Burroughs Corporation
COMPUTER SYSTEMS GROUP
SANTA BARBARA PLANT

PLANT IDENT	0 1 4

DOCUMENT TRANSMITTAL

PAGE ____ OF ____

CONTROL DOC.	REV
None	

SYSTEM/PRODUCT B1800/B1700 DISTRIBUTION TYPE ____

UNIT NAME ____ PROJ. NO. ____

COORD. ____ CHKR. J Hale RECORDS ISSUE DATE 1 15 81

DOC PFX OR DWG SIZE	DOCUMENT NUMBER	REV OR ISSUE	DOCUMENT DESCRIPTION	ENG. RECORDS ONLY				REMARKS
				QTY REV PAGE	COPIES EACH PAGE	BOND	VELLUM	
P.S.	2219 0102	G	FILE SECURITY	54	63			
DOCUMENT TRANSMITTAL								

SBP 1085 REV 8-78

PRODUCT SPECIFICATION

REV LTR	REVISION ISSUE DATE	APPROVED BY	REVISIONS
F	7/31/80		Changes for MARK 10.0 Release
			2-1 Added Security Level bit.
			2-4 Updated Syntax.
			2-5 Added "SL" option to Semantics.
			Updated Restrictions discription.
			2-9 Added "SL" to ADD syntax and semantics.
			2-11 Added "SL" to CHANGE syntax and semantics.
			3-1 Replaced "DUMP TO PAYROLL =/=" with "COPY =/= TO PAYROLL".
			3-2 Updated "PUBLIC FILES".
			3-3 Updated "READ-ONLY FILES".
			3-6 Added "SECURITY LEVELS".
			4-1 Deleted "PTN" and "PIO" from ODT command.
			4-2 Deleted "PIN or PROTECTION" and"PIO OR PROTECT.ID" from file attributes.
G	1/14/80		Changes for MARK 10.0 Release
			2-1 Updated "TYPES and LENGTHS" of fields.
			2-2 Updated "NO. 4" Syntax Diagram Conventions.
			2-3 Added "IDENTIFIER" term.
			2-4 Updated "SYNTAX".
			2-6 Updated "SEMANTICS".
			2-7 Added new example of Line Printer Output.
			2-8 Added "*ANY" and "*NONE" notes.
			2-11 Updated "ADD" syntax and semantics.
			2-13 Updated "CHANGE" syntax and semantics.
			2-16 Updated "CREATE" semantics.
			2-19 Added "DISPLAY" syntax and semantics.
			2-22 Updated "LIST" syntax and examples.

Burroughs Corporation

COMPUTER SYSTEMS GROUP
SANTA BARBARA PLANT

B1800/B1700 FILE SECURITY

PRODUCT SPECIFICATION

REV LTR	REVISION ISSUE DATE	APPROVED BY	REVISIONS
G			Changes for MARK 10.0 Release cont. 2-25 Updated "ODT MESSATES" by deleting number 21 and removing all the numbers before the statements.

PRODUCT SPECIFICATION

REV LTR	REVISION ISSUE DATE	APPROVED BY	REVISIONS
D	7/17/78	J. Hale	1-2 Updated private access rights sentence. 2-1 Changed Security bit to Public bit. Added Override bit. 2-5 Deleted *PRIV paragraph. Updated SPO message sentence. 3-2 Updated key words PROTECTION sentence. Updated US PAYROLL/ACCT header example. 3-3 Added SECURITYTYPE and SECURITYUSE to file equation. Updated file equation explanation. Added SEC and SUS to file header. 3-4 Deleted "filename" and replaced with "multifile-id" to a secure file sentence. Deleted "file-identifier" and replaced with "multifile-id" to asterisk precedes sentence. 3-8 Added RB and RF to SPO COMMANDS. Updated USER PAYROLL/ACCT RB =/= syntax explanation. 3-11 Changed "password" to "usercode" in remote users sentence. 4-1 Added SEC and SUS to SPO command. 4-2 Added SEC or SECURITYTYPE and SUS or SECURITYUSE to the FPB fields. Changes for MARK VIII.0 Release
E	8/22/79	J. Hale	Changes for MARK 9.0 Release Replaced SPO with ODT throughout. 2-4 Updated syntax. 2-5 Added *NONPRIV and PRIVATE to options and attributes. Added US Y to Example. Replaced *PRIV with Security. Replaced PUBLIC with SECURITY. 2-6 Replaced *SYS PACK with *SYS DISK. Updated *PRIVILEGED USER*. 2-8 Deleted CREATE throughout COMMAND RESTRICTIONS section. Added sentence dealing with CREATE. 2-9 Updated syntax. Added PRIVATE and *NONPRIV to options and attributes. 2-10 Updated Note. Added US=BERTHA to Example. 2-11 Updated syntax. Added PRIVATE, *PRIV, and *NONPRIV to options and attributes. 2-12 Added CHA BERTHA/= to Example. 2-23 Added 26 and 27 to OUTPUT SPO ERROR MESSAGES.

BURROUGHS CORPORATION
COMPUTER SYSTEMS GROUP
SANTA BARBARA PLANT

TABLE OF CONTENTS

FILE SECURITY

INTRODUCTION

B1800/B1700 systems support a file-security mechanism which protects disk files against accidental or deliberate misuse. A secure file, for example, cannot be removed, changed, or referenced in any way by an unauthorized user. This document provides a basic introduction to the current file security mechanism provided by the B1800/B1700 MCP.

File security is based, essentially, on one aspect of file-naming convertions that have existed since the inception of B1700 disk files: the concept of the multifile-identifier. If the multifile-identifer is enclosed in parentheses, e.g., (PAYROLL)/<filename>, and designated as a PRIVATE file in the Disk File Header (DFH), the file is a secured file. A large portion of this document, then, is devoted to explaining the proper conditions under which file names with secure multifile-id's can be accessed and created.

Disk file security is an optional feature as far as the B1800/B1700 operating system is concerned. However, once the system is invoked, there are well-defined rules for its use. It should be noted, also, that file security is not limited to datacomm activity but applies to both batch and remote modes of operation, even though its greatest application is in the area of datacomm operations.

This document provides a full discussion of both batch and remote applications of file security. It describes the structure of disk files created under file security and explains how to operate programs that access secure files.

SECURE FILE IDENTIFIERS

Disk file security is maintained through control of the multifile-id since secure files may only be created with names of: (<multifile-id>)/<file-name>. When a new secure file is created, the multifile-id given to the operating system is taken from the usercode field in the (SYSTEM)/USERCODE file. In the context of file creation, the multifile-id and the usercode are functionally the same.

Secure files are also controlled through specification of a pack-id that is associated with every usercode/password. If a user pack-id is blank, files are created, by default, on the system disk. One practical implication of this system is that the operating system cannot locate any secure disk file without going to the (SYSTEM)/USERCODE file. If the system usercode file is not present, secure files cannot be located or processed by the operating system, even though they are actually resident on disk.

When accessing (reading) a secure file, the operating system goes to the system usercode file for the location of the file (pack-id) and checks the Disk File Header (DFH) for access rights (PRIVATE or PUBLIC). If the file is found and the access rights are PUBLIC, then any user can access the file. If the rights are PRIVATE, it can be accessed only by a privileged user or by a program running under the same usercode. Access rights defined in the usercode file are used when creating a new file. When accessing an old file, security is taken from the header.

RELATED DOCUMENTATION

Name	Number
B1800/B1700 MCP II	P.S. 2212 5426
B1800/B1700 Software Operational Guide	1068731
B1800/B1700 HOST/RJE	P.S. 2212 0126

SYSTEM/MAKEUSER

The file-security system is initiatec by creating a system user-code file through SYSTEM/MAKEUSER. Input to SYSTEM/MAKEUSER consists, basically, of usercode/password pairs in a format which is defined in the USERCODE ATTRIBUTES section below. The program creates a usercode file, called (SYSTEM)/USERCODE, which contains a list of valid usercode/passwcrd pairs. Any batch program or remote user which attempts to create a secure file with a multi-file-id (i.e., usercode) that is not in this file or not his own will be denied the opportunity to do sc by the MCP.

Access to usercode-related files is also controlled through the use of PUBLIC and PRIVATE attributes that are stored as part of the disk file header. Public files are able to be accessed by any users, but private files are available only to their owners or privileged users. Usercodes can be defined as PRIVILEGED in the (SYSTEM)/USERCODE file if users wish to allow certain user-codes to access (read) private files and write them back to disk.

SYSTEM/MAKEUSER is a normal-state utility program used to create, access, or modify (SYSTEM)/USERCODE, the system usercode file of allowable usercode and password combirations. Variable fields are termed "usercode password entry attributes" and define the characteristics of the individual entries (maximum number = 1023). The declared types and lengths of these fields are:

Usercode	-	10 characters
Password	-	10 characters
Pack-id	-	10 characters
Charge number	-	24 bits
User priority	-	4 bits
Privileged bit	-	1 bit
Security	-	1 bit
Override	-	1 bit
Security level	-	2 bits
Maximum Time(Minutes)	-	16 bits
BNA Hostname	-	17 characters

SYNTAX DIAGRAM CONVENTIONS

Syntax diagrams display the required format for usercode attrib-utes and input commands, and the rules of such diagrams are:

1. Any path traced along the forward direction of the arrows will produce valid syntax.

2. Any bridge over a digit may be traversed the maximum number of times specified by a digit. If the digit is followed by an "*", then the path must be crossed at least one time.

a. ----/1\----> = MAY be traversed only once.

b. ----/1*\---> = MUST be traversed once.

3. Upper-case letters in the syntax diagrams indicate keywords which are literally in the commands. Minimum abbreviations are indicated by underscoring.

4. End-of-statement is indicated by:

----------># .

Comments after the final operand may be preceded by a "%".

5. Lower-case letters, words, and phrases are syntactic variables, which represent information to be supplied by the user. (See DEFINITION OF TERMS below.)

DEFINITION OF TERMS

The following section defines the syntactic variables NAME, INTEGER, USERCODE SPECIFIER and INPUT FILE NAME, IDENTIFIER, as well as the delimiters used in the command syntax diagrams.

Name:	a string of up to 10 alphanumeric characters, excluding blanks and delimiters. A name may be a null string, which is defined as two adjacent quote signs ("").
Integer:	a string of only numeric characters.
Delimiters:	the following special characters: blanks (""), equal sign (=), and slash (/).
Family:	a group of usercode/password combinations that all have the same usercode.
Null String:	two adjacent quote marks (""). Space is not allowed between them.
Usercode Specifier:	consists of a character string of up to eight characters for a usercode and separated from the password, which may contain ten characters, by a slash (/). The first name is the usercode, and the second name is the password. An optional form is available using the character "=" as the password. This indicates all usercodes of

the first name. The null string is allowed as the password name, and results in a password of blanks.

Password Specifier: consists of a character string of up to ten characters. A blank password may be specified as a null string ("").

Examples:

a. (JOE)/PASSWORD1
b. JOE/PASSWORD2
c. JOE/=
d. JOE/""

Input File Name consists of up to three character strings, of up to ten characters each, separated by the character "/", to form a standard MCP-recognizable file name. Note that the "=" form and the null string are not allowed in filenames.

Examples:

a. MYFILE
b. USERCODE/MYFILE
c. MY.PACK/USERCODE/MYFILE

User Job Priority denotes, by integer, the highest priority at which a batch job can be run. This prevents a user at a remote terminal from running a job at a higher priority, for example, than a network controller.

Identifier A string of up to 17 characters for use as BNA hostname. Lower case will be translated to upper case and underscore will be translated to a minus sign.

USERCODE ATTRIBUTES

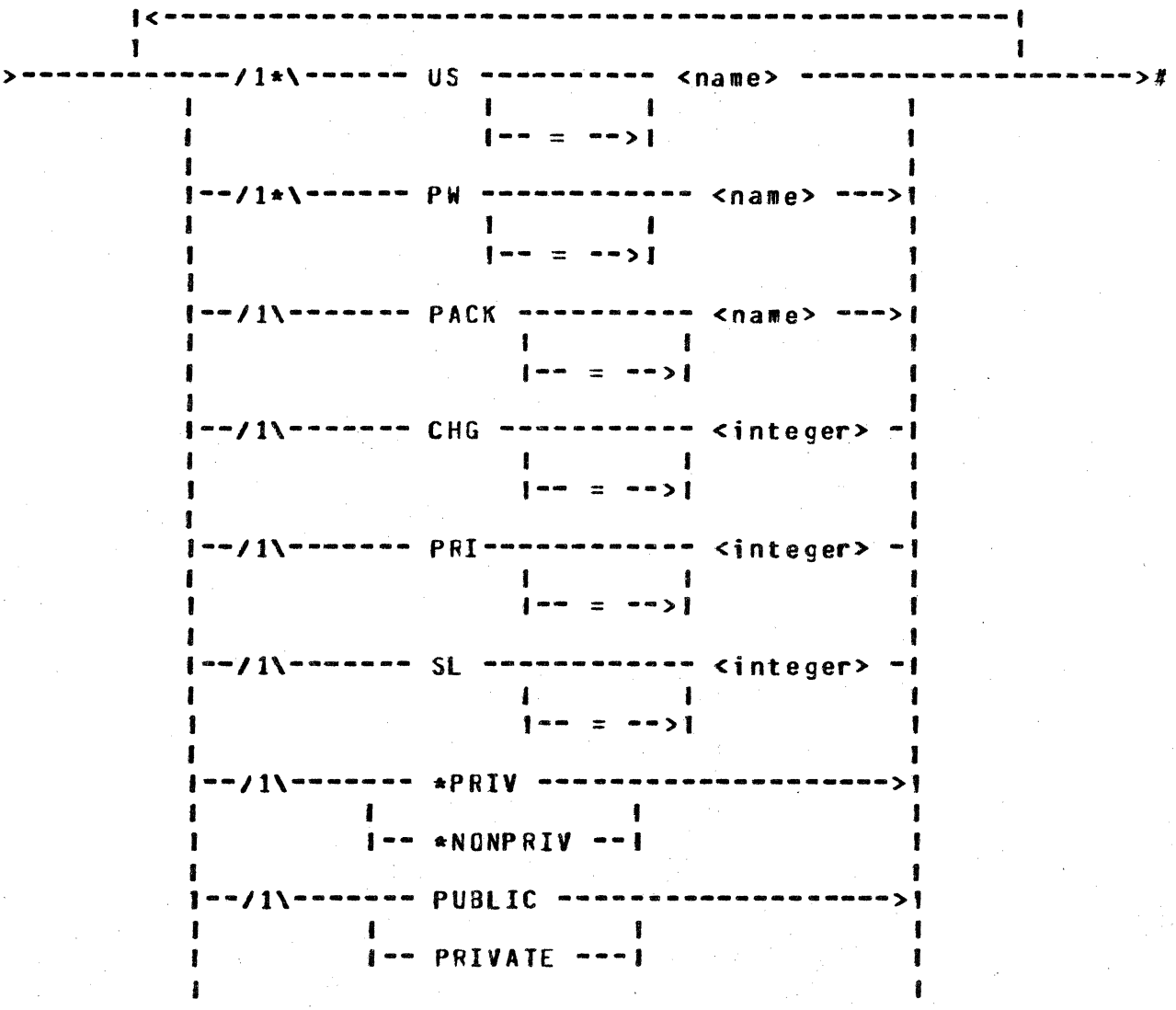
Input to SYSTEM/MAKEUSER requires the syntax:

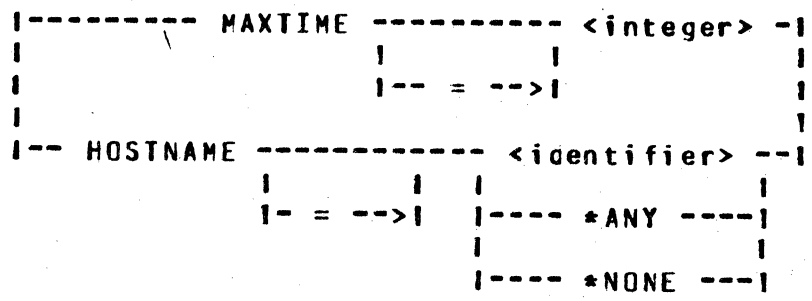
<keyword> = <attribute>

where <keyword> is one of the valid keywords listed below, the equals sign is optional, and <attribute> is a character string or integer which does not exceed the length specified for the attributes. The keyword options US and PW are required, and all others are optional. The null string ("") is valid for password (PW) and pack-identifier (PACK=).

If an option that requires an <attribute> is used, it must be followed by input.

Syntax:




MAXTIME
= -->
<integer>
HOSTNAME
= -->
<identifier>
*ANY
*NONE

Semantics:

The keyword options and their associated default attributes are as follows:

Option	Attribute	Default
US	Usercode	None
PW	Password	None
PACK	Pack specification	System disk
CHG	Charge number	0
PRI	Limiting user job priority	7
*PRIV	Privileged indicator	Not privileged
*NONPRIV	Nonprivileged incicator	Not privileged
PUBLIC	Security	PRIVATE
PRIVATE	Security	PRIVATE
SL	Security level	0
MAXTIME	Default maximum execution time	0 (infinite)
HOSTNAME	BNA hostname	*NONE

Examples:

```
US=NEWUS PW=NEWPW CHG=6666 PRI 4 PACK NEWPACK *PRIV
CHG=1000 PRI=7 US=NEWUS1 PW=NEWPASS1
US=NEWUS PW="" PACK=NEWPACK SL=1
US USERCODE PW PASSWORD PUBLIC
US Y     PW BCUZ *NONPRIV PRIVATE
US NEW PW LIMIT MAXTIME = 4          % this is a comment
US HN PW ANY    HOST  *ANY
```

RESTRICTIONS

The restrictions for PACK and Security below are enforced by SYSTEM/MAKEUSER since the MCP uses the "FIND FIRST" communicate.

PACK: indicates default pack. All usercodes which belong to the same family must default to the same pack, i.e., system or user pack.

SECURITY: all usercodes which belong to the same family must have the same security, i.e. PUBLIC or PRIVATE.

LINE PRINTER OUTPUT

The line printer output from the list command is formatted as follows:

"SYSTEM/MAKEUSER" RELEASE MARK X.0 (COMPILE DATE/TIME = MONDAY 17 NOV 1980/15:18)

SYSTEM USERCODE FILE AT HOST = "SLAVE3" RUN DATE = TUESDAY 02 DECEMBER 1980 11:07:49.9

INDEX	USERCODE	PASSWORD	OVERRIDE	DEFAULT PACK	CHARGE NUMBER	DEF MAX PRIORITY	SECURITY TYPE	SECURITY LEVEL	"*PRIV"	HOSTNAME		MAXTIME MINUTES
0139	(ACT)	CANDE	0	*SYS DISK*	0000000	12	PUBLIC	0	*PRIVILEGED USER*		*NONE	00000
0014	(ACTU)	CANDE	0	U	0000000	12	PUBLIC	0	*PRIVILEGED USER*		*NONE	00000
0287	(ALFORD)	B	0	SMCP	0000000	12	PUBLIC	0	*PRIVILEGED USER*		*NONE	00000
0830	(ANALYI0)	MCP	0	SMCP	0000000	12	PUBLIC	0	*PRIVILEGED USER*		*NONE	00000
0065	(ANALYI1)	MCP	0	SMCP	0000000	12	PUBLIC	0	*PRIVILEGED USER*		*NONE	00000
1023	(ANSI74)	BP	0	ANSI74	0000000	12	PUBLIC	0	*PRIVILEGED USER*		*NONE	00000
0208	(ANSI74)	COBOL	0	ANSI74	0000000	12	PUBLIC	0	*PRIVILEGED USER*		*NONE	00000
0161	(ART)	ART	0	UC	0000000	12	PUBLIC	0	*PRIVILEGED USER*		*NONE	00000
0050	(ARTHUR)	LE.GRAND	0	B	0000000	12	PUBLIC	0	*PRIVILEGED USER*		*NONE	00000
0858	(AV)	ART	0	X	0000000	12	PUBLIC	0	*PRIVILEGED USER*		*NONE	00000
0515	(B)		0	*SYS DISK*	0888888	12	PUBLIC	0	*PRIVILEGED USER*		*NONE	00000
0486	(BAMBI)	MC	0	DC	0000000	14	PUBLIC	0	*PRIVILEGED USER*		*NONE	00000
0634	(BARN)	YARD	0	BNA	0000000	12	PRIVATE	0	*PRIVILEGED USER*		*NONE	00000
0075	(BATES)	AL	0	D	0000000	15	PRIVATE	0	*PRIVILEGED USER*		*NONE	00000
0692	(BAUERLE)	R	0	*SYS DISK*	0000000	12	PUBLIC	0	*PRIVILEGED USER*		*NONE	00000
1003	(BDLC)	BDLC	0	*SYS DISK*	0000000	12	PUBLIC	0	*PRIVILEGED USER*		*NONE	00000
1022	(BDLC)	CLEM	0	*SYS DISK*	0000000	12	PUBLIC	0	*PRIVILEGED USER*		*NONE	00000
0772	(BEN)	MCP	0	SMCP	0000000	12	PUBLIC	0	*PRIVILEGED USER*		*NONE	00000
0210	(BIGELOW)	RICHARD	0	*SYS DISK*	0000000	12	PUBLIC	0	*PRIVILEGED USER*		*NONE	00000
1019	(BNA)	ARNOLD	0	BNA	0000000	12	PUBLIC	0	*PRIVILEGED USER*		*NONE	00000
1021	(BNA)	HYAMS	0	BNA	0000000	12	PUBLIC	0	*PRIVILEGED USER*		*NONE	00000
1020	(BNA)	MURPHY	0	BNA	0000000	12	PUBLIC	0	*PRIVILEGED USER*		*NONE	00000
0011	(BNA)	YARDI	0	BNA	0000000	12	PUBLIC	0	*PRIVILEGED USER*		*NONE	00000
0079	(BP)	BELINDA	0	*SYS DISK*	0000000	12	PUBLIC	0	*PRIVILEGED USER*		*NONE	00000
0022	(BRYAN)	SHELLY	0	DATACOMM	0000000	12	PUBLIC	0	*PRIVILEGED USER*		*NONE	00000
0157	(BUG)	SQUAD	0	U	0000000	12	PUBLIC	0	*PRIVILEGED USER*		*NONE	00000
0152	(BURGER)	TOM	0	X	0000000	12	PUBLIC	0	*PRIVILEGED USER*		*NONE	00000
1018	(B19DC)		0	D	0000000	12	PUBLIC	0	*PRIVILEGED USER*		*NONE	00000
101E	(B19DC)	BA	0	D	0000000	12	PUBLIC	0	*PRIVILEGED USER*		*NONE	00000
0868	(B6800)		0	*SYS DISK*	0000000	12	PUBLIC	0	*PRIVILEGED USER*		*NONE	00000
0771	(C)	S	0	*SYS DISK*	0000000	12	PUBLIC	0	*PRIVILEGED USER*		*NONE	00000
0136	(CACHEXY)	OFFLINE	0	*SYS DISK*	0000000	12	PUBLIC	0	*PRIVILEGED USER*		*NONE	00000
1015	(CANDE)	EH	0	BNA	0000000	12	PUBLIC	0	*PRIVILEGED USER*		*NONE	00000
0421	(CANDE)	KH	0	BNA	0000000	12	PUBLIC	0	*PRIVILEGED USER*		*NONE	00000
0315	(CC)	CC	0	X	0000000	12	PUBLIC	0	*PRIVILEGED USER*		*NONE	00000
0318	(CF)	CHRISTY	0	*SYS DISK*	0000000	12	PUBLIC	0	*PRIVILEGED USER*		*NONE	00000
0647	(CHOYE)	RANDY	0	RJC	0000000	12	PUBLIC	0	*PRIVILEGED USER*		*NONE	00000
0677	(CHRISTY)	POBO	0	*SYS DISK*	0000000	12	PUBLIC	0	*PRIVILEGED USER*		*NONE	00000
0331	(CL)	CL	0	X	0000000	12	PUBLIC	0	*PRIVILEGED USER*		*NONE	00000
0841	(CLD)	CYNDY	0	DATACOMM	0000000	12	PUBLIC	0	*PRIVILEGED USER*		*NONE	00000
0588	(CLH)	DMS	0	*SYS DISK*	0000000	12	PUBLIC	0	*PRIVILEGED USER*		*NONE	00000
0132	(COBIN)	DARRYL	0	*SYS DISK*	0000000	12	PUBLIC	0	*PRIVILEGED USER*		*NONE	00000
1014	(COBOL74)	PRIV	0	COBOL74	0000000	12	PUBLIC	0	*PRIVILEGED USER*		*NONE	00000
0024	(CON)	CLH	0	*SYS DISK*	0000000	12	PUBLIC	0	*PRIVILEGED USER*		*NONE	00000
0884	(CONTROL)	PATCH	0	PATCH8.0	0000000	12	PUBLIC	0	*PRIVILEGED USER*		*NONE	00000
0335	(CP)	CP	0	X	0000000	12	PUBLIC	0	*PRIVILEGED USER*		*NONE	00000
0905	(CRIN)	KLEIN	0	*SYS DISK*	0000000	12	PUBLIC	0	*PRIVILEGED USER*		*NONE	00000
0346	(CS)		0	*SYS DISK*	0000000	15	PRIVATE	0	*PRIVILEGED USER*		*NONE	00000
0509	(CURRY)	SAWYER	0	*SYS DISK*	0000000	12	PUBLIC	0	*PRIVILEGED USER*		*NONE	00000
1013	(C74OR)	PRIV	0	COBOL74	0000000	12	PUBLIC	0	*PRIVILEGED USER*		*NONE	00000
0569	(DA)	BP	0	*SYS DISK*	0000000	12	PUBLIC	0	*PRIVILEGED USER*		*NONE	00000
0503	(DAA)	DAA	0	*SYS DISK*	0000000	12	PUBLIC	0	*PRIVILEGED USER*		*NONE	00000
0826	(DAH)	DONNA	0	DATACOMM	0000000	12	PUBLIC	0	*PRIVILEGED USER*		*NONE	00000
0124	(DASDL)	DON	0	DASDL	0000000	12	PUBLIC	0	*PRIVILEGED USER*		*NONE	00000
0175	(DAVE)	SYS	0	*SYS DISK*	0000000	12	PUBLIC	0	*PRIVILEGED USER*		*NONE	00000

Notes:

OV:	reports that the pack override bit, which is automatically set when the default pack is not on-line, has been set on. This bit can be reset by the ODT message: US <us>/<pw> RV.
INDEX:	reports the actual number of the entry in the table of usercodes maintained by the program.
SYS DISK	is defined as the <pack-id> for those entries created with the blank (default) pack specifications.
PRIVILEGED USER	is output only for those entries which were created with the *PRIV option or changed to privileged with the CHANGE command.
*ANY	this usercode/password is valid from any BNA host as well as from the local host.
*NONE	this usercode/password is invalid from all BNA remote hosts. (It is still valid from the local host)

PROGRAM EXECUTION

The program can be executed from the operator display terminal (ODT) or through the card reader. The required usercode/password variables can come from cards or disk or be input individually through the ACCEPT mechanism (see CONSOLE KEYBOARD EXECUTION).

CONSOLE KEYBOARD EXECUTION

After SYSTEM/MAKEUSER is executed, the program generates an ACCEPT message to show that the program is ready to accept input commands. As commands and entries are entered the program validates them. Illegal parameters are noted through error messages that appear on the ODT, indicating that the input process should be repeated. The normal process of ODT execution would involve:

```
EX SYSTEM/MAKEUSER
SYSTEM/MAKEUSER = <job-number> ACCEPT.
<job-number> AX <command> <optional comment>
```

Comments may be added to command records; they must be preceded by a percent sign "%".

CARD READER EXECUTION

The system usercode file can be created from a card deck presented to the system in the following form:

```
?EX SYSTEM/MAKEUSER
?DATA NEW/USER.CODES
 <usercode entries>
?END;
```

The file will be automatically created, listed, and placed in the appropriate name table slot.

AUTOMATIC FEATURES

If a card file named "NEW/USER.CODES" is present at BOJ or after execution of a create command, the program will automatically create and list the usercode file. SYSTEM/MAKEUSER will then go to EOJ. No operator intervention is required under these circumstances.

If the program switches are set to "L", (EX SYSTEM/MAKEUSER SWITCH = L), the program produces a listing of the existing usercode file and then goes to EOJ. No operator intervention is required. Note that "L" is a legitimate, non-zero value for a B1800/B1700 program switch.

If the program switches are set to "P", (EX SYSTEM/MAKEUSER SWITCH = P), the program produces a card deck of the existing usercode file and then goes to EOJ. No operator intervention is required. Note that "P" is a legitimate, non-zero value for a B1800/B1700 program switch. In this way, all current ADDs, CHANGEs and DELETEs are captured.

INFORMATIONAL MESSAGES

SYSTEM/MAKEUSER displays informational messages which are self-explanatory on the host ODT when it arrives at BOJ, adds or deletes usercodes, or lists or punches the (SYSTEM)/USERCODE file, etc. The displays are for the user's information and require no direct response.

PROGRAM TERMINATION

SYSTEM/MAKEUSER may be normally terminated by an END or EOJ command. (See COMMAND section below.) The normal EOJ message then appears on the SPO.

COMMANDS

The syntax, semantics, and examples of the actual ODT input commands are contained in the following section. The minimum abbreviations for the commands are indicated by the underscored portion of each command, and the commands are presented in alpha-

betical order.

The commands may be abbreviated with a minimum of three letters. More than three letters, up to the full spelling, may also be used if the spelling is correct. For example, PUNCH may be abbreviated as PUN and as PUNC, but PUNH is a misspelling and would be rejected as a valid command even though the first three letters do supply the minimum abbreviation. Three-letter commands must be entered in full.

COMMAND RESTRICTIONS

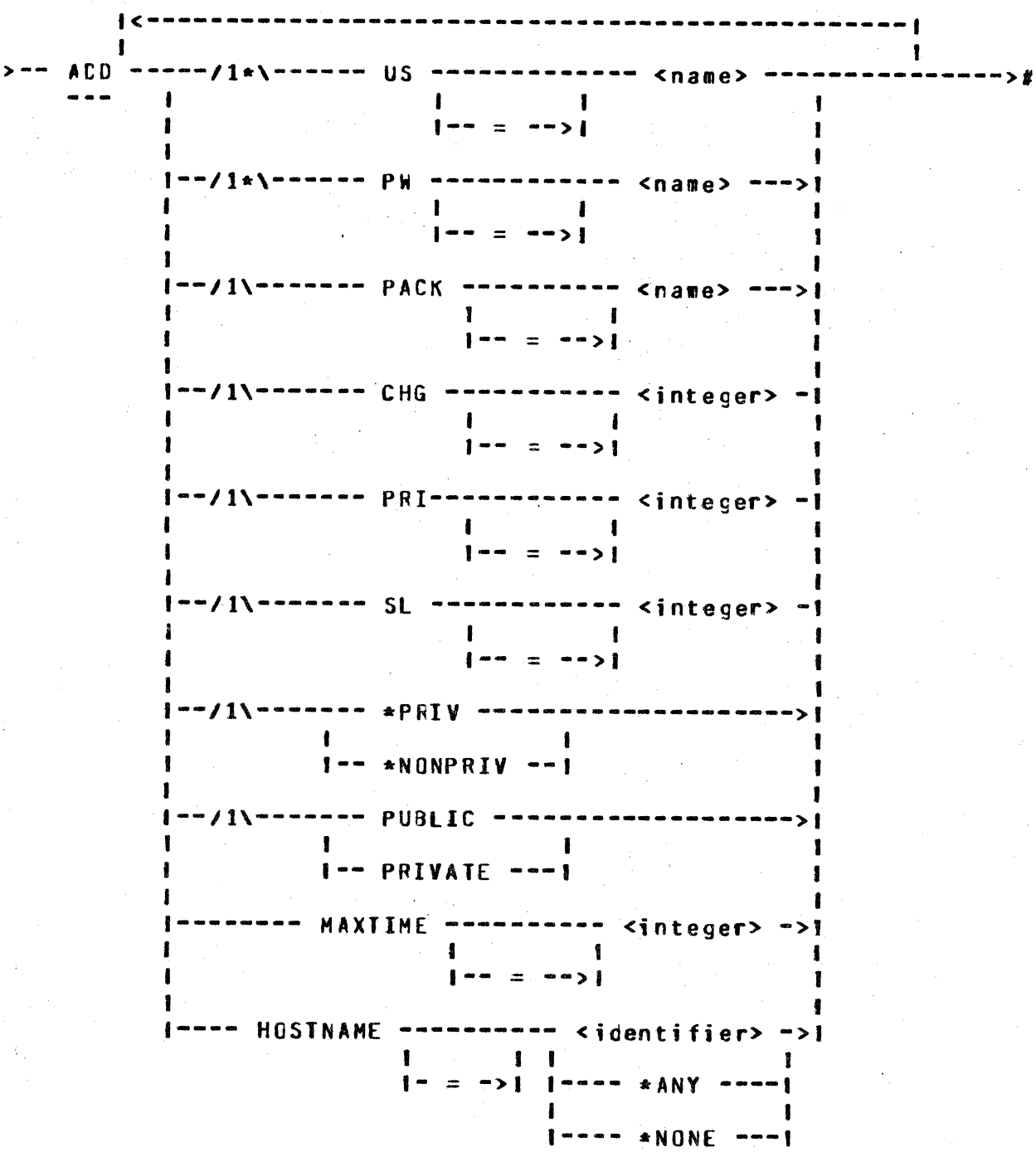
It is strongly recommended that all usercode/password changes to the (SYSTEM)/USERCODE file be made when no other jobs are running and the usercode file is definitely not in use by any program running under the file-security mechanism. Changes other than CHANGE and DELETE may safely be made to the usercode file when other jobs are in the mix. However, failure to observe this warning may result in the loss of data.

CHANGE and DELETE should not be used while other programs are running because these commands may cause a change to the index of valid usercode/password combinations that the operating system must have in order to open or to lock a disk file into the directory. For this reason CREATE is not allowed when other programs are in the mix. The operating system further needs the index to correctly point to the usercode when it checks the security of a read or a write on a file with a secure multifile id.

If a user knows for sure that the usercode file is not being accessed by the operating system (e.g., there are no programs which are running under a usercode or accessing secure files), then file maintenance can safely be performed on the system usercode file in the form of a CHANGE or DELETE. Further discussion of the method of overriding these prohibitions are contained in the separate discussions of CHANGE and DELETE.

ADD

Syntax:



Semantics:

The ADD command allows the user to add entries to the (SYSTEM)/USERCODE file. The keyword options and their associated

attributes are as follows:

Option	Attribute
US	Usercode
PW	Password
PACK	Pack specification
CHG	Charge number
PRI	Limiting user job priority
PUBLIC	Security
PRIVATE	Security
*PRIV	Privileged user
*NONPRIV	Nonprivileged user
SL	Security level
MAXTIME	Default maximum execution
HOSTNAME	BNA hostname

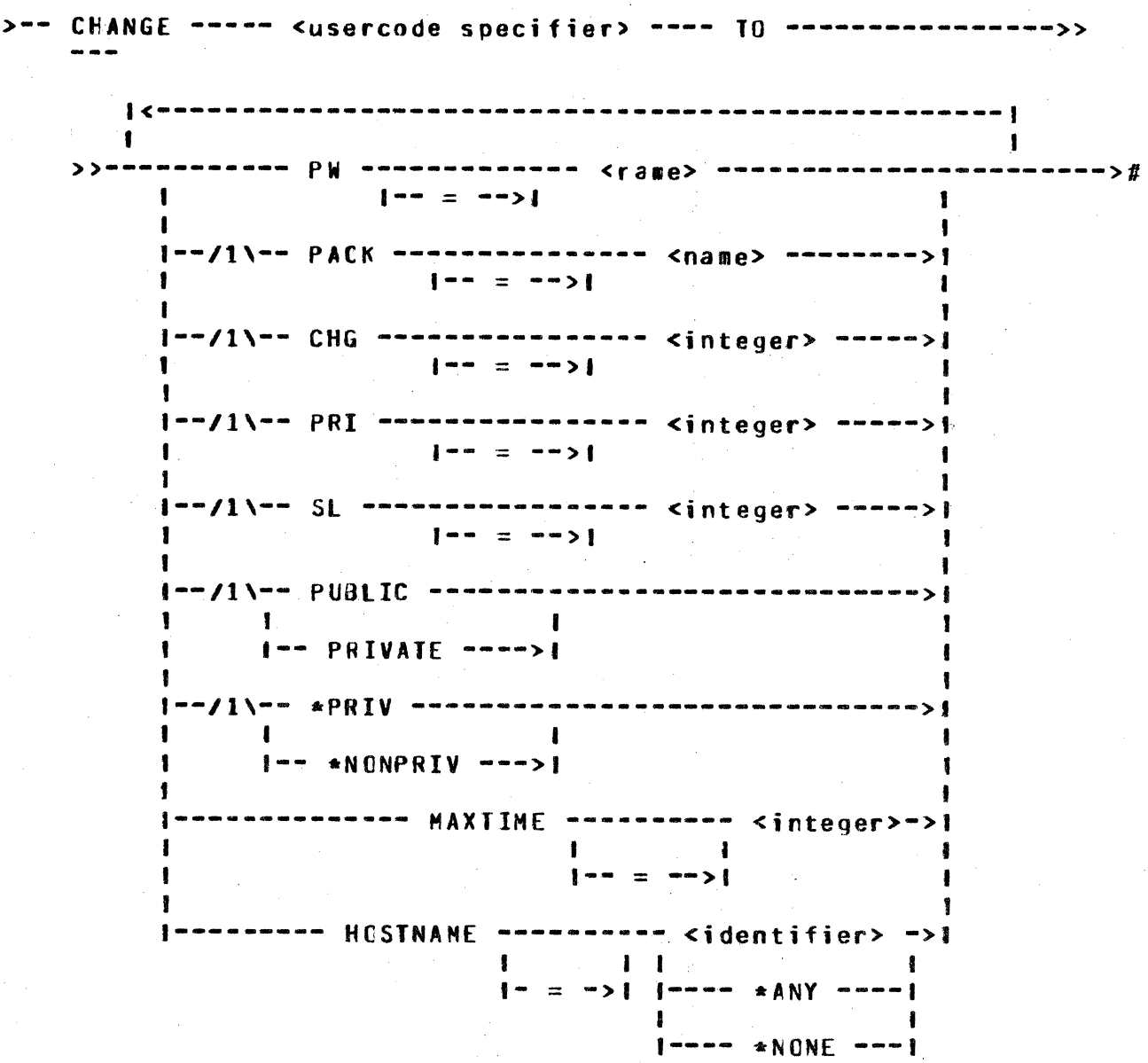
Note that the US and the PW options are required, while the rest are optional. The password name or pack specifier may be the null string which indicates a blank password or system disk.

Examples:

```
<job-number>AX ADD US=NEWUS PW NEWPW CHG 4444 PRI=5 PACK=MYPACK
<job-number>AX ADD US=NEWUS1 PW=NEWPW1 % SYSTEM DISK IS DEFAULT
<job-number>AX ADD US NEWUS2 PW="" PRI 7 PACK="" % SYSTEM DISK
<job-number>AX ADD US=USA PW PWB PUBLIC
<job-number>AX ADD US = USERCODE PW = BILL % DEFAULT IS PRIVATE
<job-number>AX ADD US=BERTHA PW=BIG *NONPRIV PRIVATE
<job-number>AX ADD US REMOTE PW BNA HOSTNAME *ANY  % "*ANY" means all
                                                     Remote BNA hosts.
<job-number>AX ADD US REMOTE PW ANY HOSTNAME ANY  % "ANY" is the actual
                                                    name of the remote
                                                    BNA host
<job-number>AX ADD US STUDENT PW 3 MAXTIME = 3  % maximum execution time
                                                  3 minutes
```

CHANGE

Syntax:



Semantics:

The CHANGE command allows the user to change the attributes of an entry or entries in the (SYSTEM)/USERCODE file. Only those attributes indicated by the options shown above can be changed. The keyword options and their associated attributes are as follows:

Option	Attribute
PW	Password
PACK	Pack specification
CHG	Charge number
PRI	Limiting user job priority
PUBLIC	File accessing rights
PRIVATE	File accessing rights
*PRIV	Privileged user
*NONPRIV	Nonprivileged user
SL	Security level
MAXTIME	Default maximum excution
HOSTNAME	BNA hostname

The CHANGE command minimum abbreviation is CHA. The usercode specifier, the literal TO, and one of the options are required.

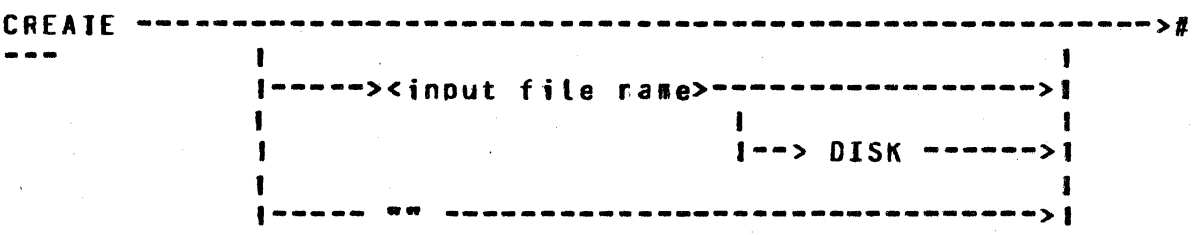
Examples:

```
<job-number>AX CHANGE JOE/PASSWORD1 TO PW=NEWPASS CHG=5555 PRI=7
<job-number>AX CHA JOE/= TO CHG=3333 PRI=5 PACK=NEWPACK
<job-number>AX CHA JOE/NEWPASS TO CHG=44444
<job-number>AX CHA JOE/"" TO PRI=7 CHG=9999
<job-number>AX CHA USERCODE/= TO PUBLIC
<job-number>AX CHA BERTHA/= TO PRIVATE  *PRIV
<job-number>AX CHANGE OLD/USER TO HOST=NEWHOST
<job-number>AX CHANGE STUDENT/1 TO MAXTIME=3 % execution time(minutes)
<job-number>AX CHANGE CLASS/= TO HOSTNAME *NONE % all usercodes in this
                                                % group are now denied
                                                % execution from all
                                                % remote BNA hosts.
```

WARNING: CHANGE should not be used while other programs are running.

CREATE

Syntax:



Semantics:

The CREATE command allows the user to create a new (SYSTEM)/USERCODE file. The user is allowed to specify the input file name, which is assumed to be a card file unless the keyword DISK is present in which case the specified disk is searched for the file. If no options are present a card file named CARD is assumed. The format of the input file records is specified in the subsection USERCODE ATTRIBUTES.

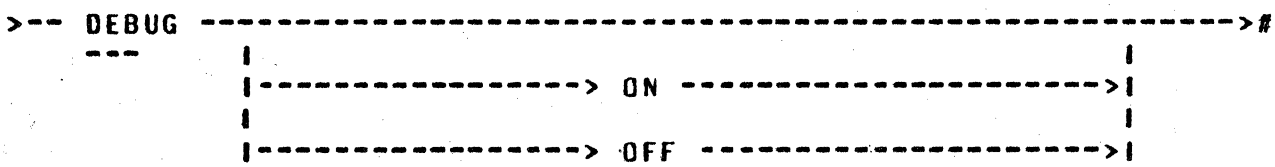
Examples:

```
<job-number>AX CRE MYCARDS
<job-number>AX CRE MYDISK/CARDFILE DISK
<job-number>AX CREATE MYPACK/MYDISK/CARDFILE DISK
<job-number>AX CREATE ""  %CREATES DEFAULT USERCODE FILE
```

If users wish to create the usercode file through entries from the CDT alone, the format CREATE "" can be used. CREATE "" produces a default usercode file that contains one entry (a privileged user). Further entries are then ADDed to the (SYSTEM)/USERCODE file, one by one.

DEBUG

Syntax:



Semantics:

ON activates printing of debug output on the printer. OFF disables the printing. The default of this command is DEBUG OFF, and a DEBUG without parameters inverts the last value.

If neither ON or OFF is specified, the value of the DEBUG attribute will be inverted (i.e., if it was OFF, it will be ON; or vice versa). Duplicate entries will reset the option to the same value (i.e., no change).

Example:

```
<job-number>AX DEBUG ON
<job-number>AX DEB
```

DELETE

Syntax:

```
>-- DELETE ----------> usercode specifier ---------------------># 
    ---
```

Semantics:

The DELETE command allows the user to delete existing entries in the (SYSTEM)/USERCODE file. The "=" option of the usercode specifier allows the deletion of a group of usercodes of the same name, and the null string indicates a password of blanks.

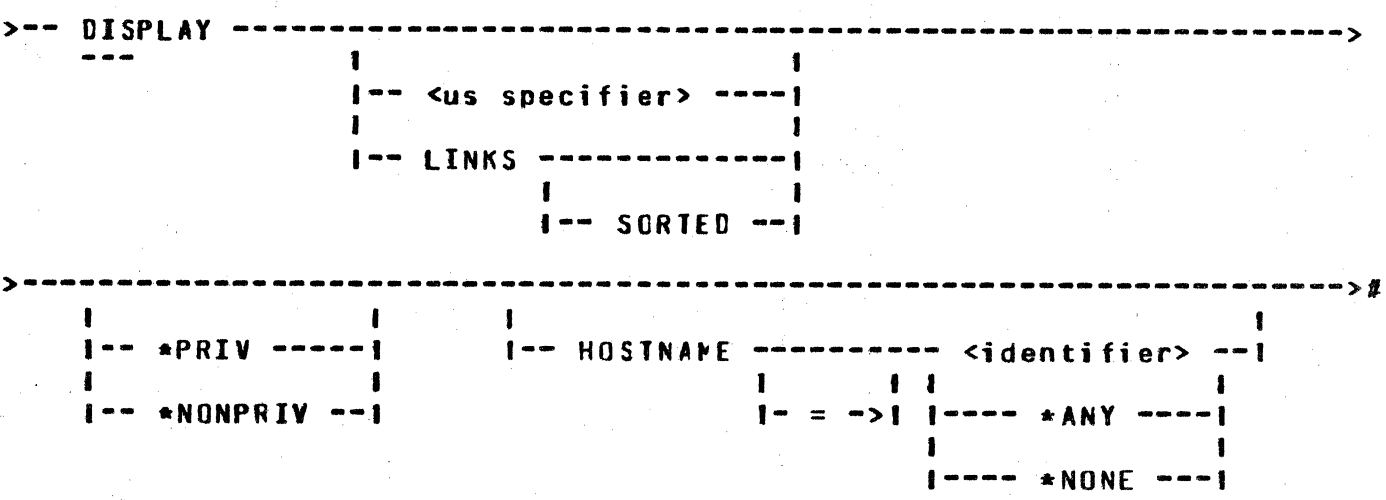
Examples:

```
<job-number>AX DELETE  USER1/PASS1
<job-number>AX DEL  USER2/=
<job-number>AX DELE  USER3/PASS3
<job-number>AX DEL USER4/""
```

WARNING: DELETE should not be used while other programs are running.

DISPLAY

Syntax:



The DISPLAY command allows the user to display the existing (SYSTEM)/USERCODE file on the ODT (or Remote ODT if program Switch 0 = 10). The default, no options set, is to display the entire file. If a usercode specifier is present only that usercode or usercodes are displayed. The *PRIV option allows the displaying of only privileged usercoces.

```
<job-number>AX DISPLAY HARRY/= *NONPRIV % Display on ODT those usercode/
                                        % password pairs of HARRY which
                                        % are nonprivileged.

<job-number>AX DISPLAY *PRIV HOST *ANY  % Display only those entries
                                        % which are privileged and
                                        % which are valid from any
                                        % remote host.

<job-number>AX DISPLAY  % This will cisplay the entire usercode file.
                        % If it is desired to interrupt this (or any
                        % display) befcre its normal completion then
                        % merely enter the next command.
```

END

Syntax:

```
>-- END ----------------------------------------------------->#
```

Semantics:

The END command allows the user to terminate the program.

Example:

```
<job-number>AX END % THIS IS THE SAME AS "EOJ"
```

EOJ

Syntax:

```
>-- EOJ ----------------------------------------------------->#
```

Semantics:

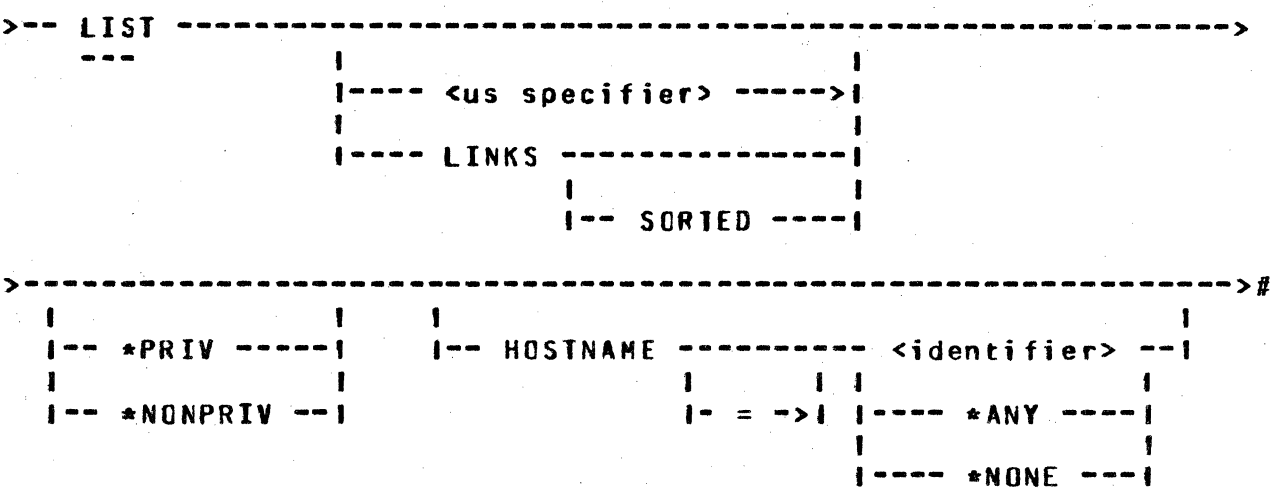
The EOJ command allows the user to terminate the program. (See also END.)

Example:

```
<job-number>AX EOJ Z ALTERNATIVE TO "END"
```

LISI

Syntax:



Semantics:

The LIST command allows the user to list the existing (SYSTEM)/USERCODE file on the line printer. The default, no options set, is to list the entire file. If a usercode specifier is present only that usercode or usercodes are listed. The *PRIV option allows the listing of only privileged usercodes.

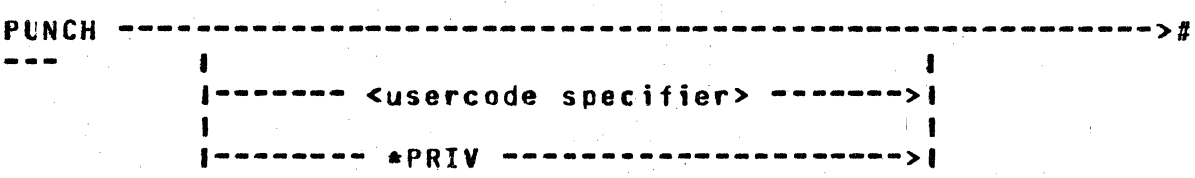
Examples:

```
<job-number>AX LIST
<job-number>AX LIST JOE/JOESPASS
<job-number>AX LIS JOE/=
<job-number>AX LIS JOE/""
<job-number>AX LIS *PRIV

<job-number>AX LIST HOSTNAME HUB % lists only entries which are
                                 % valid from the remote host
                                 % called "HUB".

<job-number>AX LIST REX/= HOST SA1 % List only those entries of REX
                                   % which are valid from the remote
                                   % host "SA1".

<job-number>AX LIST HOSTNAME *NONE % List only those entries for
                                   % which all remote access is
                                   % invalid.

<job-number>AX LIST *NONPRIV HOSTNAME USER3 % list only those entries
                                            % which are NON PRIVILEGED
```

```
% and which are valid for
% remote BNA host "USER3".
```

PUNCH

Syntax:



Semantics:

A copy of the current usercode file, including all additions, changes or deletions since the last creation, will be punched and interpreted in a format suitable for an automatic CREATE. It is labelled "NEW/USER.CODES". (See PROGRAM EXECUTION.)

If a usercode specifier is present, only that usercode or family of usercodes are punched. The *PRIV option allows the punching of only privileged usercodes.

Examples:

```
<job-number>AX PUNCH
<job-number>AX PUNC JOE/JOESPASS
<job-number>AX PUN JOE/=
<job-number>AX PUN JOE/""
<job-number>AX PUN *PRIV
```

OUTPUT ODT ERROR MESSAGES

When an error is discovered on an input record or in an ACCEPT message, the following diagnostic error messages will be displayed on the ODT:

"UNKNOWN COMMAND "<command>" , TRY ONE OF "CHANGE, ADD, DELETE, CREATE, LIST, DEBUG, PUNCH, COPY, END, OR EOJ."

"COMMANDS MUST BE FROM 3 TO 6 CHARACTERS IN LENGTH."

"UNRECOGNIZED COMMAND/KEYWORD" <input command> "OR TOO MANY PARAMETERS FOR THIS COMMAND."

"PARAMETER REQUIRED AND NOT FOUND FOLLOWING <input parameter>."

"REQUIRED PARAMETERS WERE OMITTED FOR THIS COMMAND."

"NUMBER FIELD FOR "CHARGE NUMBER" [or "PRIORITY"] TOO LARGE."

""(SYSTEM)/USERCODE" FILE NOT ON DISK, COMMAND IGNORED."

""(SYSTEM)/USERCODE" FILE LOCKED, COMMAND IGNORED."

"MAXIMUM FILE SIZE OF 1024 ENTRIES EXCEEDED, COMMAND TERMINATED."

"INVALID USERCODE "<usercode>" ENTRY DISCARDED."

"DIFFERENT PACK NAME FOR SAME USERCODE"
<usercode> "ENTRY" DISCARDED."

"FILE NAME MUST BE SPECIFIED WITH "DISK" OPTION, COMMAND IGNORED."

"PACK NAME IS INVALID FOR CARD FILES, COMMAND IGNORED."

"INPUT FILE SPECIFIED IS NOT ON DISK, COMMAND IGNORED."

"NO USERCODE FILE PRESENT, COMMAND IGNORED."

"SPECIFIED ENTRY DOES NOT EXIST, COMMAND IGNORED."

"NUMERIC FIELD CONTAINS NON-NUMERIC CHARACTERS."

"INVALID DELIMITER "<delimiter>", COMMAND IGNORED."

"CHANGE TO PACKNAME REQUIRES "<usercode>/=."

"<usercode>/<password>" ALREADY EXISTS."

"CANNOT CREATE USERCODE FILE WITH NO ENTRIES. USE CREATE "" FOR DEFAULT."

"SECURITY MISMATCH - MIXED ""PRIVATE"" AND ""PUBLIC"" NOT ALLOWED."

"CHANGE TO SECURITY REQUIRES ""<usercode>/=""."

"CANNOT CHANGE ALL PASSWORDS."

"CANNOT SPECIFY BOTH PUBLIC AND PRIVATE."

"CANNOT SPECIFY BOTH *PRIV AND *NONPRIV."

"REMOTE EXECUTION DENIED."

"ILLEGAL USERCODE."

BURROUGHS CORPORATION
COMPUTER SYSTEMS GROUP
SANTA BARBARA PLANT

CREATING SECURE FILES

BATCH MODE

Once the system's usercode file has been established, secure files can be created by programs executed under a valid usercode/password, e.g.,

```
? US PAYROLL/ACCT EX X
```

When the MCP executes program X, it associates a usercode with any files created by the program. This association is called job spawning. Control commands that are zipped by programs or submitted through the card reader must also be prefixed by a usercode/password pair if they access secure files.

If program X creates a new file labeled CHECKS, the MCP will lock into the disk directory a file labeled (PAYROLL)/CHECKS. This file is a secure file and can only be accessed by programs run under the usercode PAYROLL or a privileged usercode. To do library maintenance on this file, one has to precede the ODT commands with the usercode and password. Thus, the following messages are valid:

```
USER PAYROLL/ACCT RE CHECKS
USER PAYROLL/ACCT CH CHECKS TO PC
USER PAYROLL/ACCT COPY =/= TO PAYROLL
```

The following ODT commands are not valid:

```
RE CHECKS              %There will be no such file.

RE (PAYROLL)/CHECKS    %The MCP will not allow this command
                       %since a person is attempting to remove
                       %a secure file.

PD CHECKS              %The MCP will say: NO FILE CHECKS.
```

If program Y, executed under a different usercode or no usercode attempts to access the file (PAYROLL)/CHECKS, the MCP will disallow it.

In some instances it may be desirable to create secure files that can be accessed by all usercodes (privileged and non-privileged). This can be done by designating those files to be PUBLIC. In the example shown above, by default, the file (PAYROLL)/CHECKS was made PRIVATE and consequently no other non-privileged user could access it. However, if (PAYROLL)/CHECKS were a PUBLIC file then program Y (executed with a different usercode - say FINANCE/VP) could access this file by stating that the label of the file is "(PAYROLL)"/"CHECKS". If Y is a COBOL program, then it does this in the FD section by stating:

VA OF ID IS "(PAYROLL)"/"CHECKS"

When Y attempts to open this file as input or input/output (i.e., existence of this file is assumed), the MCP does a search for file "(PAYROLL)"/"CHECKS" and checks to see if the file is PUBLIC. If it is, then the MCP allows access. The program can read this file; it can write into it (if opened input/output) and then close it. As a "public" file, (PAYROLL)/CHECKS could contain updates made by program Y.

PUBLIC FILES

There are three ways of designating a file to be a public file. They are:

1. By doing a file equate, e.g.,

   US PAYROLL/ACCT EX X FI CHECKS SECURITYTYPE PUBLIC

   The above example assumes that the internal name of the file is CHECKS. The key word SECURITYTYPE and PUBLIC indicate to the MCP that the file is being made PUBLIC.

   Public files can be made private by the same process if one replaces PUBLIC by PRIVATE. This, however, is usually unnecessary since the default is PRIVATE when a program is running under a usercode.

2. After a file has been created and locked into the disk directory, the file may be made PUBLIC by modifying the header, e.g.,

   US PAYROLL/ACCT MH CHECKS SEC PUBLIC

3. SYSTEM/MAKEUSER has an option whereby all files created by a specific usercode can be made PUBLIC. When creating the (SYSTEM)/USERCODE file (i.e., the file that contains the usercode/password pairs), the keyword PUBLIC can be associated with any usercode/password pair. This tells the MCP that every new file created with this usercode/password will be made PUBLIC.

Currently, there are no constructs in any programming language to make files PUBLIC or PRIVATE.

CONTROL OF I/O

If a file has been designated to be PUBLIC then the creator of the file has the option of controlling the type of I/O that another user can perform, i.e., input, output, I/O. Thus, if (PAYROLL)/CHECKS is a PUBLIC read-only file, then the program Y running under the usercode/password pair FINANCE/VP can read this file but cannot write into it.

READ-ONLY FILES

There are two ways of creating read-only files. They are:

1. By file equation:

```
US PAYROLL/ACCT EX X FI CHECKS SECURITYTYPE PUBLIC

                              INPUT
                SECURITYUSE   OUTPUT
                              I.O
```

The keywords SEC and SUS can be substituted for SECURITYTYPE and SECURITYUSE, respectively. The options INPUT, OUTPUT, and I.O indicate whether the file is read only, write only, or for read/write.

2. By modification of the file header:

```
US PAYROLL/ACCT MH CHECKS SEC PUBLIC SUS   INPUT
                                           OUTPUT
                                           I.O
```

CONVERSION TO SECURE FILES

In converting non-secure files to secure files, the most direct method is to use a system utility program to copy input files to the proper pack under the secure multifile-id. If users wish to make the conversion programmatically, they must take the following points into account:

a. Security designation

b. Location of the input file

c. Location of the output file

d. Filename

The first consideration is that of the security designation given the usercode/password pair under which the program is run. If the pair is privileged, it can read and write files with any valid multifile-ids, secure or non-secure. If, for example, PROGRAM/X is executed under the privileged usercode/password of PAYROLL/ACCTS, it may access a file called OLD/INFO and make a new output disk file called (NEW)/INFO (if a usercode/password combination for (NEW)/ANYNAME has been declared), produce a new output file called (PAYROLL)/INFO that is located on the disk pack that is specified in the usercode file, or create a new file called NEW/INFO. Privileged usercode/passwords have those options open to them.

The location of the input file, which is non-secure, is determined by the file identifier, whatever it happens to be. The

location of the output file is determined by the usercode if it is a secure file; by the full file identifier if it is a non-secure file. A secure file may be created or system disk either by using a usercode/password with a no default pack-id or by telling the MCP not to change the file name with an asterisk (*) as the first character of the multifile-id. This convention is explained more fully in DEFAULT IDENTIFIERS.

The filename is restricted only if a secure file is being created. Since the multifile-id is being supplied by the operating system, a new secure file cannot have a declared name with both a multifile-id and a filename. Furthermore, no programs running under a usercode may create a new system file, i.e., a file with a single filename located on system disk.

When the usercode is non-privileged, the following conditions would be in effect, where the same four points are concerned:

The non-privileged user may access a non-secure file with a multifile-id which is not its own but cannot create a file with any other mulfifile-id than its own. Thus, PROGRAM/X may read OLD/INFO but cannot create (NEW)/INFO or NEW/INFO.

The location of the input file is the same as specified above for non-secure files. The output file, is located in only one of three places: on the system disk, on a specified pack, or on the usercode's default pack. If the file naming convention is over-riden by the asterisk convention, the file will be located on system disk, otherwise it will be created on the user's pack.

Non-privileged users are resticted to creating output files with a multifile-id that is their usercode and a filename that is assigned by them. Any attempt to circumvent this restiction is prohibited by the operating system. Furthermore, if a user program running under a non-privileged usercode/password combination declares a file with a multifile-id and a file-id, the file is not created. The only control exercised over file identifiers is in the file-name. The operating system supplies the pack-id and the multifile-id; consequently, non-privileged users must not attempt to write and close files with file identifiers other than that of their default pack, their own multifile-ids, and a file-id. The pack-id and the multifile-id would automatically be supplied by information from the system usercode file, but the duplication of effort, then, would be allowed for program documentation.

DEFAULT IDENTIFIERS

When a file is being closed with lock, the operating system automatically associates the usercode of any usercode/password pair with any new file-name and locks that file on the pack specified as the default pack for that usercode/password pair, if no instructions are presented which override the convention.

Both non-privileged and privileged users are allowed to override the default naming convention through the asterisk-convention (*). An asterisk that precedes a multifile-id instructs the operating system not to change the file-name as it appears. For non-privileged users (who cannot lock a new file without their own usercode as the multifile-id), this means that the file is saved on system disk or a specified user pack. For privileged users (who can lock a new file with any name that does not violate security naming conventions), this means that the file can be saved on system disk, a specified user pack, and/or with a multifile-id of their choice. The asterisk, then, is used to override default pack names and multifile-ids, within the restrictions allowed for privileged and non-privileged users.

To override the default pack named in the usercode entry, users must specify a pack name, as in the following example:

```
I-O-CONTROL.
    MULTIPLE FILE DISKPACK "P" CONTAINS CHECKS
    .
    .
    .
FILE SECTION
    FD CHECKS
      VA OF ID IS "CHECKS"    2This is equivalent to
                              2 VA of ID is "P"/"CHECKS"/
```

The COBOL statement above will cause the MCP to create a file named P/(PAYROLL)/CHECKS, irrespective of the default pack id.

If in the above example there was a default pack "DP" associated with the usercode in (SYSTEM)/USERCODE and the COBOL program did not have a pack defined (i.e., no MULTIPLE FILE statement) then the file would have gone to the pack DP and its name would be DP/(PAYROLL)/CHECKS. If a default pack is defined and if the user wants to look for or create a file on system disk then the asterisk convention is required. Thus, the following statement:

```
VA OF ID IS "*(PAYROLL)"/"CHECKS"
```

will cause the MCP to look for a file on system disk with name (PAYROLL)/CHECKS. The "*" is therefore a way of overriding the default pack designation and/or default multifile-id designation.

SECURITY LEVELS

The Security Level usercode attribute defines the multi-file-id's that the usercode may access. The valid values are 0, 1, and 2. A value of 0 allows any value for the multi-file-id. A value of 1 allows the multi-file-id to be set to any usercode (for example, "(PAYROLL)"). A value of 2 allows the multi-file-id of a file being accesssed only to be the same as the usercode supplied with the input command or the same that the job is running under.

These rules are relaxed slightly if the command entered is one that executes or compiles a program. A usercode with a non-zero security level can "EX CMPALL" or "COMPILE PROG WITH COBOL TO LI". However, a usercode with a security level of 2 cannot "EX (USERB)/PROG1" unless the usercode incentifier in the US command is USERB.

All of the security checking and enforcement that is based on the security level attribute is in accition to other security checking.

ACCESS: PRIV VS. NON-PRIV

Usercodes which are designated as privileged are allowed to access or create secure files with multifile-ids other than their own and this constitutes the major difference between the these two types of usercodes. Tables 3.1 and 3.2 show how the privilege option affects four different files involving the two types of usercodes.

	Usercode	PRIV	Filename Accessed	Access
1.	(PAYROLL)	YES	<dp>/(PAYROLL)/A	Allowed
2.	(PAYROLL)	YES	<dp>/(USERA)/A	Allowed
3.	(PAYROLL)	YES	*(A)/B	Allowed
4.	(PAYROLL)	YES	<pack-id>/A/B	Allowed
1.	(USERA)	NO	<dp>/(USERA)/A	Allowed
2.	(USERA)	NO	<dp)/(PAYROLL)/A	Denied
3.	(USERA)	NO	*(A)/B	Denied
4.	(USERA)	NO	<pack-id>/A/B	Allowed

Table 3.1 Comparative Access Privileges

Table 3.1 presumes the following conventions:

<dp> names the default pack asscciated with the usercode in the system usercode file. To override this convention, the user would have to precede the filename with an asterisk and specify a pack name, if the file did not reside on

system disk. If the asterisk is specified, the MCP looks for the file, by default, on the system disk.

* used to override the default pack-id and/or multifile-id designation. If the file is not a secure file, as in the last instance for both usercodes, the pack name must be specified when accessing a file that exists on a user pack.

In the first instance, both usercodes are allowed to access files under their own multifile-ids. Where the privileged user is allowed to access files under another's multifile-id (2), the non-privileged user is not. The non-privileged user is also denied access to secure files on system disk, as indicated by the *<multifile-id>/<file-id> in case three. The last instance shows that both the privileged and non-privileged user can get any non-secure file. Note that the pack identification must be specified in this instance because there is no default pack designation for files that do not have a usercode. Privileged usercodes also have the option of creating new output files with pack-ids and multifile-ids which are not their own, as shown in Table 3.2.

LOCK: PRIV VS. NON-PRIV

	Usercode	PRIV	Filename Created	Approval
1.	(PAYROLL)	YES	<dp>/(PAYROLL)/A	Allowed
2.	(PAYROLL)	YES	<dp>/(USERA)/A	Allowed
3.	(PAYROLL)	YES	*(A)/B	Allowed
4.	(PAYROLL)	YES	<pack-id>//A/B	Allowed
1.	(USERA)	NO	<dp>/(USERA)/A	Allowed
2.	(USERA)	NO	<dp)/(PAYROLL)/A	Denied
3.	(USERA)	NO	*(A)/B	Denied
4.	(USERA)	NO	<pack-id>//A/B	Denied

Table 3.2 Comparative File Creation

The conventions that existed for Table 3.1 also exist for this table. Notice that the non-privileged user is not allowed to lock a non-secure file into the disk directory.

APPENDED USERCODES

If a program running under a usercode ZIPs a control statement, the usercode of the zipping program is automatically appended to the control string. Thus, ZIP "RE (INVEN)/A" will be interpreted as USER PAYROLL/ACCT RE (INVEN)/A and will be disallowed unless PAYROLL is privileged. If the zipping program inserts a USER string in the zipped command then this usercode becomes effective and not the usercode of the zipping program. Thus, ZIP USER INVEN/TORY RE (INVEN)/A will remove the file. This may lead one to conclude that one user program can remove the files of

another, but this is possible only if the password of the other user is known by the first.

PREFIXED ODT COMMANDS

Usercode/password must be prefixed to a ODT control command if the command results in modification or removal of a secure file. The following ODT commands are affected by this rule:

CH, CO, EX, MH, MO, OF, RB, RE, RF

Examples:

```
  EX   (INVEN)/A                          % Invalid command
  CH   (INVEN)/A      TO  X               % Invalid command
USER    INVEN/TORY    CH  A TO *X         % Invalid command

USER    INVEN/TORY    EX (INVEN)/#        % Valid command
USER    INVEN/TORY    EX          #       % Valid command
USER    INVEN/TORY    CH  A TO  X         % Valid command
USER    EL/ZAPPO      CH (INVEN)/# to *X  % Valid command if
                                          %    EL/ZAPPO is a
                                          %    privileged user.
```

The commands KA and KP can be applied to any file, e.g.,

```
KA (INVEN)/A              % is OK
KP (INVEN)/A              % is OK
KA (INVEN)/=              % is OK
```

It is not necessary for a PD to be preceded by a usercode so:

```
                              / USER INVEN/TORY PD A
                             /
PD (INVEN)/A  is the same as <          or
                             \
                              \ US INVEN PD A
```

USERCODE BACKUP FILES

Backup files created by programs run under a usercode have a naming convention that is different from the current naming convention. Backup files created under usercode PAYROLL have the following names:

```
<default pack for PAYROLL>/(PAYROLL)/#<integer>% printer
                        or
<default pack for PAYROLL>/(PAYROLL)/%<integer>% punch
```

To print, remove, display secure backup files, the PB, RB, and BF commands must be preceded by the appropriate usercode and password, e.g.,

```
USER PAYROLL/ACCT PB  3   % will print <def pack>/(PAYROLL)/#3
USER PAYROLL/ACCT RB =/=  % will remove all backup files for
                          % this usercode
```

REMOTE MODE

Prior to the VI.1 release of the MCP and SYSTEM/MAKEUSER, remote applications programs ordinarily required remote users to identify themselves through a usercode and password before they were allowed access to the system. This was true for MCS-type programs such as CANDE which handled individual remote stations as well as for RJE/CONTROLLER which allowed a remote computer to function as a remote terminal in the HOST/RJE system. Furthermore, under that system, jobs in those configurations were controlled through a job-spawning process that attached a usercode and unique session number to the batch jobs executed and compiled (i.e., spawned) from the remote terminal.

The present security system is an extension of that design. When a remote-applications program is running under a secure usercode, users must sign on, as before, through usercodes and passwords. The new security system, however, allows only those usercodes and passwords that are currently contained in the (SYSTEM)/USERCODE file to have access to the system through a remote program. This means that unless remote users have been authorized entry to the system through previously validated usercodes and passwords, they cannot sign on or log on.

Furthermore, any jobs spawned from a remote terminal or computer will be checked for security violations according to the same standards that have been discussed previously in the BATCH MODE subsection of this document. For example, a remote user who attempts to access the secure file of another user and is not privileged to do so will be denied access to that file. The job is either not scheduled or DS-ed, depending upon the state at which the security violation occurs. The security designations for any file which an individual user creates will be determined by the security designation given in the usercode/password entry in the (SYSTEM)/USERCODE file, unless specifically overridden.

It should be stressed at this point that both secure and non-secure operations can occur on the same system at the same time. This means that a secure remote-applications operation can be run in the same mix of jobs that allows non-secure batch processing to take place. However, the same remote-applications job cannot allow both secure and non-secure activities to take place during a single session. A mixture of secure and non-secure jobs are allowed on the same system because the security system is independent of the datacomm operations. It is maintained by the operating system through the (SYSTEM)/USERCODE file.

LOG-ON/SIGN-ON

Log-on and sign-on procedures involve the same processes that have been established in recent releases, i.e., through a usercode and a password. Under file security, however, users who have not established valid usercodes in the (SYSTEM)/USERCODE

file are denied access to the system. This procedure is true for CANDE and HOST/RJE as well as any MCS-type program running under a secure usercode. The Supervisory Message Control System (SMCS) is a special case, since it ordinarily does not run under a secure usercode yet supports security checking for those programs which require it to do so.

JOB SPAWNING

Spawned jobs are handled in the same way that batch jobs involving secure files are treated; i.e., access to secure files and closing a disk file with lock are checked for security violations. If a violation is found, the job is either DS-ed or not scheduled. Non-privileged CANDE users, for example, cannot GET (access) a private file under another secure usercode. If they attempt to execute or compile a program with the private file that belongs to another user, the execution or compilation is not scheduled.

FILE HANDLING

All files are saved, by default, as private or public files, according to the user's default protection as specified in the (SYSTEM)/USERCODE file. Usercode/password combinations may have a default pack associated with them. If a pack has been defined for a particular usercode, all files are read from or written on the specified pack unless the default is overridden through the asterisk-convention, or explicitly through a pack name.

SYSTEM DISPLAYS

Job security inhibits certain MCP displays so that the response is given only for an individual's session. For example,

?WY -- gives the status of that user's job(s) only.

?MX -- reports on active jobs for that user only.

?RE -- removes only the files of the particular, active user.

?MO -- modifies only the files of the particular, active user.

BACKUP FILES

Backup files created by programs running under secure usercodes, both batch and remote, are controlled by the default designations of the usercode under which the job is being run. Consequently, the file is locked into the disk directory of the default pack, assigned the multifile-id of the usercode under which the job was executed or compiled, and given a number by the MCP, unless the default is overridden. Printer backup files which have been created by jobs running under a usercode are locked in the disk directory as <default pack>/(usercode)/#<number>.

DISK PACK DEFAULTS

Since the MCP will force files to a default pack associated with the usercode/password, syntax has been implemented to allow remote users to access or save files on a disk pack other than that defined in the (SYSTEM)/ USERCODE file. A remote applications program, running under a privileged usercode, allows users to access files according to the following table:

ENTER	PACK.ID	FAMILY.ID	FILE.ID
A	<default pack>	(UC)	A
A/B	<default pack>	A	B
A/B ON C	C	A	B
(UC)/A	<default pack>	(UC)	A
(UC)/A ON C	C	(UC)	A
*(UC)/A	**SYSTEM DISK**	(UC)	A
*A	**SYSTEM DISK**	A	
*A ON C	C	A	

The number of characters in a multifile-id, including the asterisk and the parentheses, may not exceed 10 characters. The identifiers *(ABCDEFG) and ABCDEFGHIJ are legal, while *(ABCDEFGH), for example, is not.

Since remote users are usually required to sign on to applications programs through usercode/password combinations, all files saved (locked or disk) contain their usercode as the multifile-id. To access another user's file, that file must be changed from private to public by the owner or be accessed by a privileged usercode. When saving a file, it cannot be saved under someone else's usercode. Thus, a user signed on as UC/PW cannot save a file with the command SAVE AS *(ANOTHER)/A; the command SAVE AS *A saves a file as (UC)/A on system disk. A command such as SAVE AS A will put the file on disk as <default pack>/(UC)/A.

DEFINITIONS AND TABLES

FILE SECURITY IMPLEMENTATION

Two fields were added to the disk file header to support file security.

Upon locking a new disk file into the directory the MCP will set DFH.PROTECTION.IO to FPB.PROTECTION.IO then look at FPB.PROTECTION. If it is zero (default), then DFH.PROTECTION is set to PUBLIC if the MULTI.FILE.ID does not contain a USERCODE. However, if the MULTI.FILE.ID does contain a USERCODE, FPB.PROTECTION will be set to the security attribute of the usercode, i.e., PUBLIC or PRIVATE. If FPB.PROTECTION is not equal to zero, DFH.PROTECTION is set to FPB.PROTECTION less one.

```
DFH.PROTECTION                          BIT (2)

0 - PUBLIC
1 - PRIVATE
2 - GUARD (not implemented)

DFH.PROTECTION.IO                       BIT (2)

 0 - INPUT OUTPUT
 1 - INPUT ONLY
 2 - OUTPUT ONLY
```

One ODT command was implemented to change these fields.

```
MH <file-identifier> SEC PUBLIC
                         PRIVATE

                         INPUT
                     SUS OUTPUT
                         I.O
```

Two fields were added to the FPB. These are used to set the fields in the disk file header.

FPE.PROTECTION BIT (2)

0 - DEFAULT
1 - PUBLIC
2 - PRIVATE
3 - GUARD (not implemented)

FPE.PROTECTION.IO BIT (2)

0 - INPUT OUTPUT
1 - INPUT ONLY
2- OUTPUT ONLY

Two file attributes can set these FPE fields.

SEC or SECURITYTYPE	DEFAULT PUBLIC PRIVATE GUARD	SUS or SECURITYUSE	I.O INPUT OUTPUT

ACCESS/OPEN TABLE

Table 4.1, Security Truth Table, outlines the steps taken by the MCP in determining whether programs running with a non-privileged usercode may or may not access or create a disk file.

MULTI.FILE.ID	PACK.ID	JOB RUNNING WITH A USERCODE: NEW FILE	JOB RUNNING WITH A USERCODE: OLD FILE	JOB RUNNING WITHOUT A USERCODE: NEW FILE	JOB RUNNING WITHOUT A USERCODE: OLD FILE
BLANK	BLANK	A	B	OPEN	C
	PRESENT	G	K	OPEN	C
USERCODE	BLANK	D	I	O	E
	PRESENT	F	H	W	C
ASTERISK IN FIRST POSITION	BLANK	L	M	J	N
	PRESENT	L	M	J	N
PRESENT	BLANK	P	C	OPEN	C
	PRESENT	P	C	OPEN	C

4.1. Security Truth Table (Non-privileged users)

Where:

A. 1. Set PACK.ID from the USERCODE table using the USERCODE under which the program is running.
   2. Set the MULTI.FILE.ID with the USERCODE under which the program is running.
   3. Allow OPEN to proceed.

B. 1. Set the PACK.ID from the USERCODE table using the USERCODE under which the program is running.
   2. Set the MULTI.FILE.ID with the USERCODE under which the program is running.
   3. Search the directory.
   4. If the file is present allow the OPEN to proceed.
   5. Clear the PACK.ID and the MULTI.FILE.ID.
   6. Proceed to Step C.

C. 1. Search the directory.
2. If the file is not present hang the program NO FILE.
3. Proceed to Step R.

D. 1. If the USERCODE in the MULTI.FILE.ID is not the same as the USERCODE under which the program is running then the job is DS-ed.
2. Set the PACK.ID from the USERCODE table using the USERCODE in the MULTI.FILE.ID.
3. Allow the OPEN to proceed.

E. 1. Set the PACK.ID from the USERCODE table using the USERCODE in the MULTI.FILE.ID.
2. Search the directory.
3. If the file is present then proceed to Step R.
4. Clear the PACK.ID.
5. Proceed to Step C.

F. 1. If the USERCODE in the MULTI.FILE.ID is not the same as the USERCODE under which the program is running then the job is DS-ed.
2. Allow the OPEN to proceed.

G. 1. Set the MULTI.FILE.ID with the USERCODE under which the program is running.
2. Allow the OPEN to proceed.

H. 1. If the USERCODE in the MULTI.FILE.ID is not the same as the USERCODE under which the program is running proceed to Step C.
2. Search the directory.
3. If the file is not present hang the program NO FILE.
4. Allow the OPEN to proceed.

I. 1. Set the PACK.ID from the USERCODE table using the USERCODE in the MULTI.PACK.ID.
2. Search the directory.
3. If the file is present proceed to Step S.
4. Clear the PACK.ID.
5. Proceed to Step H.

J. 1. Remove the asterisk and shift the name left one position
2. Allow the OPEN to proceed.
3. At CLOSE time proceed to Step T.

K. 1. Set the MULTI.FILE.ID with the usercode under which the program is running.
2. Search the directory.
3. If the file is present allow the OPEN to proceed.
4. Clear the MULTI.FILE.ID.
5. Proceed to Step C.

L. 1. Remove the asterisk and shift the name left one position.
2. If the resultant name is a USERCODE proceed to Step F.
3. Allow the OPEN to proceed.
4. At CLOSE time proceed to Step U.

M. 1. Remove the asterisk and shift the name left one position.
2. If the resultant name is a USERCODE proceed to Step H.
3. Proceed to Step C.

N. 1. Remove the asterisk and shift the name left one position.
2. Proceed to Step C.

O. 1. Set the PACK.ID from the USERCODE table using the USERCODE in the MULTI.FILE.ID.
2. Proceed to Step W.

P. 1. Allow the OPEN to proceed.
2. At CLOSE time proceed to Step U.

Q. 1. Display security error message.
2. Hang program NO FILE.

R. 1. If the OPEN violates file security proceed to Step Q.
2. Allow OPEN to proceed.

S. 1. If the USERCODE in the MULTI.FILE.ID is the same as the USERCODE under which the program is running then allow the OPEN to proceed.
2. Proceed to Step R.

T. 1. If the program is attempting to lock the file into the directory and the MULTI.FILE.ID contains a USERCODE then proceed to Step V.
2. Allow the CLOSE to proceed.

U. 1. If the MULTI.FILE.ID does not contain the USERCODE under which this program is runnirg and the program is attempting to lock this file into the cirectory proceed to Step V.
2. Allow the CLOSE to proceed.

V. 1. Display an error message.
2. Discard the file.

W. 1. Allow the OPEN to proceed.
2. Proceed to Step T.

BURROUGHS CORPORATION
COMPUTER SYSTEMS GROUP
SANTA BARBARA PLANT

INDEX

DISTRIBUTION LIST

B1800/B1700 SOFTWARE PRODUCT SPECIFICATIONS

DETROIT

S. M. Roberson - Prod. Mgmt.
P. Gonzales - Prod. Mgmt.
J. M. Ross - Int'l Group P
C. Kunkelmann - BMG
B. Dent - CSG
D. Dahm - Corp. Eng.
Dir., Pgmg. - SSG
M. Dowers - Int'l FE
D. Hill - TC, BM, & SS

U.S. AND EUROPE

D. Cikoski - (Plymouth)
J. H. Pedersen (Plymouth)
W. E. Feeser (Austin)
J. Berta (Downingtown)
W. Minarcik (Paoli)
G. Smolnik (Paoli)
T. Yama - F&SSG (Paoli)
M. E. Ryan (Tredyffrin)
J. Firth (McLean)
A. Kosla (McLean)
A. LaCivita - F&SSG (McLean)
L. Guell - F&SSG (McLean)
R. Sutton - F&SSG (McLean)
L. DeBartelo - WADC (Irvine)
R. Cole (Pasadena)
H. M. Townsend (Pasadena)
N. Cass - Pat. Atty. (Pasadena)
D. C. Swanson (Mission Viejo)
J. Lowe (Mission Viejo)
H. N. Riley (El Monte)
J. C. Allan (Glenrothes)
W. McKee (Cumbernauld)
B. Higgins (Livingston)
Mgr, NPSGrp (Ruislip)
E. Norton (Middlesex)
B. Hammersley (Croydon)
J. Gerain (Pantin)
J. Cazanove (Villers)
J. C. Wery (Liege)
R. Bouvier (Liege)
G. LeBlanc (Liege)
C. J. Tooth - SSG (London)
J. Dreystadt (Wayne)

SANTA BARBARA PLANT

S. C. Schmidt
J. Hale
R. Shobe
K. Meyers
A. van der Linden
T. Cardona
R. Bauerle
J. Henige
E. Yardi
D. Stover
L. Sweeney - 2
G. Hammond - 3
J. Morrison - 6

Distribution list current as of 01/21/81