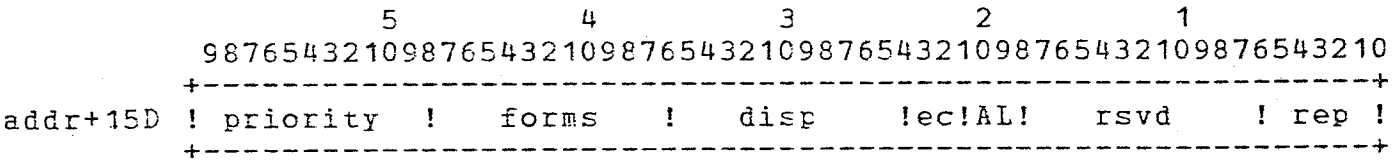
5.7.3 ALTER FLAGS - WORD 13D.

Bit 8 of the alter flags field will be used to indicate altering of security access level on selected files is desired.

5.7.4 ALTER FUNCTION - WORD 16D.

Security access level is added to the *ALTER* function portion of the QAC parameter block, word 16D.

Word Format:

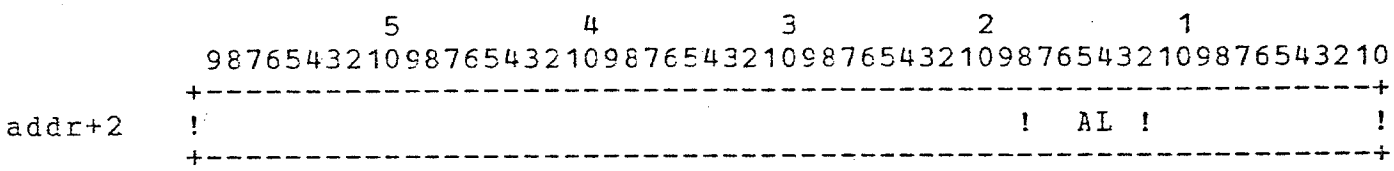


AL New access level for the selected files.

5.7.5 PEEK REPLY BLOCK - WORD 3.

The access level of an executing job or queued file will be returned to the PEEK reply block.

Word Format:



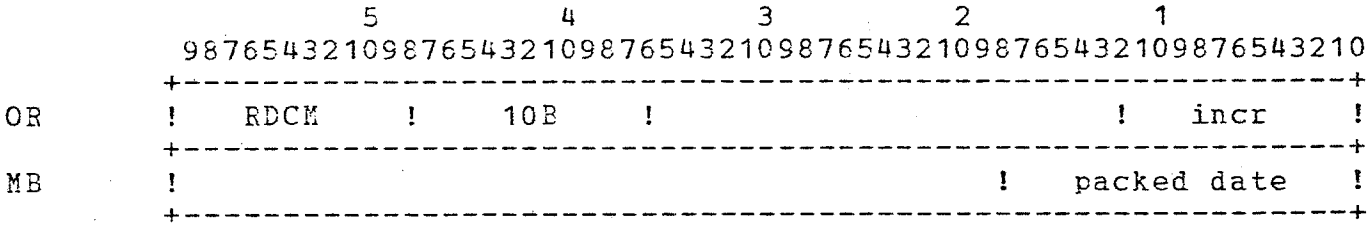
AL Access level of executing job or queued file.

5.8 MONITOR FUNCTIONS.

5.8.1 REQUEST DATA CONVERSION - RDCM.

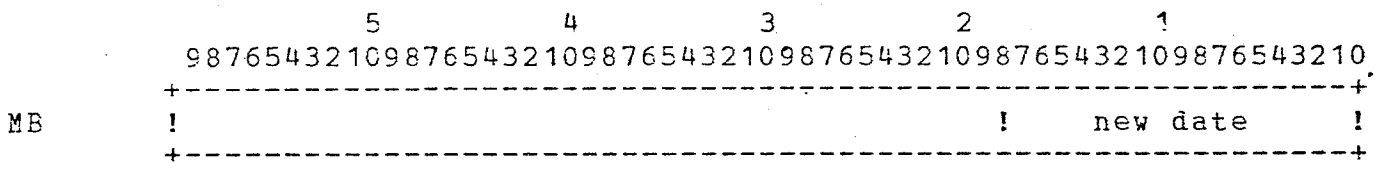
Subfunction 10 - Calculate Packed Date

RDCM function code 10 enables a PP tc have a packed date calculated using a packed date base plus an increment.



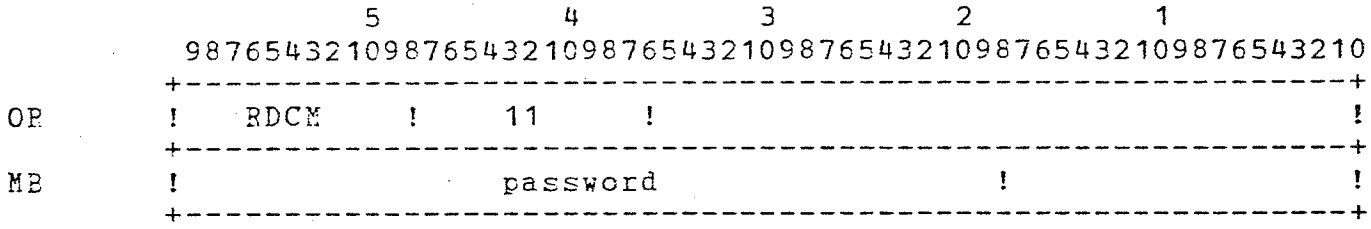
incr 12/ Increment to be added to the packed date in the message buffer.

Reply:



Subfunction 11 - Encrypt Password

RDCM subfunction 11B will encrypt a 42-bit password and return the encrypted value tc the message buffer.



Reply:

```
                5         4         3         2         1
 9876543210987654321098765432109876543210987654321098765432109876543210
+-------------------------------------------------------------------+
!           encrypted password                      !                 !
+-------------------------------------------------------------------+
```

ME

5.8.2 RESERVE TRACK CHAIN - RTCM.

```
                5         4         3         2         1
 9876543210987654321098765432109876543210987654321098765432109876543210
+-------------------------------------------------------------------+
!   RTCM    !   c*eq    !   tttt    ! AL  !      ssss               !
+-------------------------------------------------------------------+
```

OR

RTCM 12/ RTCM Function code.

c*eq 1/ Equipment checkpoint flag.
11/ Equipment number.

tttt 12/ Track or Device selection.

AL 1/ Access level selection flag.
2/ Reserved.
3/ Access Level requested.

ssss 1/ Reserved.
17/ Sector Count Requested.

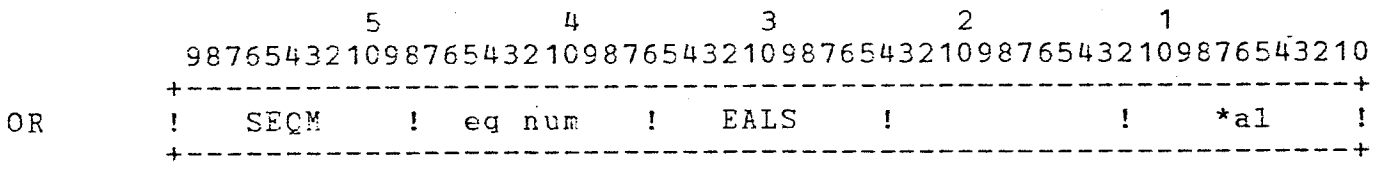
Reply:

* Byte 3 of the output register will contain the status of the request if it is rejected (byte 4 = 0). The following values are defined.

1 track limit, no tracks available
2 access level selection not available

5.8.3 SET EQUIPMENT PARAMETERS - SEQM.

Subfunction code EALS (17) will set the equipment access level limits in the equipment EST entry.

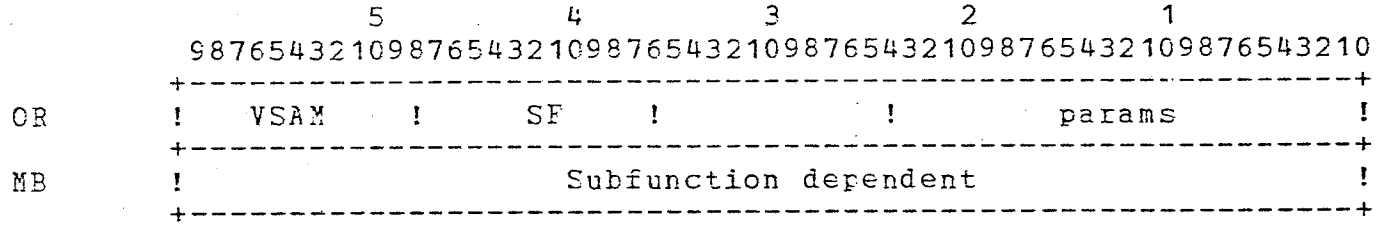


EALS — SEQM Subfunction code 17.

*al — 6/ Unused
3/ Access level lower limit.
3/ Access level upper limit.

5.8.4 VALIDATE SECURITY ACCESS - VSAM.

The VSAM monitor function is used to validate user access to classified resources and to set user security parameters.



SF — 12/ Subfunction code.

params — 24/ Parameters dependent upon subfunction.

Subfunction Codes:

Code	Function	Description
0	VJAS	Set Job Access Level.
1	VSFS	Set File Access Level.
2	VAES	Validate Access Level for Equipment.
3	VAJS	Validate Access Level/Categories for Job.
4	VJCS	Validate Job Creation Parameters.

Subfunction VJAS (0) - Set Job Access Level

VSAM subfunction VPJS validates the specified access level for the calling job and, if valid, sets the access level in the control point and EJT entry for the calling job.

```
        +-------------------------------------------------------+
OR      !   VSAM    !   VJAS    !             !          AL     !
        +-------------------------------------------------------+
```

AL Requested Access Level.

Reply

* Byte 1 of the output register will be set to zero if the access level was valid, nonzero, if the access level was not valid.

Subfunction VSFS (1) - Set File Access Level.

VSAM subfunction VSFS validates the specified access level for the specified file and, if valid, sets the access level in the FNT entry for the file. The file must be set busy before calling VSAM/VSFS.

```
        +-------------------------------------------------------+
OR      !   VSAM    !   VSFS    !             !    FA    !  AL  !
        +-------------------------------------------------------+
```

FA NFL address of FNT entry for file.
AL Requested Access Level.

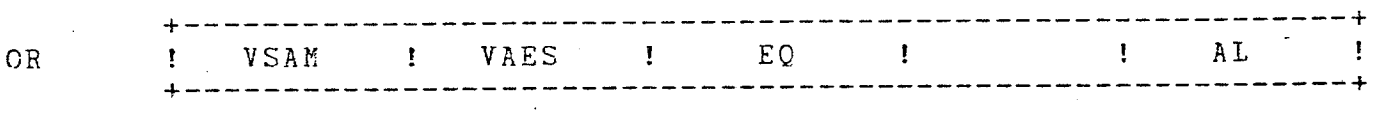
Reply

* Byte 1 of the output register will be set zero if the access level was valid, and to nonzero if the access level was not valid.

* The PP will be hung if the FNT entry specified was not set busy before the call.

Subfunction VAES (2) - Validate Access Level for Equipment.

VSAM subfunction VEQS validates that the specified access level is within the equipment and device limits for the specified equipment.



EQ EST ordinal of equipment.

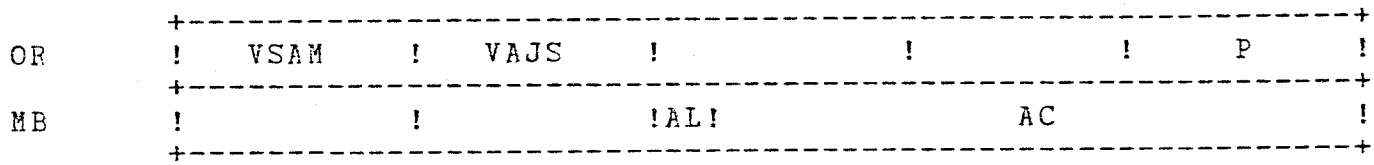
AL Requested access level.

Reply

* Byte 1 of the output register will be set to zero if the specified access level is valid for the specified equipment, and to nonzero if it is not valid.

Subfunction VAJS (3) - Validate Access Level/Categories for Job.

VSAM subfunction VAJS validates a specified access level and/or access category set against the levels and categories currently valid for the calling job.



P Processing Option:
1 - Access level only
2 - Access categories only
3 - Both access level and categories

AL Access Level.

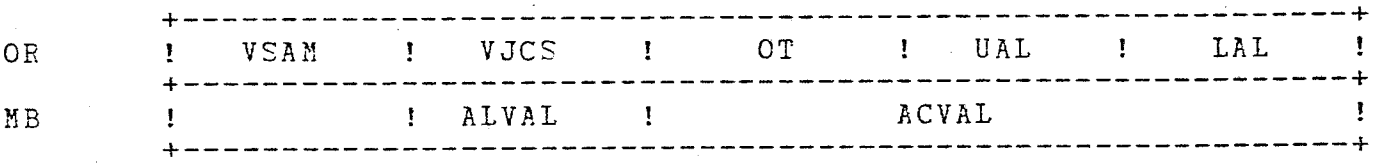
AC Access Categories.

Reply

* Byte 1 of the output register will be set to zero if the specified access level and/or access categories are valid, and to nonzero if they are not valid.

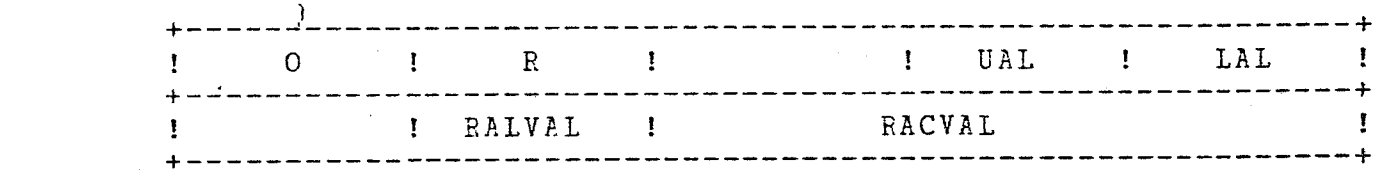
Subfunction VJCS (4) - Validate Job Creation Parameters.

VSAM subfunction VJCS validates that a new job can be created with the specified origin type, the specified validations, and the specified upper and lower access level limits. The function will return the restricted sets of access levels and categories that will be valid for the job.



OT Origin type of job to be created.
UAL Upper limit on access levels for job. (=4000B if default is to be used. This is the restricted lower access level limit.)
LAL Lower limit on access levels for job.
ALVAL Access level validation bits; from validation file entry.
ACVAL Access category validation bits; from validation file entry.

Reply



R Zero if job may be created.
RUAL Restricted upper access level limit.
RLAL Restricted lower access level limit.
RALVAL Restricted set of access level validation bits.
RACVAL Restricted set of access category validation bits.

5.9 NETWORK CONFIGURATION FILE (NCF).

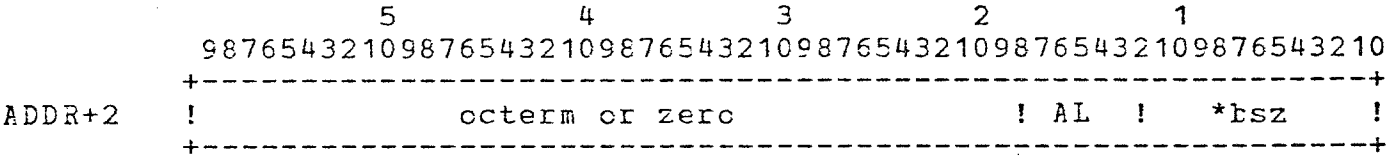
The Network Configuration File will contain a new 4-bit Line Access Level Limit parameter in each line definition. This parameter will be stored in the NCB as an FN/FV pair. This modification will be implemented by Network Host Products.

5.10 NAM TERMINAL-TO-APPLICATION CONNECTION REQUEST.

The NAM Terminal-to-Connection Connection-Request (CON/REQ/R) will contain the Access Level Limit of the terminal's communication line from the Network Configuration File and will contain the terminal user's Validation File entry word ASVW.

These modifications are to be implemented by Network Host Products.

5.10.1 REQUEST WORD 3.

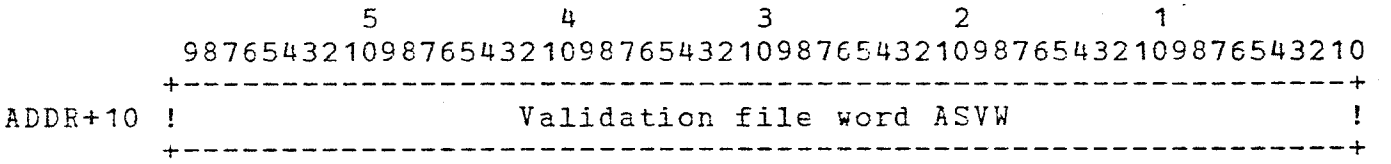


AL 6/ Line Access Level from NCF.

*bsz 11/ Block Size.
1/ zero.

5.10.2 REQUEST WORD 11D.

Request Word 11 decimal of the CON/REQ/R Supervisory message will be added and will contain word ASVW from the user's validation file entry.



6.0 INTERNAL DESIGN.

6.1 COMMON DECKS.

6.1.1 NOSTEXT (PPCOM).

1. Add field definitions as defined in section 5.3.

2. Add VSAM to the table of monitor functions. This function must be performed in the active CPU.

6.1.2 NOSTEXT (CPCOM).

The following macros are new or are modified for Multi-Level Security. See Appendix A for the formats.

6.1.2.1 OVWRITE Macro.

The OVWRITE macro will issue CIO function 244 to process the CIO OVWRITE function.

Macro Processing:

* If parameter "op" is the letter "X", set the skip count field to 1.

* Issue CIO function 244 with recall if "r" is specified.

* Issue CIO function 244 without recall if "r" is not specified.

6.1.2.2 Permanent File Request Macros.

The XT parameter will be added (as the last parameter) to the SAVE, DEFINE, PERMIT and CHANGE macros, which will in turn specify that parameter on their call to the =3 macro. The XT parameter will be added (as the last parameter) to the =3 macro, which will set the value specified into bits 17-0 of FET+15B.

6.1.2.3 SETPFAC Macro.

The SETPFAC macro will issue PFM function 22 to change the access category set of a permanent file.

Macro Processing:

* Set bits 31-0 of "cat" into bits 31-0 of FET+5, if "cat" is specified.

* Call =3 to process PFM function 22, passing all other parameters on to =3.

6.1.2.4 SETPFAL Macro.

The SETPFAL macro will issue PFM function 23 to change the access level of a permanent file.

Macro Processing:

* Compare "a1", if present, to the micros defined in COMSMLS. If no match, use "a1" as the address of a word containing the new access level.

* Set bits 38-36 of FET+4 with access level from "a1", if specified.

* Call =3 to process PFM function 23, passing all other parameters to =3.

6.1.3 COMCMAC.

The following macros will be added by Multi-Level Security. The macro formats are documented in Appendix A.

6.1.3.1 GETJAL Macro.

The GETJAL macro will issue CPM function 116 to return the Job Access Level and Job Access Level Limits to the calling program.

6.1.3.2 GETSSL Macro.

The GETSSL macro will issue SFM function GSSF to return the System Security Mode and the Origin Type Access Limits to the calling program. Use of this macro is restricted to Subsystem and SSJ= programs.

6.1.3.3 GETUSV Macro.

The GETUSV macro will issue CPM function 120 to return the user security validation word JSCW from the Control Point Area. Use of this macro is restricted to Subsystems and SSJ= programs.

6.1.3.4 SETFAL Macro.

The SETFAL macro will issue LFM function 7 to change the access level of a local file.

Macro Processing:

* Compare "al" to the micros defined in COMSMLS. If no match, use "al" as the address of a word containing the new access level.
* Set the "sp" bit, bit 39D, in FET+1.
* Set the access level in the access level bits, bits 38-36, of FET+4.
* Issue LFM request 7.

6.1.3.5 SETJAL Macro.

The SETJAL Macro will issue CPM Function 117 to change the access level of the calling job.

6.1.3.6 GETEAL Macro

The GETEAL Macro will issue SFM function GEAF to return the equipment access limits of a specified equipment. Use of this macro is restricted to Subsystems and SSJ= programs.

6.1.4 COMCBAN.

COMCBAN is a new common deck that will create a banner line of up to 8 large characters from a supplied string. The character and line formats will be the same as currently used by OBP when creating the job banner page. The banner line will be created in a caller specified buffer; trailing blanks will be ignored. This common deck will be called by SECHDR when writing security banner pages.

6.1.5 COMCECP.

COMCECP will encrypt the user password before storing it into the validation file. The program uses a polynomial scrambling algorithm to provide a one-way encryption of the user password. This common deck will be called by MODVAL when entering user passwords. An equivalent section of code in CPUMTR will be used by the RDCM subfunction. This will be called by PP programs that need to validate user entered passwords.

6.1.6 COMCFCE.

COMCFCE will be changed to format the PFC entry as described in section A.4.4.5. The password expiration date and access level will be added.

6.1.7 COMCPFS.

Add a routine to COMCPFS to determine whether or not a file meets the selection criteria as specified by the IA/UA security parameters, as well as the UI, PF, and OP=I or CP=D parameters. All of the PF utilities will call this routine.

6.1.8 COMCVAC.

COMCVAC is a new common deck that will determine if a supplied access level name or access category name is valid. The possible values for access levels and categories are defined in COMSMLS. If the supplied name is valid, COMCVAC will return the corresponding value (0-7 for access level, 0-31 for access category). Options will be provided to assemble only the tables of access levels and categories; this will be used by programs that need to convert a level number into a name.

6.1.9 COMCVDT.

COMCVDT is a new common deck that will validate a supplied date in the form YYMMDD or a time in the form HHMMSS. It will verify that the year (YY) is greater than 70, that the month (MM) is between 1 and 12, and that the day (DD) is a valid value for the specified year and month. If a time is specified it will verify that the hour (HH) is less than 24, the minute (MM) is less than 60, and that the second (SS) is less than 60. This common deck will be called by PFS, PFILES and MODVAL.

6.1.10 COMCVQF.

COMCVQF will be changed to check security access levels as selection criteria.

6.1.11 COMDDCM.

Options will be added to COMDDCM to allow restriction on the memory locations to be displayed. These will be used by DSD to restrict central memory displays to CMR on a secured system (unless security unlock status) and by DIS to restrict displays to the job's field length in all cases.

6.1.12 COMPVAC.

COMPVAC is a new common deck that will determine if a supplied access level name or access category name is valid. The possible values for access levels and categories are defined in COMSMLS. If the supplied name is valid, CCMCVAC will return the corresponding value (0-7 for access level, 0-31 for access category). Options will be provided to assemble only the tables of access levels and categories; this will be used by programs that need to convert a level number into a name.

6.1.13 COMSACC.

The new validation file entry format as described in section 5.3 will be documented and new field symbol definitions added. See section 6.36 (MODVAL) for the new symbol names.

New mnemonics are defined for user password expiration term control:

APXL — User password expiration term limit in days. Valid values range from 1 to 7777B. This value establishes the upper limit on the expiration term that the user may specify using the XT parameter on the PASSWOR control statement.

The release value of APXL is 7777B.

APXT — Defines the default user password expiration term in days. This is the value that will be assumed when the user does not specify an expiration term parameter on the PASSWOR statement and when a new password is set for a user name by MODVAL. The value ranges from 1 to 7777B.

APXT must be defined to be less than or equal to APXL.

The release value of APXT is 7777B (non-expiring).

6.1.14 COMSBIO.

Add equipment access level limits to the Buffer Point Area as defined in section 5.11.

6.1.15 COMSCIO.

Add OVWRITE and CVWRITE RETURN function codes (244 and 254).

6.1.16 COMSCPS.

Add new VSAM monitor function subfunction codes as defined in section 5.10.5.

Add SEQM monitor function subfunction code EALS (17).

6.1.17 COMSLSD.

Add new error code (STSV - Security Violation) to the list of error codes processed only by MSM.

6.1.18 COMSMLS.

COMSMLS is a new common deck that defines the Multi-Level Security parameters and options.

Redefining any of the access level or access category micros will require reassembly of all programs referencing them.

6.1.18.1 Access Level Micros.

The Access Level Micros define the symbols used by the system to reference access levels. These symbols are used by all external interfaces: user commands, operator entries/displays, MODVAL directives, etc. The associated numeric values are only used internally by the system.

Micro	Value	Meaning
ALM0	"LVL0"	Access level 0.
ALM1	"LVL1"	Access level 1.
ALM2	"LVL2"	Access level 2.
ALM3	"LVL3"	Access level 3.
ALM4	"LVL4"	Access level 4.
ALM5	"LVL5"	Access level 5.
ALM6	"LVL6"	Access level 6.
ALM7	"LVL7"	Access level 7.

6.1.18.2 Access Category Micros.

The Access Category Micros define the symbols used by the system to reference access categories.

Micro	Value	Meaning
ACM00	"CAT00"	Access Category 00.
.	.	.
.	.	.
.	.	.
ACM31	"CAT31"	Access Category 31.

6.1.19 COMSMTX.

A new error code will be defined for *DSD* display. This will be used when the equipment where the tape is mounted will not allow the access level of the assigned file.

6.1.20 COMSPFM.

Add documentation and symbols for the following:

* New PFC fields as defined in section 5.2.

* New permit entry fields as defined in section 5.12.

* New FET fields as defined in section 5.6.

* New PFM functions SETPFAC (22) and SETPFAL (23).

New symbols are defined for permanent file password and permit expiration term control:

FPXL — Permanent file or permit expiration term limit in days; valid values range from 1 to 7777B. This value establishes the upper limit on the password or permit expiration term which a user may specify on a permanent file request.

The release value of FPXL will be 7777B.

FPXT — Default permanent file or permit expiration term in days; valid values range from 1 to 7777B. FPXT must be defined as less than or equal to FPXL.

The release value of FPXT will be 7777B (non-expiring).

6.1.21 COMSPFS.

Add description of access level selection parameters as defined in section 6.40.

6.1.22 COMSPFU.

Update documentaticn of PFDUMP Tape Iabel Fcrmat to reflect current parameters.

6.1.23 COMSQAC.

Add new selection flags and fields as defined in section 5.7.

6.1.24 COMSQFS.

Add description cf access level selecticn parameters as defined in section 6.41.

6.1.25 COMSRSX.

The file access required fcr a tape request will be passed to DSD in the preview buffer. Bits 15-17 of the second wcrd of the entry will be used.

6.1.26 COMSSFM.

Add new SFM functicn codes as defined in section 6.14.

6.1.27 COMSSRU.

Add PF Increment values for SETPFAC and SETPFAL PFM functions.

6.1.28 COMS1DS.

Add function code VSAF - Validate Security Administrator. This function will be called in response to the UNIOCK,usernam,password. operator command used to set security unlock status at the console.

6.1.29 COMTBAN.

COMTBAN will contain the large character definitions used by OBP and COMCBAN.

6.2 CPM.

CPM will process new definitions of the following current requests.

Code	Function	Descriptions
021	SETUI	Set User Index.
040	VALID	Validate User Name.
056	VALID	Validate User.

The following new function codes will be added to CPM. These will be added to the Table of Function Code Processors, and the associated routines added to overlay 3CC (Loader/Miscellaneous Functions). All addresses of parameter and reply words will be checked for residing within the callers field length. If not, the job will be aborted with a CPM-ILLEGAL REQUEST error.

Code	Function	Description
116	GETJAL	Get Job Access Level.
117	SETJAL	Set Job Access Level.
120	GETUSV	Get User Security Validation.

6.2.1 SETUI (021).

The SETUI (021) function will require a SSJ= entry point as well as SYOT. An exception will be made if the user index is being set to 0; this will be allowed from non-SSJ= programs (i.e. SUI command).

6.2.2 VALIDATE USER NAME (040).

The following changes will be made to VALID (040) function processing.

Password validation processing must use the batch password from word APSW in the validation file. If the password expiration date from the validation file is not greater than the current date, the password is considered illegal. Since the password on the validation file is encrypted, the user specified password must be encrypted also before comparing them. Monitor function RDCM, subfunction 11, will be used for this.

User indexes greater than AUIMX will be accepted if the caller is system origin.

On a secured system, system origin jobs (including DIS jobs) without USER cards will be initiated with valid access levels equal to all levels within the system access limits, and valid access categories equal to all valid categories defined by the SECCATS IPRDECK entry. When such a job issues its first USER command, VSAM subfunction VCJS must be used to get the restricted access levels and categories which must be set in the Control Point Area.

6.2.3 VALIDATE USER (056).

Password validation must use the interactive password from word APWI in the validation file. Otherwise it is processed the same as function 40.

6.2.4 GETJAL (116).

The GETJAL function returns the job access level and access level limits to the calling program.

Processing:

* Return the job access level and access level limit in the format described in Section A.3.4.1.

6.2.5 SETJAL (117).

The SETJAL function is used to reset the job's current access level.

Processing:

* Validate the value of the access level parameter. If greater than 7, abort the job with a CPM - ARGUMENT ERROR diagnostic.

* Call monitor function VSAM, subfunction VSJS, to validate and set the specified access level. If this level is not valid for the job, process the request as a security violation.

* Issue the MJJA or MJJI Accounting Dayfile message as described in Section B.1.2.

6.2.6 GETUSV (120).

The GETUSV function returns Control Point Area word JSCW to the requesting program.

Processing:

* Validate that the requesting program has an SSJ= entry point or a subsystem ID. If it does not, abort the job with a *CPM - ILLEGAL REQUEST* diagnostic.

* Return Control Point Area word JSCW to the specified reply word.

6.3 DIS.

6.3.1 ABSOLUTE MEMORY

Remove all references to absolute memory displays. The '=' key will no longer toggle to absolute memory.

6.3.2 MEMORY STORAGE DISPLAYS.

Add an assembly option to COMDDCM to restrict memory displays to words within the callers field length, including negative field length. This common deck is used by the C, D, F and G displays. The other DIS displays that display memory (M,T,U,V) must be modified to also conform to this restriction.

Any words that are not within the users field length will be displayed as filled with display code asterisks to clearly indicate the out of range condition.

6.3.3 SECURITY VIOLATION PROCESSING

If a DIS job is aborted with a security violation (SVET error flag), DIS will currently remain active and allow the job to continue. This will continue to be true in an unsecured system. In a secure system, the job will be released from the system.

6.4 DSD.

6.4.1 CONSOLE DISPLAYS.

Security access levels will be shown on the following console displays if the system is in a secured mode. In all cases, the values will be the symbolic names defined in COMSMLS, not the corresponding octal level number. See section A.4.6 for the format of each display.

6.4.1.1 LEFT SCREEN HEADER.

The operating system access level limits (upper and lower bounds) will be displayed on the left screen header.

6.4.1.2 E, A DISPLAY.

The equipment access level limits (upper and lower bounds) for each mass storage, magnetic tape and unit record equipment in the EST will be displayed on the E, A display.

6.4.1.3 E, P DISPLAY.

The access level of the requested tape file will be added to the E,P display. This will be passed to DSD by RESEX in the preview buffer.

6.4.1.4 E, T DISPLAY.

The equipment access level limits for each tape equipment will be displayed on the E, T display.

6.4.1.5 I DISPLAY.

The equipment access level limits for each unit record equipment will be displayed on the I display.

6.4.1.6 J DISPLAY.

The job access level limits for each job from word PRFE of the EJT entry will be displayed on the J display.

6.4.1.7 Q DISPLAY.

The queued file access level limits from word INSQ of the QFT entry will be displayed on the Q display.

6.4.1.8 R DISPLAY.

The job access level limits from word PRFE of the EJT entry will be displayed on the R display.

6.4.2 SECURITY UNLOCK STATUS.

A new form of the UNLOCK operator command will be added to DSD to set security unlock status at the console. The format of this command will be UNLOCK, username, password.

The user name and password parameters will be passed to 1DS function VSAF through the DSD/1DS buffer in CMR. If 1DS determines that this user has security administrator privileges, the security unlock bit as well as the lock bit will be set in CMR word SSTL. If the user name is not properly validated, the operator will be informed. Security unlock status will be noted on the left screen header. See Section A.4.6.1 for the format.

A new parameter will be added to the ENTER macro, which defines syntax processing for all DSD commands. This parameter, SLOCK, will indicate that if the system is secured, security unlock status is required. If the system is unsecured, SLOCK will mean that a normal UNLOCK is required.

The following commands will be defined with the SLOCK parameter set:

Memory entry commands (central and extended)
ENGR
DEBUG
SECURES
SECUREQ
DIS,jsn
QDSPLAY

Memory displays (C,D,F,G,M) will only be allowed to display the Central Memory Resident area of central memory and the system table area of extended memory on a secured system unless the console is in security unlock status.

6.4.3 COMMANDS.

The following commands will be added to a new DSD overlay. See section A.3.2 for the formats.

6.4.3.1 SECURES.

This SECURES operator command will be identical to the IPRDECK SECURES entry. This command requires the console to be in security unlock status.

6.4.3.2 SECUREQ.

The SECUREQ operator command is used to change the access level limits of a unit record equipment. This command requires the console to be in security unlock status.

The following must be true for this command to be accepted.

The specified equipment mnemonic and EST ordinal must be defined in the EST as a unit record equipment (CP, CR, LP, LQ, IR, LS, LT).

Both upper and lower bounds must be specified and be valid names for access levels.

The associated value of the lower bound must be less than or equal to the associated value of the upper bound.

DSD will use the SEQM monitor function to change the EST access level limits.

6.4.3.3 OQSH.

The OQSH operator command will be identical to the IPRDECK OQSH entry.

6.4.3.4 RELEASE.

The RELEASE operator command is used to set the "release" bit in a QFT entry to allow a file to be released from the output queue even though its access level is greater than or equal to the output queue special handling level.

The jsn specified must be that of a file in the QFT. The UTEM monitor function will be used to set the appropriate QFT bit. See section 5.5.2 for the QFT format.

6.5 DSP.

6.5.1 INPUT FILES.

DSP will set the upper and lower access level limits returned by OVJ in the QFT entry as described in Section 5.5.2.

6.5.2 OUTPUT FILES.

If DSP creates an output file, the job access level must be specified in the RTCM call. This level must also be placed in the QFT.

When DSP is routing a previously deferred routed file, the file access level from the local FNT entry must be propagated to the QFT. This will allow the local file access level to change easily during the job.

6.6 LFM.

The following LFM functions are new or are modified for multi-level security. All tape assignment functions will be handled by RESEX. See section 6.42 for details.

SETFAL	Set local file access level (new).
STATUS	Return file status.
REQUEST	Request file assignment.
GETFNT	Get file information.

6.6.1 SETFAL (007).

The SETFAL function will set the access level of a local file.

Processing:

* If the file does not exist, process the request as an LFM error code 01, File Not Found.
* If the file is not of type LOFT, PTFT, or QFFT process the request as an LFM error code 02, Illegal File Type.
* If the "sp" bit, bit 39, is set in FET+1, take the new access level from FET+4. If the "sp" bit is not set, take the job access level to be the new file access level.
* If the access level in FET+4 is not in the range 0-7, process the request as an LFM error code 06, Access Level Out of Range.
* LFM will validate and set the requested access level using monitor function VSAM, subfunction VSFS. If the requested level is valid, LFM will issue the following Accounting Dayfile message:

  MFFA, filename.

* If the requested level is invalid, LFM will process the request as a security violation and issue the following Accounting Dayfile Message:

  MFFI, filename.

6.6.2 STATUS (013).

If the "sp" bit, bit 39D, is set in FET+1, return the file access level to bits 36-38 of FET+4. This will be done on both secured and unsecured systems.

6.6.3 REQUEST (014).

* If the file is already assigned, ignore the function (currently done this way).

* If the "sp" bit, bit 39D, is set in FET+1, take the requested access level for the file from bits 36-38 of FET+4. If the "sp" bit is not set, take the requested access level for the file from the job access level.

* If the access level in FET+4 is not in the range 0-7, process the request as an LFM error code 06, Access Level Out of Range.

* If the file access level is defined in the FET, validate the file access level using monitor function VSAM, subfunction VAJS. If the access level is invalid for the job, process the request as a security violation.

* On a secured system if the operator assigns an equipment whose access level limits do not include the requested level, reject the operator assignment and reissue the request until an acceptable equipment is assigned.

* Once an acceptable equipment is assigned, create the file at the requested access level.

6.6.4 REQUEST (015).

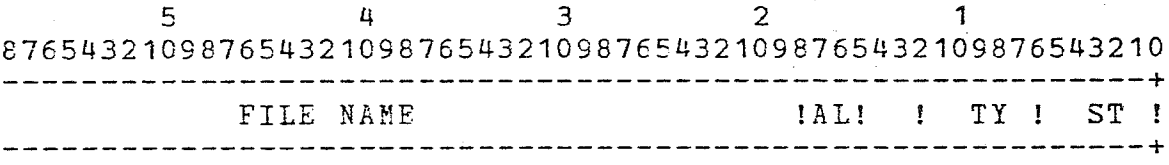
Access level processing for the REQUEST (015) function will be the same as the REQUEST (014) function will the following additions:

* If the access level limits of the specified equipment ordinal do not include the requested access level, process the request as an LFM error code 10, Equipment Not Available.

* If no device is found of the specified device type with access level limits that include the requested access level, process the request as an LFM error code 10, Equipment Not Available.

6.6.5 GETFNT (025).

The GETFNT (025) function will return the file access level in bits 17-15 of the first word of each returned entry.



AL Access level
TY File type
ST Status

6.7 MSM.

MSM will process device access levels during deadstart and during on-line recovery of removable mass storage devices.

6.7.1 DEADSTART RECOVERY (RMS).

During a level 0 deadstart, if RMS encounters a device whose access level limits in the device label are not within the equipment access level limits from the device EST entry, the device will not be recovered.

* If the device is not removable, deadstart will be halted with the diagnostic message on the B-display.

  EQnnn - DEVICE ACCESS ERROR.

  A new deadstart will be required to correct this condition.

* If the device is removable, the device will be left unavailable with SV (Security Violation) error status.

6.7.2 ON-LINE RECOVERY (CMS).

6.7.2.1 UNSECURED SYSTEM.

If CMS detects that the device access level limits in the device label are not within the equipment access level limits from the EST, CMS will suspend recovery of the device by setting the pause bit at the control point and will issue the following Error log and B-Display message:

EQnnn - SECURED DEVICE.

At this point the operator must take one of the following actions:

1) Enter "PAUSE,CMS." at the console to terminate recovery of the device. The device will be left unavailable in SV status. At this point the secured device should be removed from the system.

2) Enter "GO,CMS." to complete recovery of the device. A message will be issued to the error log with the following format:

EQnnn,SECURED DEVICE RECOVERED,ALa.

nnn = equipment EST ordinal.
a = access level of device.

6.7.2.2 SECURED SYSTEM.

This case will be handled the same way as deadstart recovery on a secured system, i.e. the device will be left unavailable with SV error status.

6.8 MTR/CPUMTR.

The following Monitor functions are new or are modified for multi-level security. The formats of the request and reply words are described in section 5.8.

RDCM	Request Data Conversion. Subfunction 10 - Calculate Packed Date. Subfunction 11 - Encrypt Password.
RSTM	Request Storage.
RTCM	Reserve Track Chain.
SEQM	Set Equipment Parameters. Subfunction 17 - Set Equipment Access Levels.
VSAM	Validate Security Access.

6.8.1 REQUEST DATA CONVERSION - RDCM.

6.8.1.1 CALCULATE PACKED DATE (10).

* Add the 12-bit value given in the lower 12 bits of the request to the packed date in the message buffer and return the new packed date to the message buffer.

6.8.1.2 ENCRYPT PASSWORD (11).

* Use common deck COMCECP or equivalent in-line code to encrypt the 42-bit value in the upper 42 bits of the message buffer and return the resultant encrypted 42-bit value to the upper 42 bits of the message buffer.

6.8.2 REQUEST STORAGE - RSTM.

If the MEMORY CLEARING bit is set in CMR word SSTL, then whenever a job releases central or extended memory with the RSTM function, it must be cleared. MTR will issue a CSTM function to do this. The memory cannot be released from the job until it has been cleared.

6.8.3 REQUEST TRACK CHAIN - RTCM.

Access level will be added as one of the device selection criteria.

If an access level is specified, the best device that allows the requested level will be assigned. If no device is found, this status will be returned to the caller.

If no access level is specified, there will be no change from current processing; no attempt will be made to insure the assigned device is valid for the job or file. The caller must insure that an access level is specified if required.

6.8.4 SET EQUIPMENT PARAMETERS - SEQM.

Add SEQM subfunction EALS (17) to set the equipment access level limits in the EST. This function will be called by DSD when processing the SECUREQ command. The PP will be hung if the requested limits are not within the system access limits, or the equipment is not a unit record equipment.

6.8.5 VALIDATE SECURITY ACCESS - VSAM.

Add VSAM function as described in section 5.8.5. This function will make all security validation decisions. If the system is not in a secured mode, no validation will be done; all requests will be considered to be valid.

6.8.6 FIELD LENGTH DECREASE.

If MEMORY CLEARING is enabled, CPUMTR routine AFL must insure that any released field length is cleared. This will be done by forcing a call to 1MA to release the field length rather than processing in CPUMTR. 1MA is already called to reduce field length at the last control point.

6.9 PFM.

PFM will process permanent file access levels, access categories, and password and PERMIT expiration terms.

6.9.1 PERMANENT FILE FET.

See Section 5.6 for a description of the new fields that are defined in the permanent file FET for multi-level security parameters on Permanent File Manager requests.

6.9.2 USER ERROR PROCESSING.

Because the job step will be aborted with an SVET error flag when a security violation occurs, there is no user error processing available for security violation error.

6.9.3 PASSWORD PERMIT EXPIRATION PROCESSING.

PFM will process password/PERMIT expiration date and term parameters as follows.

1. This field will be ignored if the command is not SAVE, DEFINE, PERMIT or CHANGE.

2. If the user is not validated to set expiration dates (validation privilege CFPX), the job will be aborted with the message:

   NOT VALIDATED TO SET XD/XT.

   This is not a security violation.

3. If an expiration date is specified, use monitor function RDCM to calculate the maximum date allowed (based on maximum term defined in COMSPFM). If the specified date is beyond this, the job will be aborted with the message:

   XD/XT EXCEEDS MAXIMUM.

   If an expiration term is specified, compare to the maximum allowed. If it is less than the maximum, use monitor function RDCM to convert to a date. If not, the job will be aborted with the above message.

   The XD/XT EXCEEDS MAXIMUM error is not a security violation.

6.9.4 ALTERNATE USER ACCESS.

On all alternate user requests, a file-not-found error will be returned if any of the following are true.

1. Password expired.
2. User not validated to access file. This checked by monitor function VSAM, subfunction VAJS. The user's access level and categories are compared to the file's access level and categories from the PFC entry.
3. Permit expired.

6.9.5 OWNER ACCESS.

Monitor function VSAM, subfunction VAJS will validate all permanent file accesses. The access level and categories of the file must be valid for the job. If not, the request will be processed as a security violation.

6.9.6 FUNCTION REQUESTS.

In addition to the above rules, each PFM function will be changed as follows.

6.9.6.1 SAVE (001,CCSV).

* If the access level of the local file is not allowed on the user's master device, the request is processed as a security violation.

* Set the password expiration date (if a password is defined), access level and access categories in the created PFC entry. The access categories are taken from Control Point Area word JSCW.

6.9.6.2 GET (002,CCGT).

* If the "sp" bit is set in FET+1, return the file access level from the PFC entry to bits 38-36 in FET+4.

* Request the local copy of the file on a device where the file is valid to reside.

* Set the file access level in the FNT entry.

6.9.6.3 CATLIST (004,CCCT).

* On alternate user requests, information will only be returned for files that are currently accessible to this user. (See 6.9.4). The file access level, access categories and password expiration date are cleared from the returned PFC entry.

* On a permit data search, the permit expiration date field will be cleared from the returned entry if it does not contain an expiration date.

6.9.6.4 REPLACE (006,CCRP).

* If the file does not currently exist, REPLACE is identical to a SAVE.

* If the access level of the local file is higher than the level in PFC of the existing permanent file, write-down validation privileges are required (validation privilege CWLF).

6.9.6.5 APPEND (007,CCAP).

* If the access level of the local file is higher than that of the permanent file to be appended to, write-down validation privileges are required.

6.9.6.6 DEFINE (010,CCDF).

* If the file already exists as a local file, and its access level is less than that of the job, write-down validation privileges are required. Also, the access level of the file must be allowed on the user's master device.

* If the file does not exist, device selection will use the job access level as a criterion.

6.9.6.7 ATTACH (011,CCAT).

* Fast attach processing will be exempt from the accessibility validation described in section 6.9.5.

* If the "sp" bit is set in FET+1, return the file access level from the PFC entry to bits 38-36 in FET+4.

* Set the file access level in the FNT entry.

6.9.6.8 CHANGE (012,CCCG).

* The new password expiration date will be set in the PFC entry, if specified.

6.9.6.9 ASSIGNPF (020,CCAN).

* The file access level from the PFC will be supplied in FET+4 by MSSEXEC. This level will be used for device selection.

6.9.6.10 OLD (021,CCOL).

* OLD is processed the same as GET.

6.9.6.11 SETPFAC (022,CCAC).

* The specified access categories must be valid for the user, or the request is processed as a security violation. This is checked by monitor function VSAM, subfunction VAJS.

* The FET must be at least 6 words long to insure the category field is present.

* If the file is a direct access file, the system sector will be read to determine if the file is currently being accessed. If so, a file-busy error is returned.

* Set the new access categories in the PFC entry.

6.9.6.12 SETPFAL (023,CCAL).

* The specified access level must be valid for the user and for the device where the file resides, or the request is processed as a security violation.

* If the file is a direct access file, the system sector will be read to determine if the file is currently being accessed. If so, a file-busy error is returned.

* Set the new access level in the PFC entry.

6.10 QAC.

QAC will process access levels as selection criteria on all requests. For user calls, the specified access level range must be within the job access level limits. The request block format is described in section 5.7. The default range will be all access levels for system calls and the job access limits for user calls.

6.10.1 PEEK FUNCTION.

QAC will return the access level of an executing job or queued file in word 1 of the PEEK reply block. See section 5.7 for the format.

6.10.2 GET FUNCTION.

QAC will return the access level of a selected queued file in word 15 of the GET parameter block. See section 5.7 for the format.

Once a file is selected, based on the access level range, the Output Queue Special Handling Level must be considered. The file will not be selected if all of the following are true:

Caller is BATCHIO.
File type is output.
Access level is greater than or equal to OQSH.
Release bit is not set in the QFT.

6.10.3 ALTER FUNCTION.

A new alter flag and field will be defined to allow altering the access level of an output file. See section 5.7 for the request block format.

If this alter flag is set, the caller must have security administrator privileges.

The new access level for a file must be within the file's origin type limits and be allowed on the device where the file resides.

6.11 QAP.

When the local file for an input job is created, the lower equipment access level limit of the card reader will be used as the access level.

6.12 QFM.

Function CQFF (Create Queue File) must set the file access level in the RTCM call when assigning mass storage space for the file. The level will come from the QFT image in the system sector. If the assignment is successful, this level must be placed in the new QFT and the FNT entry.

A new QFM error status (NSEE=11B) will be defined to indicate that the requested equipment did not have the required security level for the queued file. This error code will be returned if error processing is selected in the FET. Otherwise, the message

FILE NOT ALLOWED ON EQUIPMENT.

will be issued.

6.13 SET.

SET will process the IPRDECK entries as defined in section A.3.1.

Each entry will be added to the syntax table in IPR and a routine added to process it.

Define a .SSML word to store OQSH, OPSECM and SECCATS values, and write this word to CMR unless it is a level 3 recovery. The format of SSML is defined in section 5.3.6.

When SET releases job field length (central and extended memory) on a level 3 recovery, the memory must be cleared if MEMORY CLEARING is enabled.

6.13.1 OPSECM.

Value must be 0, 1, 2, or 3.

6.13.2 OQSH.

Must be a valid access level name.

6.13.3 SECURES.

Must be a valid origin type mnemonic (use NMOT micro from NOSTEXT).

Both LA and UA must be specified, and be valid access level names.

Corresponding value of LA must be less than or equal to the corresponding value of UA.

If origin type is SY, set all origin type limits in the Service Class Control Table (SCT). The format of this table is defined in section 5.5.

If the origin is not SY, the values must be within the system origin limits. If so, set them into the corresponding word in the SCT.

6.13.4 SECCATS.

Initialize .SSML with all 32 categories enabled.

The first time SECCATS is encountered, clear all 32 bits before processing. Then process each entry of SECCATS by setting or clearing the indicated bits.

Each entry must be a valid access category name.

6.13.5 ENABLE/DISABLE MEMORY CLEARING.

Add MEMORY CLEARING bit to .SSTL, and store value from ENABLE/DISABLE MEMORY CLEARING. entry. Bit position is defined in section 5.3.1.2. It is initially disabled.

6.14 SFM.

The following SFM functions are added for multi-level security:

Code	Function	Description
33	GSSF	Get security status.
34	GEAF	Get equipment/device access level limits.

6.14.1 GSSF FUNCTION (33).

The GSSF function returns the output queue special handling level, the operating system security mode, and the access level limits for SYOT, BCOT, EIOT, and TYOT origin types to the calling process. This function requires an SSJ= entry point or a subsystem ID. The reply word format is shown in Section A.3.5.1.

Internal Processing:

* If the calling process does not have an SSJ= entry point or subsystem ID, abort the job with an "SFM ILLEGAL REQUEST" error.

* Copy the data from CMR word SSML and from the Service Class Control Table (first JCA entry) to the reply word.

6.14.3 GEAF FUNCTION (34).

The GEAF function returns the access level limits of a specified equipment to the calling program. If the specified equipment is mass storage, the device access level limits from the MST will be returned. This function requires an SSJ= entry point or a subsystem ID. The request and reply word formats are shown in Section A.3.5.3.

Internal Processing:

* If the calling job does not have an SSJ= entry point or subsystem ID, abort the job as an *SFM ILLEGAL REQUEST*.

* If the specified EST ordinal is not a valid equipment, abort the job with an *SFM ARGUMENT ERROR*.

* Return the access level limits from the equipment EST entry, or, if the equipment is mass storage, the device access level limits from the device's MST entry, to the calling program in the reply word.

6.15 SLL.

On a non deadstart-load initiation, check the system security mode. If the system is executing as a secured system, check the user for Security Administrator privilege. If the user does not have Security Administrator privilege, abort the job using the current "SYSTEM LIBRARY CHANGE ILLEGAL" diagnostic.

6.16 VEJ.

If the security processing ("sp") bit, bit 39 of word FET+1, is set when VEJ is called, the caller has placed an access level limit in bits 36-38 of FET+4. On a secured system VEJ will compare the value to the upper limit returned by CVJ, and, if the FET+4 value is less, VEJ will return a JOB CARD ERROR status. If the FET+4 access level limit is greater than or equal to the upper limit returned by OVJ, the upper limit value will be returned in FET+4.

This interface is designed for RBF to place the communications line access level limit in FET+4 when calling VEJ.

6.17 OBF.

OBF will place the access level of the new file in word FUTL of the file FNT entry when creating the file. If no access level is specified, the job access level from Control Point Area word JSCW will be used. This access level will be used in the RTCM request, if one is made.

Entry Conditions:

ENTRY ((LA)-1) = 2/, 1/A, 3/AL, 6/Unchanged

A = Access level selection flag.
AL = Access level to set.

6.18 OBP.

OBP will print the file access level on the standard banner page, using the symbolic names defined in COMSMLS. The entire entry will be blank if the system is in the unsecured mode. See Section A.4.7 for the banner page format.

6.19 OVJ.

6.19.1 JOB CARD PROCESSING.

OVJ will process the new AL parameter on the JOB card. If the value specified is not one of the micros defined in COMSMLS, the job will be aborted with a JOB CARD ERROR.

OVJ will process the new AL parameter on the JOB card. If the value specified is not one of the micros defined in COMSMLS, the job will be aborted with a JOB CARD ERROR.

On a secured system, OVJ will use VSAM subfunction VJCS to determine if the value specified by the AI parameter is valid to use as an upper limit for the job. See section 5.8.5 for the parameters required by this subfunction, and the information returned. The default will be selected by OVJ if no AL parameter is specified. If VSAM determines that the upper bound or lower bound supplied are not valid to use for the job, OVJ will return a JOB CARD ERROR status to the caller.

OVJ will return the job's upper and lower access level limits to the calling program, which will set them in the input file QFT entry.

6.19.2 PASSWORD VALIDATION.

OVJ, together with the caller must delete the password from the first sector of the input file (USER command). The unencrypted password will be saved in the input file system sector. When OVJ is called to requeue an input file, it will use the value from the system sector for validation purposes.

6.20 1AJ.

6.20.1 JOB INITIATION.

1AJ will set up the Control Point Area word JSCW as described in section 5.5.1. The following rules will govern this procedure.

* The security privilege validation bits, access level validation bits, and category bits will be taken from the input file system sector validation file image. These values have already been restricted based on the JOB card criteria.

* The (initial) Job Access level is taken from the lower access level limit field in the EJT.

* The Job Access level limit is taken from the upper access level limit field in the EJT.

The INPUT file access level in the FNT entry will be set to the lower access level limit.

6.20.2 SECURITY VIOLATION PROCESSING.

Due to changes in the system and origin type access limits by the SECURES command, some executing jobs can be aborted with an SVET error flag. These jobs must go through job termination processing, but their access level may no longer be valid. 1AJ must set a valid level in the control point area so that normal job termination can occur. The lower limit for the job's origin type will be used.

6.20.3 MEMORY CLEARING.

If MEMORY CLEARING is enabled, it is not necessary for 1AJ to clear any additionally assigned field length.

6.21 1DS.

6.21.1 JOB CREATION.

When 1DS creates an input file the following rules will apply.

The access level used on the RTCM request will be the lower system limit.

The upper and lower job access limits will be the upper and lower system limits. These will be set in the QFT entry.

The valid job access levels will be all levels within the system limits. The valid job access categories will be all valid system categories as defined by the SECCATS IPRDECK entry.

6.21.2 VSAF FUNCTION.

Add the VSAF function to validate the username and password entered by the operator on the UNLOCK command.

This function will call OAV to read the validation file for the specified username. If this user has Security Administrator Privileges, then the password will be verified using RDCM subfunction 11 to encrypt it and compare it to the operator entered value. The Lock and SECURITY UNLOCK bits will be set in SSTL if the validation is successful. The 1DS/DSD buffer interlock in CMR will be used to return the status of this function to DSD.

Use of this function will cause an entry in the Account Dayfile. See Appendix B for the message format.

6.22 1IO.

Add the equipment access level limits to the Buffer Point Area when building it.

When making QAC requests to select output files, use the access level selection bits as described in section 5.7. The equipment access level limits will be used as the selection criteria.

6.23 1RI.

1RI currently clears any field length increase assigned at rollin time. This will not be necessary if MEMORY CLEARING is enabled.

6.24 1MT.

A new error message will be added to the list used by DSD on the E,P display. This will be used when the equipment where the tape is mounted will not allow the access level of the assigned file. The text of the message will be

ACCESS CONFLICT

6.25 1RO.

If MEMORY CLEARING is enabled, 1RO will disable dynamic field length reduction of central and extended memory. This will ensure that the RSTM monitor function is used to release all storage; in turn ensuring that all released storage will be cleared.

When requesting mass storage for the rollout file, the job access level must be specified on the RTCM call.

6.26 1SJ.

During each scheduling cycle, 1SJ examines each EJT entry. If any entry has job access level limits that are outside the current access level limits for the job's origin type, an SVET error will be set on that job. Jobs with job termination in progress are excepted.

No checking of the QFT access level limits will be performed. The jobs will be scheduled to the EJT normally, and any illegal ranges detected on the next EJT scan.

6.27 1TA.

For non-network terminals, use the interactive login password from word APWI of the validation file record.

When requesting mass storage for the input file, use the TXOT origin type access level lower bound in the RTCM call.

The communications line access limit will be sent to 1TA from IAF in the login pot. If this level is supplied, it will be used as the requested upper limit in the VSAM VJCS call; if not, the TXOT lower bound will be used as the limit. The requested lower limit in the VSAM call will be the TXOT lower bound.

If the VSAM request is invalid, 1TA will treat the login as an error. The returned upper/lower limits will be set in the QFT entry. The returned restricted validation access levels and categories will be set in the system sector.

6.28 CATLIST.

The output for CATLIST (LO=F) will include the access level and password expiration date, if present.

The output for CATLIST (LO=FP) will include the permit expiration date, if present.

A new option, LO=X, will be added to CATLIST. This option will provide "expanded" output for an individual file. The output will consist of the three lines of output normally given for LO=F, followed by a listing of the access category set of the file. The file name specification (FN= filename) will be required for this option.

See section A.4.4.5 for examples of the new CATLIST output.

6.29 CHKPT.

The access level of the checkpoint file must be set to the job access level limit before any information is written. This will insure that no local files to be checkpointed will have a higher access level than the checkpoint file.

CHKPT will use the GETUSV macro to determine the job access level limit and then issue the SETFAL macro to set the checkpoint file access level.

6.30 CPUCIO/1MS.

CPUCIO (or 1MS) is modified to process the following functions:

* Setting of file access levels on OPEN functions.
* Automatic advance of local file access level on WRITE functions.
* Automatic advance of job access level on READ functions.
* Processing of the new OVWRITE function.

6.30.1 OPEN FUNCTIONS.

If the file does not exist and if user "sp" bit (bit 39) is set in FET+1, set the file access level to the value in the access level field in FET+4. If the requested access level is not valid for the job, process the request as a Security violation.

If the file already exists and if the user "sp" bit (bit 39) is set in FET+1, return the file access level to the access level field (bits 38-36) in FET+4.

6.30.2 WRITE FUNCTIONS.

On a secured system CPUCIO will advance the access level of local files (mass storage or magnetic tapes) to the access level of the job on all WRITE functions unless the requesting process has one of the following:

(a) Write-down privilege.
(b) An SSJ= Entry Point.
(c) Subsystem ID.

For direct access permanent files the user must be validated for write-down privilege. If the user is not so validated, the request will be processed as a security violation.

If the resulting access level of the file is not within the device access limits, the request will be processed as an *ILLEGAL I/O REQUEST ON FILE* error.

If the local file does not exist prior to a WRITE operation, a mass storage file will be created on an appropriate device in the same manner as with an OPEN function.

6.30.3 READ FUNCTIONS.

On secured systems, CPUCIO will advance the job access level to the file access level on all READ functions if the file access level is greater than the jcb access level.

6.30.4 OVWRITE.

CPUCIO will recognize the OVWRITE (244) and OVWRITE RETURN (254) functions, and call 1MS to process them.

1MS will use the same threshold as defined for buffered writes when determining when to enter the recall stack. For the OVWRITE RETURN function, ODF will be called to drop the file after the operation; an "UNLOAD" type call will be made. For the OVWRITE function, the file will be left positioned at BCI.

6.31 DSDI.

All changes made to tables as described in section 5 will be reflected in DSDI cutput.

6.32 ENQUIRE.

ENQUIRE,OP=B will return the job's current access level, access level limits, and category set if the system is in a secured mode. The GETJAL and GETUSV macros will be used to obtain this information.

ENQUIRE,OP=F will return each file's access level if the system is in a secured mode. The file access level is returned by the GETFNT macro.

ENQUIRE,JSN=jsn will include the access level of each job or queued file listed if the system is in a secured mcde. The job or queued file access level is returned by the QAC PEEK request.

See section A.4.4.12 for the format cf the returned information in each case.

6.33 MAGNET.

When doing reel swap, i.e. searching for the next reel already mounted on another unit, MAGNET must ensure that the access level limits of the new unit are adequate to handle the file already assigned to the old unit.

6.34 MLSEXEC.

MLSEXEC is a new CPU program to process the following multi-level security commands. These commands are described in Section A.3.3.

SETFAL	Set file access level.
SETJAL	Set job access level.
SETPFAC	Set permanent file access categories.
SETPFAL	Set permanent file access level.

MLSEXEC will remove the access level name from the SETFAL, SETJAL, and SETPFAL commands before issuing the command to the dayfile.

The specified access level/categories will be verified against the COMSMLS micros. If the name is not found, the job will be aborted with the message: UNKNOWN ACCESS LEVEL NAME. or UNKNOWN ACCESS CATEGORY NAME, as appropriate.

Any other syntax error will cause the job to abort with the message: INCORRECT ARGUMENT.

When processing the SETFAL, SETJAL and SETPFAL commands, the corresponding macro will be issued. No further validation of the specified access level will take place.

When processing the SETPFAC command, if the "cat1 = 0" syntax is not used, the current access categories for the file must be determined. The CATLIST macro will be used for this. In both formats, the resulting bit map (bit = 1 means category is set) will be used when issuing the SETPFAC macro. No further validation of the categories will take place.

The optional PN and R parameters for SETPFAL and SETPFAC will be passed along as parameters on the respective macro. The WB and NA parameters will be processed the same as for other permanent file commands.

6.35 MFILES.

MFILES will have an additional entry point, OVWRITE, to process the OVWRITE command. The OVWRITE command is described in section A.3.3.1.

Internal Processing:

* If both the X and the Z options are selected abort the job with the diagnostic *Z AND X OPTIONS SELECTED* error.

* Using the named-file format, if any file selected is not on mass storage, issue the message *lfn NOT ON MASS STORAGE* where "lfn" is the file name specified on the control statement, and continue with the next named file. Using the exclusion format, if any file found is not on mass storage, do not process that file.

* Using the named-file format, if any file is in read-only status, issue the mesage *lfn IS READ-ONLY* where "lfn" is the file name specified on the command, and continue with the next named file. Using the exclusion format, if the file is in read-only status, do not process that file.

* Issue CIO function 244 (OVWRITE), or 254 (OVWRITE RETURN) if the R option is specified, to process each file selected.

6.36 MODVAL

MODVAL will process the following new or modified functions for multi-level security.

* New validation parameters.
* Multiple passwords.
* Password encryption.

6.36.1 EXECUTION VALIDATION REQUIREMENTS.

Console input or the use of the FA parameter on a secured system will require that the job have security administrator privilege set in Control Point Area word JSCW.

If the user does not have security administrator permission, abort the job with the following diagnostic:

ILLEGAL USER ACCESS.

6.36.2 SPECIAL USER INDEXES.

When MODVAL creates the default special user names SUBFAM0-SUBFAM7, APPLLIB, FLAWPFX and LIBRARY, it will set the associated passwords as immediately expiring. These passwords are public knowledge since they appear in the source to MODVAL; setting them as immediately expiring will force the security administrator to change them (from SYSTEMX, with a non-expiring password) before they can be used. The password to SYSTEMX should be changed at this time, since it also appears in MODVAL.

When MODVAL creates the default special user name SYSTEMX (user index 377777), it will be given security administrator privileges.

6.36.3 CONSOLE (K) DISPLAYS.

Existing display pages are modified and a new page, page 4, is added for security validations. The user password and security count lines are removed from page 1. The format of the new page 4 is shown in section A.4.3.1.1.

6.36.4 PASSWORD INPUT DIRECTIVES.

New directives will set the batch and interactive passwords. The current PW directive will set both passwords. Whenever a password is entered, the associated expiration date is set to the default. See section A.4.3.1.2.4. for the directive formats.

6.36.4.1 OCTAL PASSWORD SPECIFICATION.

Passwords may also be specified in an octal rather than alphanumric format. Octal format will be indicated by the specification of the preradix "+" ("plus" sign), followed by 14 octal digits (42 bits), representing the internal representation of the password in the user validation file. The system default minimum number of characters will not be required using this format.

This form of password entry is not allowed using the PASSWOR command.

The primary use of this form of password entry is to allow the re-creation of encrypted password files without needing to specify the unencrypted form of the password, i.e. when re-creating the validation file from source.

6.36.5 PASSWORD EXPIRATION DIRECTIVES.

The user password expiration dates are stored in standard packed date format, yymmdd, where yy = the current year minus 1970, and mm and dd are the current month and day, respectively, in the lower 18 bits of the password entry.

When a password is created or is changed, the system default expiration term, COMSACC parameter APXT, is added to the current date and is stored as the password expiration date. After this, the expiration date may be changed by input directive.

See section A.4.3.1.2.5 for the directives to set the password expiration, specified either by term or date.

6.36.6 SECURITY ACCESS LEVEL INPUT DIRECTIVES.

The SAL input directive defines the user's validated security access levels. See section A.4.3.1.2.1 for the directive format.

6.36.7 SECURITY ACCESS PRIVILEGES INPUT DIRECTIVES.

The SAV input directive sets or clears the user's security access privileges. See section A.4.3.1.2.3 for the directive format.

6.36.8 SECURITY ACCESS CATEGORY INPUT DIRECTIVES.

The SAC input directive defines the user's validated security access categories. See section A.4.3.1.2.2 for the directive format.

6.36.9 PASSWOR COMMAND.

MODVAL will process the optional password expiration date or expiration term parameter on the PASSWOR command.

These parameters can be used to set the expiration date of a new password or to change the expiration date of an existing password without changing the password itself. Validation bit CPWX is required to use these parameters. They will also be accepted on the INPUT file form of the PASSWOR command.

The interactive password can only be changed by a job with TXOT origin type. The batch password can only be changed by a job with any other origin type (SYOT, BCOT, or EICT).

See Section A.4.4.4 for the PASSWOR command format.

6.36.10 LIMITS OUTPUT.

LIMITS output will include all security related data: valid access levels, access categories, access privileges, and password expiration dates. If the user is not valid for any values in one of these areas, no header will be printed. See section A.4.3.1.3 for the LIMITS output format.

6.36.11 OP=I.

Since MODVAL, OP=I is equivalent to LIMITS, this option will be deleted.

6.37 MSI.

MSI will be changed to process operator entry of upper and lower device access level limits during on-line device initialization.

The LA and UA parameters will be added for this purpose, and will be processed as follows.

1. They will be added to the K-display parameter list. The current values will be displayed until changed.

2. The default values will be the equipment access limits from the EST.

3. All values entered must be within the equipment access limits.

4. Any illegal value entered (outside limits, LA greater than UA, or both values not specified) will be ignored and a message displayed on the K-display.

5. These parameters can only be entered on a full initialize (AL) of the device.

6. These parameters will not be displayed or accepted if the system is unsecured.

6.38 MSS.

When MSS does an ASSIGNPF PFM function to create a local file on the appropriate permanent file device, it must specify the file's access level from the PFC. This will be passed to PFM in FET+4.

6.39 PFILES.

PFILES will process file password expiration date or term parameters and permit expiration date or term parameters. See Appendix A.4.4.3 for the new keywords and options for permanent file commands.

6.39.1 PASSWORD EXPIRATION PARAMETERS.

PFILES will process the XT and XD parameters for password expiration date or term options. These parameters are valid for the CHANGE, DEFINE, and SAVE commands. When used with SAVE and DEFINE, the PW parameter must also be specified.

Internal Processing:

* Add the XD and XT parameters to the PFILES internal tables.

* Process the following situations as an *ERROR IN ARGUMENTS* error.

  - Both XD and XT specified.
  - Either XD or XT specified on a command other than CHANGE, DEFINE or SAVE.
  - Either XD or XT specified on a DEFINE or SAVE command without also specifying PW.

* Process the following situations as an *ERROR IN EXPIRATION DATE.* error.

  - XD is a date previous to today's date.
  - XD is not a legal YYMMDD date as determined by COMCVDT.
  - The XT specified term is greater than the maximum allowed as defined by COMSPFM symbol MPXT.

* Process XT = * as a non-expiring password (XT = 7777B).

* Process XT = 0 as an immediately expiring password by setting the expiration date to today's date.

6.39.2 PERMIT EXPIRATION PARAMETER.

PFILES will process the expiration term or date parameter on the PERMIT control statement.

The format and processing of the expiration term or date parameter is identical to that done for the CHANGE, DEFINE, and SAVE commands.

6.40 PERMANENT FILE UTILITIES.

The PF utilities will be changed to process security access levels as selection criteria.

6.40.1 PFS.

The LA (lower access level) and UA (upper access level) parameters will be added to specify the range of access levels to be selected, and will be processed as follows.

1. They will be added to the K-display as valid parameters for all utilities, and a routine added to process them.

2. The default will be to process all files meeting the other selection criteria, regardless of access level.

3. If any access level selection is made, both LA and UA must be entered. If not, PFS will issue the message:

   BOTH UA AND LA MUST BE SPECIFIED.

4. The value associated with the LA name must be less than or equal to the value associated with the UA name. If not PFS will issue the message:

   INCORRECT ACCESS LEVEL LIMITS.

5. If either the LA or the UA access level names is not one of those defined in COMSMLS, PFS will issue the message:

   UNKNOWN ACCESS LEVEL NAME.

6. For PFDUMP, PFLOAD and PFCOPY, if access levels limits are selected, they must be within the system limits. If not, PFS will issue the message:

   ACCESS LEVEL LIMITS OUT OF RANGE.

6.40.2 PFATC.

No security restrictions will apply to PFATC.

6.40.3 PFCAT.

No security restrictions will apply to PFCAT.

6.40.4 PFCOPY.

For each file selected to be copied, the REQUEST macro will be used to assign the local file to an appropriate device. The access level from the file's PFC entry will be used; error processing will be set to return status from LFM. If no device can be found, PFCOPY will skip the file and issue the message:

   PFCOPY - NO DEVICE FOUND FOR FILE,FN=filename,UI=userindex.

6.40.5 PFDUMP.

PFDUMP will determine the maximum range of access levels that can potentially be dumped. If access level limits were selected by the LA and UA parameters, these values will be used. If no selection was made, PFDUMP will use the device limits from the MST of each device to be dumped; these limits will be saved in the MSTT table entry for each device. The maximum range is calculated by taking the lowest lower access limit and the highest upper access limit of all the devices in the table.

The range of possible access levels must be within the system limits or PFDUMP will abort with the message:

PFDUMP - ACCESS LEVEL LIMITS OUT OF RANGE.

The range of possible access levels must also be within the equipment access limits of the equipment assigned to the ARCHIVE and VERIFY files. If not, PFDUMP will abort with the message:

PFDUMP- ACCESS LEVELS NOT ALLOWED ON ARCHIVE FILE EQUIPMENT.

6.40.6 PFLOAD.

For each file selected to be loaded, PFLOAD must check that the device where is file is to reside is appropriate for the file's access level from the PFC entry. If not, PFLOAD will skip the file and issue the message.

PFLOAD - NO DEVICE FOUND FOR FILE,FN=filename,UI=userindex.

If PFLOAD is loading direct access files to the device with the most space (OP=L), it will use the largest device that also allows the required access level.

6.41 QUEUE UTILITIES.

The queue utilities will be changed to process security access levels as selection criteria. No security restrictions will apply to the utilities not listed here. In order to add these parameters to the K-display, the origin type/disposition type matrix will be moved to a second page.

6.41.1 QFSP.

The LA (lower access level) and UA (upper access level) parameters will be added to specify the range of access levels to be selected. These parameters will be processed in the same manner as for PF Utilities, as described in Section 6.40.1 (items 1-5).

1. For QDUMP and QLOAD, if access level limits are selected, they must be within the system limits. If not, QFSP will issue the K-display message:

   ACCESS LEVEL LIMITS OUT OF RANGE.

The NAL (new access level) parameter will be added to allow changing the access level of a queue file with QALTER. Use of this option is restricted to users with Security Administrator privileges. The selected new access level must be within the system limits.

6.41.2 QALTER/QFILIST.

The access level of queue files will be added to the LIST=qft display and the detailed output report.

The new access level (NAL) must be within the origin type limits for the file, and within the device limits of the device where the file resides.

6.41.2 QDUMP.

A maximum range test similar to the one for PFDUMP will be done for QDUMP. The device access level limits will be saved in a table built by QFSP Preset.

6.41.3 QLOAD.

For each file selected to be loaded, the access level must be within the file's origin type limits. The file must be assigned to an appropriate mass storage device.

6.41.4 QMOVE.

For each file selected to be moved, the destination device must have access level limits appropriate to accept it. If the file is being reactivated as well as moved, its access level must be within the file's origin type limits.

6.41.5 QREC.

Any file selected to be reactivated must be within the file's origin type limits.

6.42 RESEX.

RESEX will process the optional access level (AL) parameter on the ASSIGN, LABEL and REQUEST commands. The "sp" bit in FET+1 will be set and the requested access level, if valid, will be set in FET+4. If the AL parameter is used on any other RESEX entry point, it will be processed as an ARGUMENT ERROR. If the access level name is not defined in COMSMLS, it will be processed as an UNKNOWN ACCESS LEVEL NAME error.

When RESEX makes the association between a job and a tape equipment (either automatically on a LABEL request, or after operator assignment), it must insure that the tape equipment will allow the required access level on the file. This is the job access level, or the level specified by the AL parameter on the ASSIGN, LABEL or REQUEST command. If the equipment will not allow the level, i.e., the level is outside of the equipment access level limits, the assignment will not be made, and a message posted on the E,P display. The tape must be mounted on an appropriate unit before the assignment can take place.

RESEX will consider equipment access levels in the overcommitment algorithm. In order to qualify as an assignable resource, the equipment must allow the access level of the job.

The equipment access level limits of each tape equipment will be saved in the Resource Equipment Table (RET). When RESEX builds the preview display buffer, the access level of the file on each tape request will be included. This is used by DSD when formatting the E,P display.

When a request for an unlabelled tape is made, or an unlabeled tape assigned by the operator, the user's validation for writing unlabeled tapes must be checked. If the user is not valid (security validation word bit CULT), then the RING-CUT option will be forced for the tape.

6.43 SECHDR.

The SECHDR command adds security header information to a file. It is described in Section A.3.3.2.

Internal Processing:

* If no arguments are present, abort the job with the message:

  NO FILE NAME SPECIFIED.

* If a syntax error or unknown CP option is specified, abort the job with the message:

  UNKNOWN OPTION.

* If the specified file is not on mass storage, abort the job with the message:

  FILE NOT ON MASS STORAGE.

* The STATUS macro is used to determine the file access level to be displayed on the head/foot lines and the banner pages.

* Whether or not a file is already formatted (page ejects present) is determined by the FF parameter, not by inspecting the file. This information is only required if the P option is selected.

  If the file is formatted, the page divisions are not changed; the extra lines (blank line, header line, blank line at the top and the same at the bottom) are added. The print density is forced to 8 lines/inch to retain the match-up between the logical page boundaries and the physical pages. This is not possible if the original file was already formatted at 8 lines/inch.

  If the file is not formatted, it will be formatted at 6 lines/inch with the head/foot lines as described above, with 58 lines from the file on each page. Each line will be shifted right by one space to insure carriage control.

* The banner page is written as a separate record, at 6 lines/inch, at the intervals specified by the command options (EOR, EOF, or BOI/EOI).

  The banner page will consist of the following lines:

  (1) Page eject.
  (2) File name line + blank line.
  (3) Date line + blank line.
  (4) User name line + blank line.
  (5) Access level name line + blank line.
  (6) The access level name in large characters (16 lines high) centered on the page.
  (7) Deselect auto page eject (Q).
  (8) Select 8 lines/inch (T).

(9) 4 lines of page separator characters (116 "S" each).
(10) Select auto page eject (R).
(11) Select 6 lines/inch (S).

* If both banner and head/foot options are selected, the operations will be performed in one pass through the file.

6.44 INTERACTIVE FACILITY (IAF).

IAF will extract the line access level limit and user validation word ASVW from the CON/REQ/R login supervisory message received from NVF and will copy the fields into the login pot to be passed to 1TA to login the terminal job.

6.45 JOB TERMINATION IN PROGRESS FLAG.

As shown in Section 5, the job termination in progress flag is being moved from Control Point Area word ECJW to word SCHE of the EJT entry.

All programs that reference this flag will be changed to obtain it from its new location. The following decks are affected: DSP, REC, TLX, 1AJ, CPUMTR, DSDI, PPCOM.

7.0 NETWORK HOST PRODUCTS.

The following modifications to Network Host Products processes are to be implemented by Network Host Products.

7.1 INTERACTIVE LOGIN TRUSTED PATH.

For each terminal class there will be one reserved character that can be transmitted from the terminal to the TIP and which will be unconditionally recognized by the TIP as a reconfigure request. Upon receipt of this character any connection active on the terminal will be terminated and the login sequence will be initiated.

The character for each terminal class may be redefined by the installation, but once defined will be fixed and cannot be altered by any TERMDEF, user, or program means. This means that the character defined as the unconditional logoff/login signal will be unavailable to the user as a data character.

Instead of a single character, NHP may prefer to define a sequence of characters to allow the reconfigure character to be used as a data character when it does not appear in the reconfigure sequence.

7.2 PASSWORD BLANK-OUT.

Two means will be provided to decrease the possibility of passwords being left on the CRT screen for unauthorized users to read. These are in addition to the current black-out for hard-copy terminals.

1. Echoplex terminals will have echoplex disabled while the user is inputting the user number, password, and family. After login is completed, echoplex will be restored.

2. In addition to transmitting a clear-screen control character before the login dialogue, NVF will transmit an additional clear-screen control character immediately after each component of the user number, password, and family identification is entered.

7.3 NETWORK DEFINITION LANGUAGE PROCESSOR (NDLP).

The Network Definition Language Processor (NDLP) will allow specification of a new, 4-bit access level limit value for each line definition. This parameter will be stored in the NCB. If the upper bit, bit 3, of the four bit field is set, the lower three bits will contain the access level limit of the line. If the upper bit is not set, the lower three bits are not significant and the line has no access level limit defined.

NDLP will accept this line access level limit parameter, AL, on the LINE statement and the parameter value will be validated for the range of 0 to 7. If valid, the value will be placed in the NCB with bit 2**3 set.

If the value of the AL parameter is missing or is invalid, it will be processed as a "W" type error and the FN/FV pair value will be set to the special value of 00B which indicates an unspecified access level limit.

If the AL parameter is not included on the LINE statement, NDLP will set the value of the FN/FV pair to the default value of 00B which indicates an unspecified access value for that line.

LINE Statement Format:

abcdefg: LINE (other parameters)[AL=al].

al Access level limit for the line, 0 - 7.

7.4 CONNECTION PROCESSING (CS, CCP, NIP, NVF).

7.4.1 LINE ACCESS LEVEL LIMIT.

The line access level limit will be sent to the NPU as part of the NCB during the load process.

The Initiate Terminal Connection service message sent by CCP to NIP will include the line access level limit field extracted from the Line Control Block. NIP will, in turn, transmit this field to NVF in the Initiate Terminal Connection supervisory message.

NVF will retain the value and will pass it to the connecting application in every CON/REQ/R supervisory message during the life of the device connection to the system.

The line access level limit parameter will be placed in bits 13-17 of word 3 (block address + 2) of the CON/REQ/R connection request supervisory message.

7.4.2 USER VALIDATION PARAMETERS.

NVF will read the security validation word ASVW from the user validation file entry during validation processing. NVF will retain this word and will pass it to the connecting application as word 12D (block address + 11D) of the CON/REQ/R connection request Supervisory Message.

7.5 REMOTE BATCH FACILITY (RBF).

7.5.1 JOB INPUT PROCESSING.

On a secured system RBF will pass the line access level limit to VEJ in FET+4, and set the "sp" bit (39) in FET+1. If the AL parameter is specified on the JCB card, it must be less than or equal to the line access level limit. If so, VEJ will return the calculated job upper access level limit in FET+4.

7.5.2 JOB OUTPUT PROCESSING.

On a secured system RBF will extract the line access level limit received during login within the CON/REQ/R Supervisory Message and store it in RBF's terminal tables. This value determines the highest access level of data which may be transmitted over the line to the terminal.

RBF will then use this line access level limit value as a QAC call parameter to select output files to be transmitted to the terminal.

8.0 CODING CONVENTIONS.

The NOS Multi-Level Security project will be coded in COMPASS assembly language in conformance with the NOS COMPASS Programming Standards.

New modules and decks will comply with the 10-decision point complexity rule. Simply stated, this rule means that there should be no more than ten control transfer location tags in any routine or subroutine.

A.0 APPENDIX A - EXTERNAL INTERFACE CHANGES.

A.1 AFFECTED MANUALS.

NOS Version 2 Reference Set, Volume 3	60459680
NOS Version 2 Reference Set, Volume 4	60459690
NOS Version 2 System Maintenance Reference Manual	60459300
NOS Version 2 Operator/Analyst Handbook	60459310
NOS Version 2 Installation Handbook	60459320
NOS Version 2 Applications Programmer's Instant	60459360
NOS Version 2 Systems Programmer's Instant	60459370
Network Terminal User's Instant	60459380
Network Definition Language Reference Manual	60480000
Remote Batch Facility Version 1 Reference Manual	60499600

A.2 GLOSSARY OF NEW TERMS.

The following security related terms will be defined.

Security access level
Security access category
Operating system mode
System access level limits
Job access level limits
Device access level limits
Equipment access level limits
Security Administrator
Security Unlock status
Output queue special handling level
Batch password
Interactive password
Password expiration term
Read-down
Write-down
Downgrade
Password encryption
Security violation
Overwrite

A.3 NEW COMMANDS AND MACROS.

A.3.1 IPRDECK ENTRIES.

A.3.1.1 MEMORY CLEARING ENTRY.

The MEMORY CLEARING entry enables or disables the clearing of central and extended memory whenever it is released from a job. It can be entered only during deadstart. The default is that MEMORY CLEARING is disabled.

Entry Format:

```
ENABLE, MEMORY CLEARING.
DISABLE, MEMORY CLEARING.
```

A.3.1.2 OPSECM ENTRY.

The OPSECM entry sets the operating system security mode. It can be entered only during deadstart.

Entry Format:

```
OPSECM=n.
```

0 Sets the system to the unsecured mode. This is the default value and is selected when the OPSECM IPRDECK entry or parameter value is omitted.

1 Multi-level security is enabled. The values of the system access level limits may be set either by the SECURES IPRDECK entry or by console command. The SECURES console command may be used to either raise or lower system access level limits.

2 Multi-level security is enabled. The values of the system access level limits are set by the SECURES IPRDECK entry. The SECURES console command may be used to raise but not to lower system access level limits.

3 Multi-level security is enabled. The values of the system access level limits are set by the SECURES IPRDECK entry only; the SECURES console command is invalid.

A.3.1.3 OQSH ENTRY.

The OQSH entry may be entered either during deadstart or under DSD during system operation. The OQSH entry selects the value of the output queue special handling level. Output files with an access level greater than or equal to the output queue special handling level will remain in the queue until released by the operator. (See RELEASE command). The default is 0; all files will be processed.

Entry Format:

OQSH=level.

level	Access level name corresponding to desired output queue special handling level.

A.3.1.4 SECCATS ENTRY.

The SECCATS entry determines the security access categories which will be allowed in the system for processing when the system is in a secured mode. The SECCATS entry can be entered only during deadstart.

Entry Formats:

SECCATS,cat1,...,catn.

catk (k=0,31)	Category names corresponding to desired categories. Initially, all categories are enabled; the first time that the SECCATS entry is encountered, all categories are cleared and are then set as defined in the SECCATS entry. Subsequent SECCATS entries then set additional categories as desired.
SECCATS,ALL.	This form of the SECCATS entry enables all 32 access categories.
SECCATS,NUL.	This form of the SECCATS entry disables all 32 access categories.

A.3.1.5 SECURES,SY ENTRY.

The SECURES,SY entry sets the system access level limits. The default is that both the upper and lower limits are zero; no system access at higher levels is allowed.

Entry Format:

SECURES,SY,LA=lowerlevel,UA=upperlevel.

lowerlevel = access level name corresponding to desired lower limit.

upperlevel = access level name corresponding to desired upper limit.

Both lowerlevel and upperlevel must be entered; however, they may be set to the same value, restricting system access to a single level.

A.3.1.6 SECURES,ot ENTRY.

The SECURES,ot entry sets the access level limits for an origin type. The default limits for all origin types are the system access limits. Origin type access limits must be within the system access limits.

Entry Format:

SECURES,ot,LA=lowerlevel,UA=upperlevel.

ot = Origin Type. Valid values are:

SY	System
BC	Batch
TX	Interactive
EI	Remote Batch

If ot = SY is specified, this command will set the system access limits.

A.3.2 OPERATOR COMMANDS.

A.3.2.1 OQSH COMMAND.

The OQSH command is identical to the OQSH IPRDECK entry. See section A.3.1.3. It is used to change the Output Queue Special Handling Level.

A.3.2.2 RELEASE COMMAND.

The RELEASE command will allow an output file to be released from the output queue and processed by BATCHIO, even though its access level is above the current output queue special handling level.

Command Format:

RELEASE,jsn.

jsn Jcb sequence name of cutput queue file to be released.

A.3.2.3 SECUREQ COMMAND.

The SECUREQ command will reset the equipment access level limits for a unit record equipment.

Entry Format:

SECUREQ,EQnnn,LA=lowerlevel,UA=upperlevel.

EQ	Two character mnemonic for the unit record equipment (CR, LP, IR, etc.).
nnn	EST ordinal.
lowerlevel	Access level name corresponding to the desired lower limit.
upperlevel	Access level name corresponding to the desired upper limit.

A.3.2.4 SECURES COMMAND.

The SECURES,SY and SECURES,ot commands are identical to the IPRDECK entries. See section A.3.1.5. These commands are used to change the system access level limits (which resets all origin type limits), or a single origin type's limits.

A.3.3 USER COMMANDS.

A.3.3.1 OVWRITE COMMAND.

The OVWRITE command will cause a mass storage file to be overwritten to destroy classified information on the file. The file is first overwritten with binary zeroes, then the file may be optionally overwritten with binary ones followed by a pattern of alternating binary ones and zeroes.

Command Format:

OVWRITE,lfn1,...,lfnn/OP=options.

Overwrites the named files (lfn1,...,lfnn). All files named must be on mass storage.

OVWRITE,*,lfn1,...,lfnn/CP=options.

Overwrites all files assigned to the job except named files (lfn1,...,lfnn).

Option

Z — Overwrite the file with binary ones. This is the default automatically selected unless the X option is selected. Both the Z and the X options cannot be simultaneously selected.

X — Overwrite the file first with binary zeroes, then with binary ones, then with a pattern of alternating binary ones and zeroes. Both the X and the Z options cannot be simultaneously selected.

R — Return all files processed after completion. This option is normally deselected.

A.3.3.2 SECHDR COMMAND.

The SECHDR command adds security header information to a file. Two types of header information can be selected.

(1) Page headings and footings on each page of output. If the file already if formatted (carriage control present), the print density will be forced to 8 lines per inch, so the additional information will fit on each page. The following information will be added to the top and bottom of each page.

ACCESS LEVEL = levelname

(2) Banner pages at the beginning and end of the selected file division (end of record, end of file, BOI/EOI). The banner page will have the following header lines followed by the access level name in large characters in the center of the page.

FILE NAME = filename

DATE PRINTED = yy/mm/dd

USER NAME = username

ACCESS LEVEL = levelname

Command Format:

SECHDR,lfn,FF,CP=options.

lfn — File name to be receive header information.

FF — File is already formatted, i.e. carriage control is already present (page ejects and print density selection).

Option	Meaning
B	Print banner page at beginning and at end of each unit specified by the F or R option. If neither the F nor R options is specified, banner pages will be printed at the beginning of the file and at End-of-Information (EOI). The B option will be selected by default unless the P option is specified. Selection of the P option by itself deselects the B option; if both B and P options are desired they must both be explicitly selected.
F	Use logical files as the banner page unit. Selection of the F option also selects the B option.
R	Use logical records as the banner page unit. Selection of the R option also selects the B option.
P	Print page headings and footings on each page of output. Default for the P option is deselected. Selection of this option will deselect the B option. All combinations of the options are allowed.

A.3.3.3 SETFAL COMMAND.

The SETFAL command sets the security access level of a local file to the named level.

Format:

SETFAL,lfn,AL=levelname.

lfn Local file name. The file cannot be a direct access permanent file.

On an unsecured system, this command will be processed; the only checking will be to insure a valid levelname has been specified.

On a secured system, the specified levelname must be valid for the job and valid for the device where the file resides (mass storage or tape). In addition, if the specified levelname is a lower level than the current file access level, the user must be validated to lower the file access level. The command will be processed as a security violation if these conditions are not met.

A.3.3.4 SETJAL COMMAND.

The SETJAL command sets the security access level of the job to the named level.

Format:

SETJAL,AL=levelname.

On an unsecured system, this command is ignored except to check that a valid levelname has been specified.

On a secured system, the specified levelname must be valid for the job. If not, the command will be processed as a security violation. In addition, if the specified levelname is a lower level than the current job access level, the user must be validated to lower the job access level.

A.3.3.5 SETPFAC COMMAND.

The SETPFAC command sets the security access categories of a permanent file. Individual categories can be added or subtracted from the current category set, or an entire new set of categories can be specified.

Format:

SETPFAC,pfn,AC=cat1,cat2...,catn/PN=packname,R=r,WB,NA.

pfn Permanent file name.

catn or +catn — category names to add to the current category set of the file.

-catn — category names to subtract from the current category set of the file.

Example: SETPFAC,FILE,AC=CAT1,+CAT2,-CAT3.

Categories CAT1 and CAT2 will be added to the set. Category CAT3 will be subtracted from the set.

If the first category in the list is specified as 0, the rest of the list will be the entire new category set of the file.

Example: SETPFAC,FILE,AC=0,CAT2,CAT4.

Categories CAT2 and CAT4 will be the only categories set on the file.

On an unsecured system, this command will be processed; the only checking will be to insure that valid category names have been specified.

On a secured system, the specified categories must be valid for the job. If not, the command will be processed as a security violation.

If the permanent file is a direct access file and is currently attached by this or another job, File-Busy processing will be controlled by the WB and NA parameters.

A.3.3.6 SETPFAL COMMAND.

The SETPFAL command sets the security access level of a permanent file to the named level.

Format:

SETPFAL,pfn,AL=levelname/PN=packname,R=r,WB,NA.

pfn — Permanent file name.

On an unsecured system, this command will be processed; the only checking will be to insure a valid levelname has been specified.

On a secured system, the specified levelname must be valid for the job and valid for the device where the file resides. In addition, if the specified levelname is a lower level than the current file access level, the user must be validated to lower the file access level. The command will be processed as a security violation if these conditions are not met.

If the permanent file is a direct access file and is currently attached by this or another job, File-Busy processing will be controlled by the WB and NA parameters.

A.3.4 USER MACROS.

A.3.4.1 GETJAL MACRO.

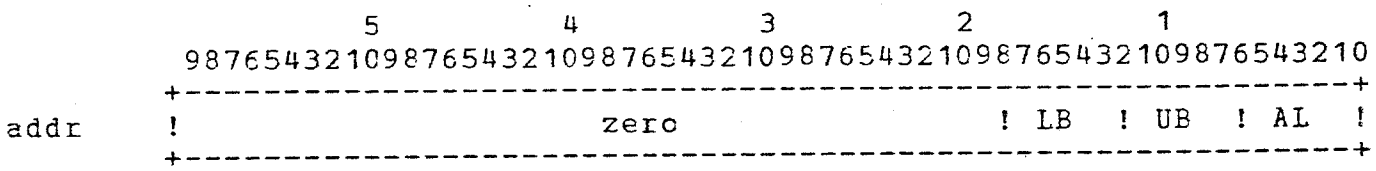
GETJAL (116)

The GETJAL macro returns the current job security access level and the job access level limits to the specified address.

Macro Format:

Location	Operation	Variable
	GETJAL	addr
addr	Address to receive job access level information	

The following information is returned to location addr:



UB Job Access Level Upper Limit.

LB Job Access Level Lower Limit.

AL Job Access Level.

A.3.4.2 OVWRITE MACRO.

OVWRITE (244)

OVWRITE writes a specified pattern of information to a file. This function is only valid for mass storage files.

Macro Format:

LOCATION	OPERATION	VARIABLE
	OVWRITE	addr,op,r

addr	Address of the FET.
op	Option to specify the pattern to be written. If op = "X", the file will be overwritten first with binary zeroes, then binary ones, then a pattern of alternating binary ones and zeroes. If op is omitted or any value other than "X", the file will be overwritten once with binary zeroes.
r	If r is specified, control is not returned until the operation is complete.

OVWRITE RETURN (254)

The OVWRITE RETURN function will perform an OVWRITE (244) function, followed by a return of the file. There is no macro to issue the OVWRITE RETURN function.

A.3.4.3 SETFAL MACRO.

SETFAL (007)

The SETFAL function sets the specified security access level on a file.

Macro Format:

LOCATION	OPERATION	VARIABLE
	SETFAL	addr,al

addr	Address of the FET for the file.
al	Access level tc set the file. If this one is one of the defined access level names, that level will be used. If not, al is used as the address of the location containing the desired access level.

A.3.4.4 SETJAL MACRO.

SETJAL (117)

The SETJAL macro changes the security access level of a job.

Macro Format:

LOCATION	OPERATION	VARIABLE
	SETJAL	a1

a1 — Access level to set on the job. If this is one of the defined access level names, that level will be used. If not, a1 is used as the address of the location containing the desired access level.

A.3.4.5 SETPFAC MACRO.

SETPFAC (022,CCAC)

The SETPFAC macro enables the user program to change the security access category set of a permanent file. This operation will not be performed if the file is direct access and currently attached by a job.

Macro Format:

LOCATION	OPERATION	VARIABLE
	SETPFAC	addr,pfn,cat,pn,r,sr

addr — Address of the FET. FET+0 must contain the local file name of the file.

pfn — Address containing the name of the permanent file whose category set is to be changed. If not present, the contents of FET+0 is used for the permanent file name.

cat — Address containing the new category set for the file. Bits 0-31 of this location are used; each bit controls whether the corresponding category is set.

pn — Address containing the name of the auxiliary device where the file resides.

r — Type of auxiliary device identified by the pn parameter.

sr — Special request subfunction (SSJ= only).

A.3.4.6 SETPFAL MACRO.

SETPFAL (023,CCAL)

The SETPFAL macro enables the user program to change the security access level of a permanent file. This operation will not be performed if the file is direct access and currently attached by any job.

Macro Format:

LOCATION	OPERATION	VARIABLE
	SETPFAL	addr,pfn,al,pn,r,sr

addr — Address of the FET. FET+0 must contain the local file name of the file.

al — Access level to be set on the file. If this is one of the defined access level names, that level will be used. If not, al is used as the address containing the desired access level.

pn — Address containing the name of the auxiliary device where the file resides.

r — Type of auxiliary device identified by the pn parameter.

sr — Special request subfunction (SSJ=only).

A.3.5 SYSTEM MACROS.

Use of the following macros is restricted to subsystems and SSJ= programs.

A.3.5.1 GETSSL MACRO.

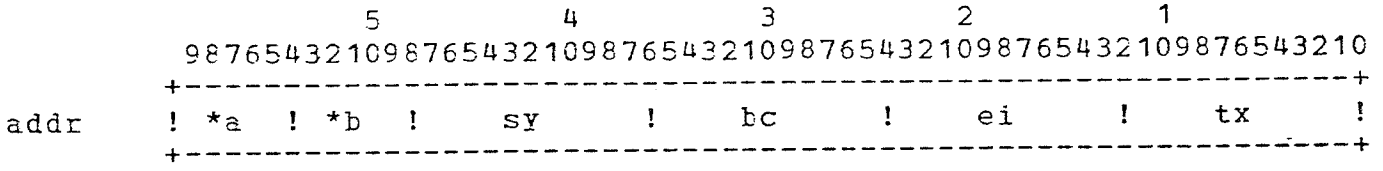
The GETSSL macro returns the Operating System Security Mode, Output Queue Special Handling Level and the Origin Type Access Limits to the calling program.

Macro Format:

GETSSL addr

addr Reply word address.

Reply Word Format:



*a Output Queue Special Handling Level.

*b Operating System Security Mode.

sy 6/ SYOT lower Access Limit.
6/ SYOT upper Access Level Limit.

bc 6/ BCOT lower Access Level Limit.
6/ BCCT uppper Access Level Limit.

ei 6/ EICT lower Access Level Limit.
6/ EIOT upper Access Level Limit.

tx 6/ TXCT lower Access Level Limit.
6/ TXOT upper Access Level Limit.

A.3.5.2 GETUSV MACRO.

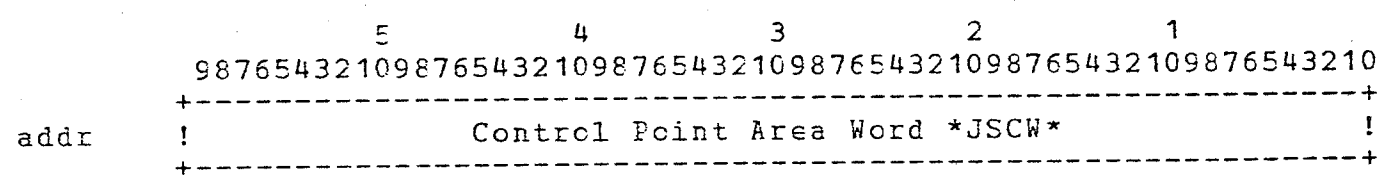
The GETUSV macro returns the user's security validations from Control Point Area word JSCW to the calling program.

Macro Format:

GETUSV addr

addr Reply word address.

Reply Word Format:



A.3.5.3 GETEAL MACRO.

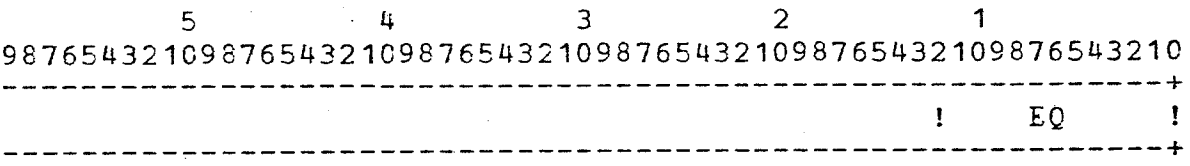
The GETEAL macro returns the equipment access limits of the specified EST ordinal to the calling program. If the equipment is mass storage, the device access limits from the MST will be returned.

Macro Format:

GETEAL addr

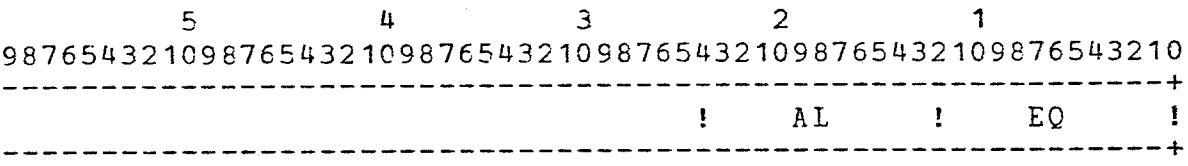
addr Request/Reply word address.

Request Word Format:



EQ EST ordinal

Reply Word Format:



AL 6/ lower access level limit
6/ upper access level limit

A.3.6 EQPDECK ENTRIES.

A.3.6.1 ACCESS ENTRY.

The equipment access level limits can be specified on the ACCESS EQPDECK entry. The default equipment access level limits are zero; no secure data can be read from or written tc the equipment. Equipment access level limits are meaningful for mass storage, magnetic tape and unit record type equipments; these values are ignored for other equipment types.

Entry Format:

ACCESS=nnn,lowerlevel,upperlevel.

nnn EST ordinal

lowerlevel access level name corresponding tc desired lower limit

upperlevel access level name corresponding to desired upper limit

A.4 COMMANDS/MACROS WITH NEW PARAMETERS.

A.4.2 OPERATOR COMMANDS.

A.4.2.1 UNLOCK COMMAND.

A new form of the UNLOCK command will be used to set security unlock status at the console.

```
UNLOCK,username,password.
```

If the specified user has Security Administrator privileges, security unlock status will be set.

On a secure system, the following commands are restricted to entry only when the console is in security unlock status.

```
DEBUG.
DIS,jsn.
DISABLE,ENGR.
ENABLE,ENGR.
QDISPLAY,jsn.
SECUREQ,EQnnn,LB=lb,UB=ub. (nnn is a unit record equipment)
SECURES,ot,LB=lb,UB=ub.
All memory entry commands
```

A.4.3 SYSTEM UTILITIES.

A.4.3.1 MODVAL.

A.4.3.1.1 K-DISPLAY.

New Page Format:

```
+-----------------------------------------------------------------------+
!                                                                       !
!                      USER              RCS2767     PAGE 4 OF 4.       !
!                                                                       !
!          CREATED    79/11/09.    UPDATED    81/09/08.                 !
!                                                                       !
!                                                                       !
!  CONTENTS                            DESCRIPTION                      !
!                                                                       !
!                        PASSWORDS MUST BE 4-7 CHARACTERS               !
!    XB =  YYMMDD.       BATCH PASSWORD EXPIRATION DATE.                !
!    XI =  YYMMDD.       INTERACTIVE PASSWORD EXPIRATION DATE.          !
!                                                                       !
!    SC =         55B    SECURITY COUNT (0-77B).                        !
!                                                                       !
!    SAL =       177B    SECURITY ACCESS LEVELS (1-7 CHARACTERS).       !
!                                                                       !
!    SAC = 37777777777B  SECURITY ACCESS CATEGORIES (1-7 CHARACTERS).   !
!                                                                       !
!    SAV =      7777B    SECURITY ACCESS PRIVILEGES (3-4 CHARACTERS).   !
!                                                                       !
!    SECURITY ACCESS PRIVILEGE IDENTIFIERS STARTING AT BIT 59 ARE -     !
!    CSAP COLD CPWX CFPX CLJL CLFL CWLF CULT                            !
!                                                                       !
+-----------------------------------------------------------------------+
```

A.4.3.1.2 DIRECTIVES.

A.4.3.1.2.1 SECURITY ACCESS LEVEL DIRECTIVE.

Directive Format:

SAL=level	level is one of the one - to seven-character symbolic names defined for access levels. It toggles a bit in the access level field (bits 43-36) in the security validation word. For each bit that is set, the corresponding access level is available to the user. Blanks are suppressed.
SAL=ALL	Sets all 8 access level validation bits.
SAL=NUL	Clears all 8 access level validation bits.

A.4.3.1.2.2 SECURITY ACCESS CATEGORY DIRECTIVE.

Directive Formats:

SAC=category. category is one of the one - to seven-character symbolic names defined for access categories. It toggles a bit in the access category field (bits 31-0) in the security validation word. For each bit that is set, the corresponding access category is available to the user. Blanks are suppressed.

SAC=ALL. Sets all 32 access category validation bits.

SAC=NUL. Clears all 32 access category validation bits.

A.4.3.1.2.3 SECURITY ACCESS PRIVILEGE DIRECTIVE.

Directive Format:

SAV=xxxx xxxx is a four-character designation that toggles a particular access privilege validation bit in the security validation word (bits 59-48). For each bit that is set, the corresponding special permission is allowed to that user. The bit is set when the identifier is first encountered and cleared if the identifier is used again. Blanks are suppressed.

xxxx	Bit	Description
CSAP	59	User is permitted Security Administrator privileges. This permission may not be cleared by the owner of this permission; the user executing MODVAL and clearing this permission may not be the user whose permission is being cleared.
COLD	58	User may execute On-Line Diagnostics.
CPWX	57	User may assign user password expiration term.
CFPX	56	User may assign permanent file expiration date or term.
CLJL	55	User may lower (downgrade) job access level.
CLFL	54	User may lower (downgrade) file access level.

CWLF 53 User may write tc or extend a lcwer level file (write-dcwn privilege).

CULT 52 User may write unlabeled magnetic tapes.

AV=ALL. Sets all multi-level security access privilege validation bits.

AV=NUL. Clears all multi-level security access privilege validation bits.

A.4.3.1.2.4 PASSWORD DIRECTIVES.

Directive Formats:

PW = pswd — This form is identical tc the current password directive implementation. This form will cause the passwords to be set to "pswd". Entry of this form will alsc cause the associated password expiration dates to be set to the default.

PB = pswd or PI = pswd — Sets the Batch (PB) or Interactive (PI) password to "pswd". This format causes the corresponding password expiration date to be set to the default.

A.4.3.1.2.5 PASSWORD EXPIRATION DIRECTIVES.

Password expiration dates may be specified by date-format entry.

Entry Format:

XD=yymmdd. Sets the password expiration date for the batch and interactive passwcrds to "yymmdd'.

XB=yymmdd. Sets the password expiration date for the batch password to "yymmdd".

XI=yymmdd. Sets the password expiration date for the interactive passwcrd to "yymmdd".

Password expiration dates may be alternatively specified by entry of a 1 to 4 octal digit expiration term value. This value will be added to the current date and the resultant date will be stored as the password expiration date.

Entry Format:

XT=nnnn.	Adds the value 'nnnn' in days to the current date to calculate the password expiration date. Valid values range from 0 to 4095 (decimal is assumed unless the postradix B is specified). The value of zero will set the password to immediately expired. This value can be used to temporarily disable a password without deleting it from the validation file. The value of 4095 (7777B) may be used to set a non- expiring password. The special character "*" may also be used to denote a non-expiring password. If the "XT' format is used the password expiration dates for both passwords will be set.
XTB=nnnn.	Same as XT but sets only the batch password expiration date.
XTI=nnnn.	Same as XT but sets only the interactive password expiration date.

A.4.3.1.3 LIMITS OUTPUT.

The following sections will be added to the output from the LIMITS command.

```
THE FOLLOWING ARE VALID SECURITY ACCESS LEVELS -

    LVL0
    LVL1
     .
     .
    LVL7

THE FOLLOWING ARE VALID SECURITY ACCESS CATEGORIES -

    CAT00
    CAT01
     .
     .
     .
    CAT31
```

THE FOLLOWING ARE VALID SECURITY ACCESS PERMISSIONS -

WRITE UNLABELED MAGNETIC TAPES
WRITE TO OR EXTEND A LOWER LEVEL FILE
LOWER FILE ACCESS LEVELS
LOWER YOUR JCB ACCESS LEVEL
ASSIGN PERMANENT FILE PASSWORD EXPIRATION DATE
ASSIGN USER PASSWORD EXPIRATION DATE
EXECUTE ON-LINE DIAGNOSTICS
SECURITY ADMINSTRATOR PRIVILEGES

If the user is not valid for any levels/categories/permissions, that section and its associated header will be suppressed. The access levels and categories listed will be the symbolic names defined in COMSMLS.

The following lines will be added to the "OTHER CHARACTERISTICS" section of the LIMITS command output.

BATCH PASSWORD EXPIRATION DATE - YY/MM/DD.
INTERACTIVE PASSWORD EXPIRATION DATE - YY/MM/DD.

If the password is non-expiring, the word NONE will replace the date field.

A.4.3.2 MSI (INITIALIZE).

The LA and UA options are added to set the device access level limits during on-line initialization.

LA = One - to seven-character access level name. This sets the security access level lower limit for the device being initialized. No data with an access level lower than this may reside on this device. This option is legal only on a total initialize of a device.

UA = One - to seven-character access level name. This sets the security access level upper limit for the device being initialized. No data with an access level higher than this may reside on this device. This option is legal only on a total initialize of a device.

These options will be added to the K-display as follows:

LA = level SECURITY LEVEL LOWER LIMIT
UA = level SECURITY LEVEL UPPER LIMIT

A.4.3.3 PERMANENT FILE UTILITIES.

The LA and UA parameters are added to all of the Permament File Utilities to select a range of access levels to process. See section 6.40 for additional information.

LA = level — One - to seven-character access level name to set the lower bound of the range of access levels to process. If this parameter is specified, UA must also be specified. If neither LA nor UA is specified, the default is that all access levels are selected.

UA = level — One - to seven-character access level name to set the upper bound of the range of access levels to process. If this parameter is specified, LA must also be specified. If neither LA nor UA is specified, the default is that all access levels are selected.

These parameters will be added to the second page of the K-display as follows:

Option		Value	Description
LA	=	0	LOWER SECURITY ACCESS LEVEL
UA	=	0	UPPER SECURITY ACCESS LEVEL

A.4.3.4 QUEUE UTILITIES.

The LA and UA parameters are added to all of the Queue Utilities to select a range of access levels to process. See section 6.41 for additional information.

LA = level — One - to seven-character access level name to set the lower bound of the range of access levels to process. If this parameter is specified, UA must also be specified. If neither LA nor UA is specified, the default is that all access levels are selected.

UA = level — One - to seven-character access level name to set the upper bound of the range of access levels to process. If this parameter is specified, LA must also be specified. If neither LA nor UA is specified, the default is that all access levels are selected.

These parameters will be added to the K-display as follows:

Option		Description
LA	=	LOWER SECURITY ACCESS LEVEL (1-7 CHARACTERS)
UA	=	UPPER SECURITY ACCESS LEVEL (1-7 CHARACTERS)

Access level will be added to the QAITER/QFTLIST LIST=qft command display.

```
                    *** ACTIVE QUEUE LIST ***

      JSN          =  AAAQ          ORDINAL    = 3
      ORIGIN =     =  REMOTE        QUEUE      = PRINT

   DESTINATION                   CREATION
      FAMILY       =  SYS964        FAMILY     = SYS964
      LID          =  M64           LID        = M64
      USER         =  GAK2741       USER       = GAK2741
      TUI/ID       =  2741          USR INDX   = C

      FORMS        =  AX            USR JCBNM  = J0
      DISP CODE    =  LP            DATE       = 82/01/13
      EXT.CHR.     =  LP            LENGTH     = 41
      INT.CHR.     =  DIS           REPEAT     = 0

   RESIDENCE                       INTERRUPT  = NO
      FAMILY       =  SYST64        PRIORITY   = 366
      DEVICE       =  1             ACCESS     = LVL3
```

A.4.4 USER COMMANDS.

A.4.4.1 JOB CARD.

The AL parameter is added to the JCB card as follows:

Positional format:

```
ujn,p,t,fl,fe,lid,sc,level.cm
```

Keyword format:

```
ujn,ALlevel.
```

Equivalence format:

```
ujn,AL=level.
```

Description

One - to seven-character access level name specifying the maximum security access level the job can attain. The default is the lowest access level for which you are validated (refer to the LIMITS command).

A.4.4.2 ASSIGN/LABEL/REQUEST/COMMANDS.

When requesting file assignment with the ASSIGN, LABEL or REQUEST commands, an access level different from the current job access level can be specified with the AL parameter. If operator assignment is required, the assigned equipment must allow the specified access level.

AL = level	One - to seven-character access level name specifying the access level to set on the assigned file.

A.4.4.3 PERMANENT FILE COMMANDS.

New parameters are added to the CHANGE, DEFINE, PERMIT and SAVE commands to specify a password or permit expiration date or term. When used with the DEFINE and SAVE commands, these parameters can only be used if the PW parameter is also used. Users must be validated to use these parameters.

Parameter	Description
XT=nnnn	Specifies the number of days to add to the current date to define the expiration date of the password or permit.

nnnn	expiration term
0	Sets the password or permit as immediately expiring. This can be used to temporarily prevent access to a file by alternate users.
1-4094	Sets the password or permit expiration term to the specified number of days.

4095 or * Sets the password or permit as non-expiring.

The default expiration term is installation controlled; the largest value allowed to be specified is also installation controlled (but it must be less than 4096).

XD=yymmdd Specifies the expiration date for the password or permit. This date must be within the maximum allowed term. The default is the date calculated by adding the default expiration term to the current date.

A.4.4.4 PASSWORD COMMAND.

New parameters are added to the PASSWOR command to set the expiration date of the user password by specifying a date or term. Users must be validated to use these parameters.

Format:

PASSWOR,oldpassword,newpassword,XD=yymmdd.

or PASSWOR,oldpassword,newpassword,XT=nnnn.

The XD and XT parameters and their values are processed identically to the way they are processed for the permanent file commands. See section A.4.4.3.

These parameters may be used to change the expiration date of an existing password without changing the password itself. They may also be used when the parameter values are read from file INPUT.

Once a password for a user name has expired, no system access is allowed under that user name until a new expiration date is entered with the MODVAL utility.

A.4.4.5 CATLIST COMMAND.

The following is the new format generated by CATLIST,LO=F. The access level and password expiration date are added.

```
FILE NAME ACCESS FILE-TYPE LENGTH DN
 PASSWORD MD/CNT INDEX PERM.  SUBSYS
  EXPIRES   LEVEL  PR BR RS

1 FILEXXX  DIR. PRIVATE      9999 40
  PASSWRD   8888        MODIFY BASIC
  82/10/01  SECRET N  Y  D
```

The LO=X option is added to CATLIST.

X Lists security access categcries for the file named by the FN=pfn option. All informaticn that LO=F lists is also included.

The followcng is the new format generated by CATLIST,LO=FP, FN=filename. The PERMIT expiration date is added, if present.

```
USER NUMBER    PERM.    EXPIRES   ACCESSES  DATE      TIME

  1. ABCDEFG   WRITE*  82/09/29.      5555  82/09/29. 10.10.10.
```

A.4.4.6 ENQUIRE COMMAND.

ENQUIRE,OP=B. will return the fcllcwing infcrmation.

SYSTEM ACTIVITY.

JOB ACCESS LEVELS

CURRENT	LVL2
LOWER LIMIT	LVL0
UPPER LIMIT	LVL5
ACCESS CATEGCRIES	CAT01
	CAT05
	CAT20
	CAT21

ENQUIRE,OP=F. will return the fcllowing infcrmation.

LOCAL FILE INFORMATION.

FILENAME	LENGTH/PRUS	TYPE	STATUS	FS	LEVEL
INPUT*	1	IN.*	ECR	NAD	LVL2
ABC	5	LO.	BOI		LVL5

ENQUIRE,JSN=jsn. will return the following information as the first line for an executing job or queued file.

```
 JSNN.C.LID.EXECUTING              UJN=JCBNAME.   LEVEL=LVL0.
```

A.4.5 USER MACROS.

A.4.5.1 PERMANENT FILE MACROS.

The XT parameter is added to the SAVE, PERMIT, DEFINE and CHANGE macros to specify a password or permit expiration date/term.

SAVE addr,pfn,pwd,ucw,ct,m,pn,r,fo,ss,br,,,xt

PERMIT addr,pfn,un,m,pn,r,fo,,xt

DEFINE addr,pfn,pwd,ucw,r,ct,m,pn,s,fo,br,pr,,xt

CHANGE addr,ofn,nfn,pwd,ucw,ct,m,pn,r,fo,ce,ss,
br,pr,xt

xt Address of word containing password or PERMIT expiration date or term. This value is placed in FET+15B, bits 0-17. PFM will process this field in the following manner.

If bits 12-17 are zero, bits 0-11 contain the number of days to add to the current date to calculate the password or PERMIT expiration date.

If bits 12-17 are non-zero, the entire field is processed as a packed expiration date.

A.4.6 CONSOLE DISPLAY CHANGES.

A.4.6.1 LEFT SCREEN HEADER.

```
JSN=AACR ENGR 99 MID=72.   VERSION HEADER
JSNN STEP  444  SECURITY-UNLOCK DEBUG  LOWIEVL-UPPLEVL
```

A.4.6.2 E,A DISPLAY.

```
 EQUIPMENT STATUS TABLE.  ADDRESS =1234. INDEX =12.

EST TYPE STAT JSN  EQ UN CHANNELS          SECURITY RANGE

 3. DI-2  ON  JSNB  4.26. 4. 24.           LVL6    LVL7
53. MT    OFF       5.  .31. 33* 11. 13.   LVL0    LVL3
60. LP    ON  JSNA  7. 4.12.
```

A.4.6.3 E,P DISPLAY.

To be provided.

A.4.6.4 E,T DISPLAY.

```
 EST  VSN       DEN RING FMT  JSN    STATUS  SECURITY RANGE

MT51  SCRATCH 6250  IN  SI  AABC    IOADPT  LVL5     LVL6
      UNLABELED          REEL=1234.  MODE=BC
```

A.4.6.5 I DISPLAY.

```
BIO STATUS.
 JOB    EST  TRAIN  ID  EC   REP   SECURITY RANGE
ZZ20    CR20.                     LVL1     LVL5

*IDLE*  LP40.    1   3. AF      .  LVL0     LVL5

JSNA    LP42.    7  10.         4.  LVL6     LVL7
```

A.4.6.6 J DISPLAY.

```
EJTO    CP      UI     FM         PN       CS  CONN    JAL
1234. 1200. 123456. FAMNAME   PAKNAME   ON  1234. JACCLVL

    P       RA    FL     RAE   FLE   SRUA    SRUL
123456.  12345. 1122.  12345. 1234. 123333. 123400.

EQ= 14. 15. 16. 17. 20. 21. 22. 23. 24. 25. 26. 27.

ASSEMBLING LIBEDIT.
TRACK LIMIT.  EQ 5.

REWIND,LGO.
LIBEDIT.
REWIND,NEW,TAPE.
COPYEI,NEW,TAPE,V.
```

A.4.6.7 Q DISPLAY.

```
Q.                        FREE=1234. ADDRESS= 11300. INDEX=1234.

      JSN SC QFT     QP  QT  LID DS  ID  FC  EC    AL

     AAAB B  1234. 4474. LP  AAA BC  20. AF  A9  LVL3
```

A.4.6.8 R DISPLAY.

ADDRESS=123456. INDEX=1234.

JSN	SC	EJT	SPR	RO-FL	RC-FLE	ST	AL
AAAC	B	1234.	1234.	1234.	1234.	RO*	LVL3
AAAL	S	2222.				PF	LVL2
AAAR	R	3333.	123.			TE	IVL7

A.4.7 BANNER PAGE

```
+-----------------------------------------------------------------+
!                                                                 !
!                                                                 !
!OPERATING SYSTEM = NOS 2-5A50T/R1C.  82/04/15. PRINTED = 82/05/11.!
!                                                          12.45.35.!
!                                                                 !
!UJN          = ABZG  FAMILY       = NOSCLSH  JOB ORIGIN  = BATCH.  !
!CREATING JSN = XYAB USER NUMBER = GRZABB   SERVICE CLASS = BATCH. !
!                                            ACCESS LEVEL = "text" !
!                                                                 !
!                                                                 !
+-----------------------------------------------------------------+
```

A.5 CMR TABLE CHANGES.

See section 5.

A.6 NEW FUNCTION REQUESTS.

New and changed function requests for PP processors are listed here. These changes are described elsewhere in the GID, as noted.

A.6.1 CIO.

1. Bits 18-35 of the RA+1 call are used for the OVWRITE function option, as well as for skip count. This field is 1 for the 'X' option, 0 otherwise. See section A.3.4.2.

2. New functions OVWRITE (244) and OVWRITE RETURN (254) are added. See section A.3.4.2.

3. Bit 39 in FET+1 ("sp" bit) and bits 36-38 in FET+4 are used as described in section 5.6 and 6.30.

A.6.2 CPM.

New functions 116, 117 and 120 are added as described in section A.3.4.1, A.3.4.4 and A.3.5.2 respectively.

116	GETJAL	Get job access level limits.
117	SETJAL	Set job access level.
120	GETUSV	Get user's security validations (SSJ=only).

A.6.3 LFM.

1. LFM functions 13, 14 and 15 use FET+1 and FET+4 fields. See section 6.6.

2. LFM function 7 is added.

007	SETFAL	Set file access level.

3. LFM function 25 (GETFNT) returns file access level. See section 6.6.5.

A.6.4 PFM.

1. PFM uses new FET fields as described in section 5.6.

2. New functions.

022,CCAC	SETPFAC	Set security access categories for file.
023,CCAL	SETPFAL	Set security access level of file.

A.6.5 QAC.

New parameter block fields and flags are described in section 5.7.

A.6.6 SFM.

New functions are added. See section 6.14.

33	GSSF	Get system security status. (SSJ= only).
34	GEAF	Get equipment access level limits (SSJ= only).

A.6.7 MONITOR FUNCTIONS.

Changes to monitor functions and the new VSAM monitor function are described in section 5.8.

A.7 ERROR MESSAGES.

Most of the new and changed messages are described in the sections referring to the decks that issue them. A complete list will be provided for this section.

A.8 INSTALLATION PARAMETERS.

A.8.1 COMSACC PARAMETERS.

Parameter	Default	Significance
APXL	7777B	See section 6.1.13.
APXT	7777B	See section 6.1.13.

A.8.2 COMSPFM PARAMETERS.

Parameter	Default	Significance
FPXL	7777B	See section 6.1.20.
FPXT	7777B	See section 6.1.20.

B.0 APPENDIX B - ACCOUNTING DAYFILE MESSAGES.

This appendix describes the Acccunting Dayfile messages added to the system by the Multi-Level Security project.

B.1 MULTI-LEVEL SECURITY MESSAGES.

A new Accounting Dayfile Message group is defined for logging Multi-Level Security events. The new information group is denoted by the initial letter "M". The general format of the "M" message group is as follows:

Meac, additional information.

e — Event descriptor character. The meaning of the individual event designator characters are described below.

e	Description
F	Local file security activity.
J	Job Access Level activity.
P	Permanent File security activity.
S	System operaton security activity.
U	User security activity.

ac — Activity being recorded. The meaning of the individual activity disignators will be described with the event designator characters with which they are associated below.

B.1.1 F-ACTIVITY (LOCAL FILE) MESSAGES.

MFFA, filenam, levelname.
MFFI, filenam, levelname.

MFFA — Denotes a change of the access level of the filenam to level levelname.

MFFI — Denotes an invalid attempt to change the access level of local file filenam to level levelname.

B.1.2 J-ACTIVITY (JOB ACCESS LEVEL) MESSAGES.

MJJA, oldlevel, newlevel.
MJJI, oldlevel, newlevel.

MJJA — Denotes a user change of the job access level from level oldlevel to level newlevel by use of the SETJAL control statement or macro.

MJJI — Denotes an invalid attempt by the user to change the job access level from level oldlevel to level newlevel using the SETJAL command or macro.

B.1.3 S-ACTIVITY (SYSTEM OPERATION) MESSAGES.

MSSA, username.
MSSI, username.
MSEQ, EQnnn,LA=level,UA=level.
MSOT, ot,LA=level,UA=level.

MSSA — Security unlock status has been set at the console with user name username.

MSSI — An invalid attempt was made to set security unlock status at the console with user name username.

MSEQ — The equipment access level limits for unit record equipment EQnnn have been changed by the operator.

MSOT — The origin type access level limits for origin type ot have been changed by the operator.

B.1.4 U-ACTIVITY (USER OPERATIONS) MESSAGES.

MUPW.
MUPX.

MUPW — Indicates user change of user password.

MUPX — Indicates user change of password expiration date.

B.2 PERMANENT FILE MESSAGES.

The following is a list of the P (Permanent File) activity messages added by the Multi-Level Security project.

```
SPAX, filenam, usernam, packnam.
SPGX, filenam, usernam, packnam.
SPAC, filenam, usernam, packnam.
SPAL, filenam, usernam, packnam.
```

SPAX — Indicates that the user has attempted to ATTACH file filenam, on pack packnam, from alternate user usernam, and has been denied access for any reason (File-Not-Found error).

SPGX — Indicates that the user has attempted to GET file filenam, on pack packnam, from alternate user usernam, and has been denied access for any reason (File-Not-Found error).

SPAC — Denotes permanent file SETPFAC operation.

SPAL — Denotes permanent file SETPFAL operation.

C.0 APPENDIX C - FUTURE CONSIDERATIONS.

The current Multi-level Security design meets the requirements for providing a secured operating system as outlined by the U.S. Department of Defense ADP Security Manual, DoD 5200.28-M, as implemented on a single-mainframe, stand-alone type secured system.

Large, complex systems are becoming more common, however, as many ADP installations are moving away from the concept of a single, monolithic, central computer. There is no doubt that CDC is aware of this and is actively involved in the development of commercial, standard distributed computing networks. The next step, then, in providing Multi-Level Security capability to the ADP community is to extend MLS to CDC's distributed systems.

Some other areas also are addressed in this section, not necessarily related to the problem of distributed or networking systems, but more general in nature and applicable to single mainframe systems or distributed systems.

C.1 RHF/LCN.

Transmission of data among networks of linked computer systems, possibly from different manufacturers, with no CDC control of the mandatory access policies toward classified information in other manufacturers' systems, may require a prohibitive policy toward MLS on RHF/LCN systems. It appears at this time that there are too many variables outside the control of the CDC security mechanisms to be able to provide an acceptably trusted system. This area definitely needs More study if MLS is to be implemented on RHF/LCN.

C.2 MULTI-MAINFRAME.

We have been providing multi-mainframe systems now for several years. The logical next step in MLS will be to extend MLS to multi-mainframe systems to allow concurrent processing of classified information at different sensitivity levels. Possible implementations would be:

(a) Concurrent processing on secured mainframes.

(b) Concurrent processing on a mix of mainframes, where certain mainframes would be secured and others would be unsecured.

C.3 SHARED RMS.

Providing Multi-level Security on shared RMS systems may require a dual approach, as many users' security requirements will call for a total prohibition of sharing classified information except when shared by secured systems. Other users will want to share devices among a mix of secured and unsecured systems with the operating system(s) to provide the necessary mandatory access controls.

C.4 CLASSIFIED MAGNETIC TAPES.

The problem of transportability of classified data recorded on magnetic tapes has come up often in discussions on the general subject of multi-level security. The problem involves both providing access controls on tapes generated by a CDC MLS system and providing access controls on tapes generated by another system. Unfortunately there is no common industry standard for identifying classified magnetic tape data other than by the Volume and File Accessibility fields of the ANSI standard label, and these fields were not designed for system policy control. They were designed instead for user access control, but could be adopted for MLS access control with the loss of the user access control capability.

C.5 FUTURE OPERATING SYSTEMS.

With the Government's declared intention to require certified, secure operating system classification of the systems to be sold to the government in the future (when the classification requirements become official), providing MLS under NOS V2 will no longer be sufficient. We will definitely be required to provide a certified, secure system on our future operating systems as well in order to just meet RFP requirements.

Since the U.S. Government is one of our major customers, future CDC operating systems under development or in the planning stage should incorporate provisions for a Multi-Level Security mechanism. This MLS system should be designed to cause the minumum amount of trauma to an installation attempting to migrate from the NOS V2 MLS system, as to an upgrade or successor product, for instance.