PLAN	ARBARA PLANT		DOCUMENT TRA	NSMITT	AL .			nore
VSTEM/		B180	0/81700	-				
				PE				
OORD.	1E		снкк. На	proj. No				
DOC PFX OR DWG SIZE	DOCUMENT	REV OR ISSUE	DOCUMENT DESCRIPTION	ENG. QTY REV PAGE	RECORD COPIES EACH PAGE	OND CINOE	/ELLUM 4	REMARKS
P.S.	2219 0102	G	FILE SECURITY	54	63			
	· · · · · · · · · · · · · · · · · · ·				 			
				· · ·				
			·					
					<u>}</u>			
	n yn de man yn yn yw yn arllen a fefnin yn a fefnin a fefnin a fernan a fernan fernan er fan ar er yn yn a							
			· · · ·					

Burroughs Corporation

COMPUTER SYSTEMS GROUP SANTA BARBARA PLANT

B1800/B1700 FILE SECURITY

P.S. 2219 0102

PRODUCT SPECIFICATION REV REVISION APPROVED BY REVISIONS ISSUE DATE LTR 7/31/80 F 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". Deleted "PTN" and "PIO" from ODT command. 4-1 4-2 Deleted "PIN or PROTECTION" and "PIO OR PROTECT.ID" from file attributes. 1/14/20 X Xa 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 - 4Updated "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. Added "DISPLAY" syntax and semantics. 2 - 192-22 Updated "LIST" syntax and examples.

"THE INFORMATION CONTAINED IN THIS DOCUMENT IS CONFIDENTIAL AND PROPRIETARY TO BURROUGHS CORPORATION AND IS NOT TO BE DISCLOSED TO ANYONE OUTSIDE OF BURROUGHS CORPORATION WITHOUT OF THE PRIOR WRITTEN RELEASE FROM THE PATENT DIVISION OF BURROUGHS CORPORATION"

Burroughs Corporation

COMPUTER SYSTEMS GROUP SANTA BARBARA PLANT

÷ ŝy

B1800/B1700 FILE SECURITY

PRODUCT SPECIFICATION

REVISIO	TE APPROVED BY	REVISIONS
		Changes for MARK 10.0 Release cont.
		2-25 Updated "ODT MESSATES" by deleting number 21 and removing all the numbers before the statements.
ан 1		
7 7 8		
- N.		

2219 0102

Burroughs Corporation

COMPUTER SYSTEMS GROUP SANTA BARBARA PLANT

Υċ.

B1800/B1700 FILE SECURITY P.S. 2219 0102

27 KAP

PRODUCT SPECIFICATION

	EV TR	REVISION	APPROVED BY		REVISIONS
F	D	7/17/78		1-2	Undated private access rights sentence
I.		.)	Nace	2-1	Changed Security bit to Public bit.
ľ		3	Ŭ l	-	Added Override bit.
	н., I			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.
		1		3.4	Added SEC and SUS to file header.
				5=4	to a secure file sentence
					Deleted "file-identifier" and replaced with
				1 A.	"multifile-id" to asterisk precedes sentence.
ĺ				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
		l			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
			N Mala		
]	E	8/22/79	1) Nace	Changes	for MARK 9.0 Release
			V		Replaced SPO with ODT throughout.
				2-4	lindated syntax.
		1		2-5	Added *NONPRIV and PRIVATE to options and attributes.
					Added US Y to Example.
		λ.			Replaced *PRIV with Security.
					Replaced PHRIC with SECURITY.
				2-6	Replaced *SYS PACK with *SYS DISK.
				2.0	Indated *PRIVILEGED USER*
				2-8	Deleted CREATE throughout COMMAND RESTRICTIONS section
				2-0	Added sentence dealing with CREATE.
				2-9	Indated syntax.
					Added PRIVATE and *NONPRIV to options and attributes.
				2-10	Indeted Note
				2-10	Added IIS=REPTHA to Evennle
	•		-	2 1 1	Hudeted aunter
				2-11	Upuated Syntax.
I					Added PRIVALE, MPRIV, and MONPRIV to options and
				2 10	allributes.
				2-12	Added UHA BEKTHA/= TO EXAMPLE.
T				2-23	Added 20 and 27 to UUTPUT SPU ERROR MESSAGES.
	l a				
T		THE IN	FORMATION CO	NTAINED IN	I THIS DOCUMENT IS CONFIDENTIAL AND PROPRIETARY TO BURROUGHS DISCLOSED TO ANYONE OUTSIDE OF BURROUGHS CORPORATION WITHOUT
		THE DE	A HUN AND IS P	FIFACE EP	OM THE PATENT DIVISION OF BURROUGHS CORPORATION'
	× 5	INE PRI	OR WRITEN R	ELEASE FRI	

COMPANY CONFIDENTIAL B1800/B1700 FILE SECURITY P.S. 2219 0102 (G)

IABLE OF CONTENTS

FILE	SECUF	ITY	•	•	•	• •						•			•	•			• •					1-1
	INTRO	DUCI	ION	i																	-	-	-	1-1
	SECUR	F FI	IF	TD	FN	TTF	TE	RS																1 1
	RELAT	ה ה	loci	INE	NT	 . T T		11.0	1			•			•	•	•	•	• •	. •	•	•	•	1-1
EVCT.			10% 10	I FIL		A 1 1	. U N																	1-2
31310	- M / M A N	EUSE	. K 	•	•	• •	•		•	•	•	•	•		•. •	•	٠	•	• •			٠	•	2-1
4	STNIA	X DI	. AGR	AM	CI	ONV	EN	TI	ON	S														2-1
	CEFIN	ITIC	IN O	IF	TEI	RMS	ì		•		•			•			٠		• •		•		•	2-2
	USERC	ODE	ATT	RI	BU	TES	;																	2-4
		REST	RIC	TI	0 N .:	S .										-	· ·				_			2=6
	ITNE	PRTN	ITER	n s	UTI	- P 11 T		•	•		•	•	•	•	•	•		• •	•	•	•	• •	e	2 0
	PROGR		YEC	нт	Tni																			2-0
	I NOON	CON C	 				•			•			•		•	•	•	•	•	•		۰	•	2-8
		LUNS	ULE	. K	ET	BUA	RD	Ł	XE	CU	11	UN												2-8
		CARD	RE	AD	ER	EX	EC	UT	I 0	N		•				•		٠	• •	•	•			2-9
		AUTO	INAT	IC	F	EAT	U R	ES																2-9
		INFO	RMA	II	ÓN.	AL	ME	SS	AG	ES											-		-	2-9
	PROGR	AM T		TN	A T	TON	1					-	_	-		-	•	-		-		•	•	2-0
	COMMA	NDS																			•			2-9
	COMIN	COMP	-90 1 A ALIT	• n	• •	• • T D T	С Т	т о		•	•		•		•		۰	•	• •	•			•	2-9
		LUMP	ANU	R	сэ	IKI	LI	LU	ND															2-10
		AUU		•	٠		•	٠	٠	٠	•	٠	-	•	٠		•		٠		• •	• •		2-11
		CHAN	iGE																					2-13
		COPY		100		•	•	•		•	•			•	•	•					• •			2-15
		CREA	TE																	_				2-16
		DEBL	G					_	_	_	_	_	_	_	_	_								2-17
		DELE	. 15	•	-	•		•	•	•	•	•	•		•	•	•	• •		٠	• •	•		2-17
			 18 AV	,																				2-18
		0121	LAI		•	• •				49	•	•	•		•		•	•	¢. ≉		۰			2-19
		END																						2-20
		EOJ					4		3	•			٠		49			•	6	•				2-21
		LIST																						2-22
		PUNC	H	•	•							_		_			-	_			_		_	2-26
	OUTPU		TF	RR	กค	ME	< <	A C	FC		-		•	-			-	•				•		2-25
CREAT	TNC S	Fruo			בכ	FIL.		ņ u	LJ															2-23
CHLAI	DATON		i Li F	16	сJ		•	•	•				•	•	-	•	•	•	٠			• . •		5-1
	CAILM	MUU	E			_																		3-1
		PUBL	IC	FI	LES	S	٠	0	9		•	۲	-8		á.	•	•			•	•		· .	3-2
		CONT	ROL	0	F 1	[/0																		3-2
		REAC	-0N	LY	F]	ILE	S		•	•							•		•				_	3-3
		CONV	FRS	TO	N	r n	SF	сu	RF	F	TI	FS	-	•	~	• .			-	-		•		7 a 7
		DEEA	T	T	nFI		FT	FD	c	•	* L										- 1			J J 7
		SECH	OTT			181	. I	Ln	3	•	•		•	•		•	•			•	•	٠	•	5-4
		JELU	RI	I		VEL				_														3-6
		AUCE	. 55:	P	KI I	V V	5.	N	UN	-P	RI	V		•	•	•		• •	٠	•	• •	• •	•	3-6
		LOCK	:: P	RI	A 1	vs.	N	ON	- P	RI	۷													3-7
		APPE	NDE	D	บรเ	ERC	: O D	E S		•	•	•				•	•			•	•			3-7
		PREF	IXE	D	00.	T C	O M	MA	ND	S									-					3-9
		USFR	COD	F	BAI	скі	P	FT	IF	ŝ		-	-		_		_				-			7-0
	REMOT	E MO		-				• •	840 H.	5		۳	a .	•	•	•	•			40 a	• •	• •		J-7 7-10
	n L N U I		. O N 4	CT.	C M -	- 0 -																		5-10
		LUU-		31	un '	- U M	I	•	•	9	•		•	-		٠	•		•	٠	• •	•		5-10
		ากค	SPA	WN	IN	J																		3-11
		FILE	: HA	ND	LI	NG		•	٩	•	٠	6	•	é -		•	• •		٠		• •	•		3-11
		SYST	EM	DI	SPI	LAY	S.																	3-11

TC-2

BURROUGHS CORPORATION	COMPANY CONFIDENTIAL
COMPUTER SYSTEMS GROUP	B1800/B1700 FILE SECURITY
SANTA BARBARA PLANT	P.S. 2219 0102 (G)
BACKUP FILES	••••••••••••••
DISK PACK DEFAULTS	3-12
DEFINITIONS AND TABLES	•••••••••••••
FILE SECURITY IMPLEMENTATION	4-1
ACCESS/OPEN TABLE	• • • • • • • • • • • • • • 4-2

COMPANY CONFIDENTIAL B1800/B1700 FILE SECURITY P.S. 2219 0102 (G)

EILE SECURITY

INTROLUCTION

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 dataccmm activity but applies to both batch and remote modes of operation, even though its greatest application is in the area of dataccmm 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 ICENIIFIERS

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 wultifile-id given to the operating system is taken from the usercode field in the (SYSTEM)/USERCEDE 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.

COMPANY CONFIDENTIAL B1800/B1700 FILE SECURITY P.S. 2219 0102 (G)

1-2

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 PLBLIC, 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.

RELAIED DOCUMENTATION

Name

¶t – ≤

Number

B1800/B1700	MCP II			P.S.	2212 5426
B1800/B17C0	Software	Operational	Guide		1068731
B1800/B1700	HOST/RJE			P.S.	2212 0126

COMPANY CONFIDENTIAL B1800/E1700 FILE SECURITY P.S. 2219 0102 (G)

SYSIEM/MAKEUSER

The file-security system is initiatec by creating a system usercode 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/password pairs. Any batch program or remote user which attempts to create a secure file with a multifile-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 usercodes 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 combinations. 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	400	24 bits
User priority	-	4 bits
Privileged bit	-	1 bit
Security	- 4000	1 bit
Gverride	-	1 bit
Security level	-	2 bits
Maximum Time(Minutes)	-	16 bits
BNA Hostname	-	17 characters

SYNIAX DIAGRAM CONVENIIONS

Syntax diagrams display the required format for usercode attributes 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.

1

COMPANY CONFIDENTIAL B1800/B1700 FILE SECURITY P.S. 2219 0102 (G)

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. Erd-cf-statement is indicated by:

-----># Ccmments after the final operand may be preceded by a "2".

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 JERMS

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 cuote 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

2-2

COMPANY CONFIDENTIAL B1800/B1700 FILE SECURITY P.S. 2219 0102 (G)

the first name. The null string is allowed as the passwere 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 -	J0E/=
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 MCPrecognizable 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 retwork 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 ε minus sign.

BURROLGHS CORPORATION Computer systems group Santa Barbara plant

 \bigcirc

COMPANY CONFIDENTIAL B1800/B1700 FILE SECURITY P.S. 2219 0102 (G)

USEBCODE AIIRIBUIES

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:

1< 1 --/1*\----- US ----- <name> ---|-- = -->|-/1*\----- PW ------ <name> ---> 1 |-- = -->|-/1\----- PACK ----- <name> --1 1-- = -->1 --/1\----- CHG ----- <integer> --|-- = -->| --/1\----- PRI----- <integer> -| --- = -->1 -/1\----- SL ------ <integer> -| 1-- = -->1 /1\----- *PRIV -----I-- +NONPRIV -----/1\----- PUBLIC --I-- PRIVATE ---I

BURROUGHS CORPORATION COMPUTER SYSTEMS GROUP SANTA BARBARA PLANT

1

1

i e

COMPANY CONFIDENTIAL B1800/B1700 FILE SECURITY P.S. 2219 0102 (G)

1

----- MAXTIME ----- <integer> -1 1 1 I 1-- = -->1

I-- HOSTNAME ----- <identifier> -- I

1 1 1 1- = -->1 1---- *ANY ----1 1 1

1---- *NONE ----1

COMPANY CONFIDENTIAL B1800/B1700 FILE SECURITY P.S. 2219 0102 (G)

Semantics:

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

Gption	Attribute	Default
48 4a 49 49 10 10 10		-CC0 2550 4550 4550 4550 456
US	Usercode	None
PW	Password	None
PACK	Pack specification	System disk
CHG	Charge number	0
PRI	Limiting user jct 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

FESIRICTIONS

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

PACK: indicates default pack. All usercodes which belong to the same family wust 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 PRINIER OLIPUI

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

"SYSTEN/HAKEUSER"

RELEASI MARK X.O

COMPILE DATE/TIME = HENCAY 17 NOV 1980/15:18)

DEFAULT CHART DEFAULT SECURITY THE		SYSTE	4 USERCODE	FILE P	T HOST =	"51. A VE 3 "		RUN DATE	= TUESDAY	0 2	2 DECEMBER 1980 11:07	:49.9			COMP U
OLIS CALT CANDE C SYS DISK 0000000 12 PUBLIC C PUFFILEED USE 000000 PUBLIC PUBLIC PUBLIC PUFFILEED USE 000000 PUBLIC PUBLIC PUBLIC PUFFILEED USE 00000000 PUBLIC PUBLIC PUBLIC PUBLIC PUFFILEED USE 0000000 PUBLIC PUBLIC PUFFILEED USE USE 000000 PUBLIC PUBLIC PUFFILEED USE USE </th <th></th> <th>INDEX</th> <th>LSERCODE</th> <th>PASSHORE</th> <th>OVEKRIDE</th> <th>DEFAULT PACK</th> <th>CHARCE NUMBER</th> <th>DEF MAX PRIORITY</th> <th>SECURITY TYPE LEN</th> <th>T Tel</th> <th>"+FRIV"</th> <th>HOSTNAME</th> <th></th> <th>NAXTINE NINUTES</th> <th>HER HAN</th>		INDEX	LSERCODE	PASSHORE	OVEKRIDE	DEFAULT PACK	CHARCE NUMBER	DEF MAX PRIORITY	SECURITY TYPE LEN	T Tel	"+FRIV"	HOSTNAME		NAXTINE NINUTES	HER HAN
DD14 (ACTUD) C AACC 0 V 0000000 12 PUBLIC 0 PPHVILEGE0 U ADDE COUNTY CTSTERS ADDE ADDE <thadde< th=""> <thadde< th=""> ADDE</thadde<></thadde<>		0139	(ACT)	CANDE	0	*SYS DISK*	0000000	12	PUBLIC	C	*PRIVILEGED USER*		*NONE	00000	2 2
0287 (ALF HQ) 0 0 3 KCP COMMON 12 PUBLIC C PUBLIC 0 STATE 7 0300 (ALF HQ) 0 0 SKCP COMMON 12 PUBLIC C PUBLIC 0 SKTET 7 SKTET 7 0300 (ALF HQ) 0 PC AKSTA COMMON 12 PUBLIC C PUBLIC 0 SKTET 7		0014	(ACTU)	CANCE	0	U	0000000	12	PUBLIC	0	*PRIVILEGED USER*		*NONE	00000	> < C
degs (AMALTIO) (CF) 0.000000 12 PULLE 0 PULLE		0287	(ALFURD)	8	0	SHCP	000000	12	PUBLIC	C	*PRIVILEGED USER*		*NONE	00000	A NO
0355 CAMALTI1 ACF C SALETY 0000000 12 FUNICE C FUNICE SALETY FUNICE C FUNICE C FUNICE C FUNICE		0830	(ANALY10)	MCP	Q	SHCP	00000000	12	PUBLIC	0	*PRIVILEGED USER*		+NUNE	00000	
1023 (Mai/A) 0************************************		0065	(ANALY11)	NCP	C	SNCP	0000000	12	PUBLIC	6	*PRIVILEGED USER*		TNUNE	00000	
06161 CARSIND CARSIND CARSIND CARSIND CARSIND CARSIND 0050 CARTUND LE GERARE 0 D CONDOCO 12 PUBLIC C PRIVILEGED USER+ *NORE CONDO 0050 CARTUND LE GERARE 0 D CONDO 12 PUBLIC C PRIVILEGED USER+ *NORE CONDO 0050 CARTUND LE GERARE 0 D CONDO 12 PUBLIC C PRIVILEGED USER+ *NORE CONDO 00515 GERARENTO D D CONDONO 12 PUBLIC C PRIVILEGED USER+ *NORE CONDO 0052 CERARENTO D D D D D PUBLIC C PRIVILEGED USER+ *NORE CONDO 12		1023	(ANS174)	86	C C	ANS 174	0000000	12	PUBLIC	0	*PRIVILEGED USEP*		+NONE	00000	E S H
0.005 CANHAMUN DEC.GRANC 0 0 0.000000 12 PUBLIC 0 PRIVILEGED 000000 10 PUBLIC 0 PRIVILEGED 0000000 10 PUBLIC <t< td=""><td></td><td>0208</td><td>(ANSI/4)</td><td></td><td>0</td><td>ANS174</td><td>0000000</td><td>12</td><td>PUBLIC</td><td>C C</td><td>*PRTVILEGED USER*</td><td></td><td>+NONE</td><td>00000</td><td>A A</td></t<>		0208	(ANSI/4)		0	ANS174	0000000	12	PUBLIC	C C	*PRTVILEGED USER*		+NONE	00000	A A
Bits Like Like <thlike< th=""> Like Like <thl< td=""><td></td><td>0101</td><td>CARIJ ZADTHHUN</td><td>AKI 15.CRAND</td><td>0</td><td>R</td><td>0000000</td><td>12</td><td>PUSEIC</td><td>õ</td><td>*PRIVILEGED USER=</td><td></td><td>*NONE</td><td>00000</td><td>Z G H</td></thl<></thlike<>		0101	CARIJ ZADTHHUN	AKI 15.CRAND	0	R	0000000	12	PUSEIC	õ	*PRIVILEGED USER=		*NONE	00000	Z G H
0515 051 <td></td> <td>0050</td> <td>(AV)</td> <td>AUT</td> <td>. 0</td> <td>x</td> <td>00000000</td> <td>12</td> <td>PUBLIC</td> <td>č</td> <td>*PRIVILEGED USER*</td> <td></td> <td>+NONE</td> <td>00000</td> <td>ㅋ콩ㅋ</td>		0050	(AV)	AUT	. 0	x	00000000	12	PUBLIC	č	*PRIVILEGED USER*		+NONE	00000	ㅋ콩ㅋ
Dids CALL C Did Did CALL PUBLIC PHYLICED USER* PHONE DODOD 0053 CGAN TARD D DODOD Did DODOD PHYLICED USER* PHONE DODOD 0053 CGANCALD N D DODOD DIS PHYATE C PHYLICED USER* PHONE DODOD 0053 CGANCALD N DIS DODOD DIS PHONE C PHONE DODOD PHONE DODOD PHONE DODOD PHONE PHONE PHONE PHONE PHONE PHONE DODOD PHONE	٠.	0515	(8)		Ő	*SYS DISK*	8896860	12	PUBLIC	č	*PRIVILEGED USER*		*NONE	00000	
D654 COARNY YARD 0 BMA 0000000 12 PRIVATE C +PRIVILEGE USER* +HONE 00000 0057 CRALENLY R 0 +SYS DISK* 0000000 12 PRIVATE C +PRIVILEGE USER* +HONE 00000 0015 CRALENLY 0 +SYS DISK* 0000000 12 PRIVATE C +PRIVILEGE USER* +HONE 000000 1022 CRALENLY 0 +SYS DISK* 0000000 12 PRIVILEGE USER* +HONE 000000 1021 CRALE 0 +SYS DISK* 0000000 12 PRIVILEGE USER* +HONE 000000 1021 CRALE 0 DAA 0000000 12 PRIVILEGE USER* +HONE 00000 1021 CRALE DAA 0000000 12 PRIVILEGE USER* +HONE 00000 1021 CRALE DAA 0000000 12 PRIVILEGE USER* +HONE 00000 1021 CRALE DAA 0000000 <		0486	(BANBI)	нC	Č	DC	0000000	14	PUBLIC	0	*PRIVILEGED USER*		*NONE	00000	
0075 CRAIESS AL 0 D 0000000 15 PRIVALESC **PRIVALEGED USER* **NONE 00000 0692 CARLELD # 6 *STS DISK* 0000000 12 PUBLIC 0 *PRIVALEGED USER* **NONE 00000 1003 CGULO CLF 0 *STS DISK* 0000000 12 PUBLIC 0 *PRIVALEGED USER* **NONE 00000 0021 CGULO CLF 0 *STS DISK* 0000000 12 PUBLIC **PRIVALEGED USER* **NONE 000000 1021 CGNA) NARADE DNA 0000000 12 PUBLIC **PRIVALEGED USER* *NONE 000000 1021 CGNA) NURPHY DNA 0000000 12 PUBLIC **PRIVALEGED USER* *NONE 000000 1021 CGNA) NURPHY DNA 0000000 12 PUBLIC **PRIVALEGED USER* *NONE 000000 1022 CGNA) NURPHY DNA <td< td=""><td></td><td>0634</td><td>(BARN)</td><td>YARD</td><td>0</td><td>BNA</td><td>0000000</td><td>12</td><td>PRIVATE</td><td>C</td><td>*PRIVILEGED USER*</td><td></td><td>*NONE</td><td>00000</td><td>-</td></td<>		0634	(BARN)	YARD	0	BNA	0000000	12	PRIVATE	C	*PRIVILEGED USER*		*NONE	00000	-
Decg: CALVERLED H 0 +STS DISK 000000 12 PUBLIC 0 +PHIVILEGED USER** +NONE 000000 1022 COLC1 DLC 0 +STS DISK* 000000 12 PUBLIC 0 +PHIVILEGED USER** +NONE 000000 1022 COLC1 DLC 0 +STS DISK* 000000 12 PUBLIC 0 +PHIVILEGED USER** +NONE 000000 1022 COLC1 DLC 0 +STS DISK* 0000000 12 PUBLIC 0 +PHIVILEGED USER** +NONE 000000 1021 CONA MTARSI DNA 0000000 12 PUBLIC 0 +PHIVILEGED USER** +NONE 000000 1021 CONA MTARSI DNA 0000000 12 PUBLIC +PHIVILEGED USER** +NONE 000000 1021 CONA MTARSI DNA 00000000	,	0075	(BATES)	AL	0	a	00000000	15	PRIVATE	C	*PRIVILEGED USÉR*		*NONE	00000	
1001 CDLC) DDLC 0 *SYS DISK* 000000 12 PUBLIC 0 *PRIVILEGED USER* *ADDE 00000 0122 CBLC) CLFH SKCP 000000 12 PUBLIC 0 *PRIVILEGED USE* *ADDE 00000 0210 GIELUNIN ALCAARD SKCP 000000 12 PUBLIC 0 *PRIVILEGED USE* *ADDE 00000 1011 GBAN MARLE DAA 0000000 12 PUBLIC *PRIVILEGED USE* *ADDE 00000 1020 GBAN MARDE DAA 0000000 12 PUBLIC *PRIVILEGED USE* *ADDE 00000 1020 GBAN MARDE DAA 0000000 12 PUBLIC *PRIVILEGED USE* *ADDE 00000 1022 GUEAS SUADA U 0000000 12 PUBLIC *PRIVILEGED USE* *ADDE 000000 1016 GUEAS SUADA U 00000000 12 PUBLIC *PRIVILEGED USE* <td></td> <td>0692</td> <td>(BAUERLE)</td> <td>R</td> <td>0</td> <td>*SYS DISK*</td> <td>00000000</td> <td>12</td> <td>PUBLIC</td> <td>0</td> <td>*PRIVILEGED USER*</td> <td></td> <td>*NONE</td> <td>00000</td> <td></td>		0692	(BAUERLE)	R	0	*SYS DISK*	00000000	12	PUBLIC	0	*PRIVILEGED USER*		*NONE	00000	
1022 CBLC) CLEM 0 *SYS DISK* 0000000 12 PUBLIC 0 *PRIVILEGED VERV *ADDE 00000 0210 GBLAN MEC SMCP 000000 12 PUBLIC C *PRIVILEGED VERV *ADDE 00000 0210 GBLAN MEANDE DAA 000000 12 PUBLIC C *PRIVILEGED VERV *ADDE 00000 1021 GBAN MEANDE DAA 000000 12 PUBLIC C *PRIVILEGED VERV *ADDE 00000 1021 GBAN MEANDE DAA 000000 12 PUBLIC C *PRIVILEGED VERV *ADDE 000000 0022 GBERAN SKELY DATACOM 0000000 12 PUBLIC *PRIVILEGED VERV *ADDE 000000 12 PUB		1003	(8010)	BDLC	. 0	*SYS DISK*	0000000	12	PUBLIC	0	*PRIVILEGED USER*		*NONE	00000	
0772 CBERN MEP 0 0000033 12 PUBLIC C PHIVILEED USER* MUME 00000 1010 CBLAN ARAUL C DAA 000000 12 PUBLIC C PHIVILEED USER* MUME 000000 1011 CBAN MARSIN DAA 0000000 12 PUBLIC C PHIVILEED USER* MUME 000000 1011 CBAN TARSIN O DAA 0000000 12 PUBLIC C PHIVILEED USER* MUME 000000 0017 EIPO BELLIDA O ASS DISK 0000000 12 PUBLIC C PHIVILEED USER* MUME 000000 0012 CBARAN SHELY O DATACOM V 0000000 12 PUBLIC C PHIVILEED USER* MUME 000000 012 CBARCER TGH O D 00000000 12 PUBLIC		1022	(BDLC)	CLEN	0	*SYS DISK*	0000000	12	PUBLIC	0	*PRIVILEGED USER*		*NONE	00000	
0210 CHALLEN RICHARD C *STS DISK* 0000000 12 PUBLIC C *RIFILECD USER* *NUME 00000 1019 CBA1 MTAMS C DBAA 0000000 12 PUBLIC C *RIFILECD USER* *NUME 00000 1021 CBA1 MTAMS C DBAA 0000000 12 PUBLIC C *RIFILECD USER* *NUME 00000 0017 CBD- SELINDA 0 SYS DISK* 0000000 12 PUBLIC C *RIFILECD USER* *NOME 00000 0015 TEMAND SHELY OATACAM 0000000 12 PUBLIC C *RIFILECD USER* *NOME 00000 0152 CBARCE(N) TOM O OATACAM 0000000 12 PUBLIC *RIFILECD USER* *NOME 00000 0152 CBARCE(N) TOM O OATACAM OATACAM PUBLIC *RIFILECD USER* *NOME 00000 12 PUBLIC *RIFILECD USER* *NOME 00000 12 PUBLIC *RIFILECD USER* *NOME 00000 12 PUBLIC *RIFILECD USER* *NOME 000000 12<		0772	(8EN)	NCP	0	SHCP	0000000	12	PUBLIC	C	*PRIVILEGED USER*		*NUNE	00000	
1011 CHAAJ AHAULL 0 DAA 0000000 12 FUBILE C FRUTLEED DSER FRUTLEED DSER <td></td> <td>0210</td> <td>(BIGELUW)</td> <td>RICHARD</td> <td>ç</td> <td>*SYS DISK*</td> <td>0000000</td> <td>12</td> <td>PUBLIC</td> <td>C</td> <td>*PRIVILEGED USER*</td> <td></td> <td>#NUNE</td> <td>00000</td> <td></td>		0210	(BIGELUW)	RICHARD	ç	*SYS DISK*	0000000	12	PUBLIC	C	*PRIVILEGED USER*		#NUNE	00000	
1021 104A3 FTAAS 0 DAA 0000000 12 FUBILE -FRIVILEGED DEF- FUDE FUDE <td></td> <td>1019</td> <td>(BNA)</td> <td>ARNOLD</td> <td>0</td> <td>UNA</td> <td>00000000</td> <td>12</td> <td>PUBLIC</td> <td>u c</td> <td>=FRIVILEGED USER=</td> <td></td> <td></td> <td>00000</td> <td></td>		1019	(BNA)	ARNOLD	0	UNA	00000000	12	PUBLIC	u c	=FRIVILEGED USER=			00000	
1020 LUMAY MUMPH 0 DMA 0000000 12 PUBLIC -*PTIVILEGED DUSCH *NOME 000000 0011 CBA TARIDA 0 DATACOMM 0000000 12 PUBLIC -*PTIVILEGED DUSCH *NOME 000000 0015 CBA SUMAD 0 DATACOMM 0000000 12 PUBLIC -*PTIVILEGED USCH *NOME 000000 0155 CBMAGEN SUMAD 0 DATACOMM 0000000 12 PUBLIC -*PTIVILEGED USCH *NOME 000000 0155 CBMAGEN SUMAD 0 D 00000000 12 PUBLIC *PTIVILEGED USCH *NOME 000000 1016 CB190C3 BA 0 D 00000000 12 PUBLIC *PTIVILEGED USCH *NOME 000000 14 PUBLIC *PTIVILEGED USCH *NOME 000000 14 PUBLIC *PTIVILEGED USCH *NOME 000000 14 000000 12 PUBLIC *PTIVILEGED USCH *NOME <td></td> <td>1021</td> <td>(UNA)</td> <td>HIANS</td> <td>0</td> <td>DNA</td> <td>0000000</td> <td>12</td> <td></td> <td>ň ·</td> <td>*PRIVILEGED VJER*</td> <td></td> <td>+NONE</td> <td>00000</td> <td></td>		1021	(UNA)	HIANS	0	DNA	0000000	12		ň ·	*PRIVILEGED VJER*		+NONE	00000	
0013 00000 12 PUBLIC 0 PRIVILEED 00000 00000 0022 00000 000000 12 PUBLIC 0 PRIVILEED 00000 000000 0022 00000 000000 12 PUBLIC 0 PRIVILEED 00000 000000 0022 000000 12 PUBLIC 0 PRIVILEED 00000 000000 00122 000000 12 PUBLIC 0 PRIVILEED 00000 000000 00122 0000000 12 PUBLIC 0 PRIVILEED 0100000 000000 000000 12 PUBLIC 0 PRIVILEED 010000 000000 000000 000000 0000000 000000 0		1020	(DNA)	NURPHI	0	DNA RNA	0000000	12	PHRITC	č	*PRIVILEGED USER*		ANONE	00000	
0022 CB1/MAD 00171 CD174 00171 CD174 CD174 <t< td=""><td></td><td>0011</td><td>(BP)</td><td>RELINDA</td><td>. 0</td><td>ASYS DISKA</td><td>0000000</td><td>12</td><td>PUBLIC</td><td>õ</td><td>*PRIVILEGED USER*</td><td></td><td>+NONE</td><td>00000</td><td></td></t<>		0011	(BP)	RELINDA	. 0	ASYS DISKA	0000000	12	PUBLIC	õ	*PRIVILEGED USER*		+NONE	00000	
00157 CBUGD 0		0022	(RRYAN)	SHELLY	ő	DATACONM	00000000	12	PUBLIC	ă	*PRIVILEGED USER*		*NONE	00000	
0152 CBURCELL) TUN 0 X 0000000 12 PUBLIC G PRTVILEGED USER+ *NONE 000000 1016 G19DCJ D 0 0000000 12 PUBLIC G *PRTVILEGED USER+ *NONE 000000 1016 G19DCJ D 0 0000000 12 PUBLIC G *PRTVILEGED USER+ *NONE 000000 0166 G6800J 0 *SYS DISK* 0000000 12 PUBLIC G *PRTVILEGED USER+ *NONE 000000 10 0166 CANEEJY OFFLINE *SYS DISK* 0000000 12 PUBLIC *PRTVILEGED USER+ *NONE 000000 10 *NONE 000000 12 PUBLIC *PRTVILEGED USER+ *NONE 000000 PUBLIC *NONE 000000 PUBLIC *RTVILEGED USER+ *NONE 000000 PUBLIC *RTVILEGED USER+ *NONE 000000 PUBLIC *NONE 000000 PUBLIC *NONE 0000000 PUBLIC		0157	(BhG)	SAHAD	õ	4	0000000	12	PUBLIC	č	*PRIVILEGED USER*		+NONE	00000	
1016 (6190C) 0 0 000000 12 PUBLIC C +PRTVILEGED USEP+ +NOME 000000 0666 066900 0 *SYS <disk+< td=""> 0000000 12 PUBLIC C +PRTVILEGED USEP+ +NOME 000000 10 0771 (C) S 0 *SYS<disk+< td=""> 0000000 12 PUBLIC C +PRTVILEGED USEP+ +NOME 000000 10 0116 (CANEE) K 0 000000 12 PUBLIC C +PRTVILEGED USEP+ +NOME 000000 10 1015 (CANEE) KH 0 BHA 0000000 12 PUBLIC C +PRTVILEGED USEP+ +NOME 000000 PDT PDT<td></td><td>0152</td><td>(BURGER)</td><td>TOM</td><td>0</td><td>X</td><td>0000000</td><td>12</td><td>PUBLIC</td><td>C</td><td>*PRIVILEGED USER*</td><td></td><td>*NONE</td><td>00000</td><td></td></disk+<></disk+<>		0152	(BURGER)	TOM	0	X	0000000	12	PUBLIC	C	*PRIVILEGED USER*		*NONE	00000	
101E (0190C) BA 0 0 0000000 12 PUBLIC C +PRIVILEGED USER* +NONE 000000 II 0466 (06600) 0 +SYS <disk*< td=""> 0000000 12 PUBLIC C +PRIVILEGED USER* +NONE 000000 II 0156 (CACHEXY) 0FFLINE 0 *SYS<disk*< td=""> 0000000 12 PUBLIC C +PRIVILEGED USER* +NONE 000000 00000 00000 000000</disk*<></disk*<>		1018	(B190C)		Ō	D	00000000	12	PUBLIC	C	*PRIVILEGED USER *		*NONE	00000	
Obset OBSET OFFLIGE Stress NOME OD0000 Image: Constraint of the con		1016	(819DC)	BA	. · · · · · · · · · · · · · · · · · · ·	D	0000000	12	PUBLIC	C	*PRIVILEGED USER*		*NONE	00000	
0771 (C) S 0 *SYS DISK* 0000000 12 PUBLIC C *PRIVILEGED USER* *NONE 000000 000000 1015 (CANDE) E 0 BNA 0000000 12 PUBLIC C *PRIVILEGED USER* *NONE 000000 000000 0421 (CANDE) E 0 BNA 0000000 12 PUBLIC C *PRIVILEGED USER* *NONE 000000 000000 000000 12 PUBLIC *PRIVILEGED USER* *NONE 000000 D 000000 D 1015 (CANDE) *NONE 000000 D PUBLIC *PRIVILEGED USER* *NONE 000000 D D PUBLIC *PRIVILEGED USER* *NONE 000000 D D PUBLIC *PRIVILEGED USER* *NONE 000000 S O O N NONE 00000 S O N NONE 000000 S O N NONE 00000 S O N NONE 00000 S O N NONE 00000 S O N NONE 000000 S NONE		0888	(86800)		0	*SYS DISK*	0000000	12	PUBLIC	C	*PRIVILEGED USER*		*NONE	00000	
0136 (CACHERY) 0FFLIME 0 *YS DISK 0000000 12 PUBLIC C *PRIVILEGED USER* *NONE 000000 00000 0421 (CANDE) KH 0 BMA 0000000 12 PUBLIC C *PRIVILEGED USER* *NONE 000000 DO000 DO0000 PUBLIC C *PRIVILEGED USER* *NONE 000000 SOON DO0000 DO00000 SOON DO0000		0771	(0)	S	0	*SYS DISK*	0000000	12	PUBLIC	C	*PRIVILEGED USER*		=NONE	00000	3
1015 (CANDE) EK 0 BNA 0000000 12 PUBLIC 0 PUBLI		0136	(CACHEXY)	OFFLINE	0	*SYS DISK*	0000000	12	PUBLIC	G	*PRIVILEGED USER*		*NONE	00000	0
0421 CCANDE) KH 0 BNA 0000000 12 PUBLIC C *PRIVILEGED USER* *NONE 000000 PIERY 0316 CCC) CC 0 X 0000000 12 PUBLIC C *PRIVILEGED USER* *NONE 000000 PIERY 0647 CCHOYE) RANDY 0 RJCC 0000000 12 PUBLIC C *PRIVILEGED USER* *NONE 000000 SOOO PIERY 0647 CCHRISTY) P0B0 0 *SYS DISK* 0000000 12 PUBLIC C *PRIVILEGED USER* *NONE 000000 SOOO ON		1015	(CANDE)	Eh	0	BNA	0000000	12	PUBLIC	G	*PRIVILEGED USER*		*NUNE	00000	0
0315 (CL) CL 0 X 000000 12 PUBILC 0 PRIVILEGED 054P* *NONE 000000 PIX 0316 (CF) CHAISIY 0 *SYS DISK* 0000000 12 PUBILC C *PRIVILEGED USER* *NONE 000000 %OO %OO 0647 (CHRISIY) POBD 0 *SYS DISK* 0000000 12 PUBIC C *PRIVILEGED USER* *NONE 000000 %OO		0421	(CANDE)	KH	Û	BNA	0000000	12	PUBLIC	C	*PRIVILEGED USER*		TNUNE	00000	≥ 0
0310 CLF/Y CHRISIT 0 #SIS DISK* 000000 12 PUBLIC C *PRIVILEGED USER* *NORE 00000 5 O 0647 (CHRISIY) P080 0 *SYS DISK* 0000000 12 PUBLIC C *PRIVILEGED USER* *NORE 00000 *O O 0331 (CL) CL 0 X 0000000 12 PUBLIC *PRIVILEGED USER* *NORE 00000 *O O X 000000 *O Y O O X 000000 12 PUBLIC *PRIVILEGED USER* *NORE 00000 N N T C O N N T C O N <t< td=""><td></td><td>0315</td><td></td><td></td><td>U</td><td>A DICKA</td><td>0000000</td><td>12</td><td>PUBLIC</td><td>c U</td><td>-FRIVILLUED USER-</td><td></td><td></td><td>00000</td><td></td></t<>		0315			U	A DICKA	0000000	12	PUBLIC	c U	-FRIVILLUED USER-			00000	
0647 (CHR1E) NADL 0 NSC 0000000 12 PUBLIC C PHRIVILEGED USER* *NONE 000000 *O 0331 (CL) CL C X 0000000 12 PUBLIC C *PRIVILEGED USER* *NONE 000000 *O Y 0841 (CLD) CYNDY 0 DATACOMH 0000000 12 PUBLIC C *PRIVILEGED USER* *NONE 00000 NT 0132 (COBIN) DARRYL 0 *SYS DISK* 0000000 12 PUBLIC C *PRIVILEGED USER* *NONE 00000 NT C 0132 (COBIN) DARRYL 0 *SYS DISK* 0000000 12 PUBLIC C *PRIVILEGED USER* *NONE 000000 NT C *NONE 000000 NT C *SYS DISK* 0000000 12 PUBLIC *PRIVILEGED USER* *NONE 000000 D T T T C *SYS DISK* 000000		0510	(04045)	CHNISII	U O	*212 DI2V=	00000000	12	PUBLIC	č	+PRIVICEDED USER-		*NONE	00000	
0331 CLL CL CX 0000000 12 PUBLIC C PRIVILEGED USER* *NONE 00000 NT 0841 CLD CYNDY 0 DATACOMM 0000000 12 PUBLIC C *PRIVILEGED USER* *NONE 00000 NT 0588 CLHD DMS 0 *SYS DISK* 0000000 12 PUBLIC C *PRIVILEGED USER* *NONE 00000 NT C 0132 CC0B0L74) DARKYL 0 *SYS DISK* 0000000 12 PUBLIC C *PRIVILEGED USER* *NONE 00000 NT C 1014 CC0B0L74) PRIV C C0B00000 12 PUBLIC C *PRIVILEGED USER* *NONE 000000 15 PRIVILEGED USER* *NONE 000000 15 PRIVILEGED USER* *NONE 000000 16 PUBLIC *PRIVILEGED USER* *NONE 000000 01 C PRIVILEGED USER* *NONE 000000 01		0647	(CHQISTY)	PORO	0	ASYS DISKA	0000000	12	PURLTC	õ	*PRIVILEGED USER*		*NONE	00000	SON
0841 (CLD) CYNDY 0 DATACOMM 000000 12 PUBLIC C *PRIVILEGED USER* *NONE 00000 PUBLIC *PRIVILEGED USER* *NONE 000000 PUBLIC *PRIVILEGED USER*<		0331	(CI)	CI	ő	X DIG DIGN-	00000000	12	PUBLIC	č	*PRIVILEGED USER*		+NONE	00000	• o z
0588 (CLH) DHS 0 *SYS DISK* 000000 12 PUBLIC C *PRIVILEGED USER* *NONE 00000 PUBLIC *PRIVILEGED USER* *NONE 0		0841	(CLO)	CYNDY	0	DATACOMM	0000000	12	PUBLIC	ā	*PRIVILEGED USER*		+NONE	00000	≺
0132 (C0BIN) DARRYL 0 *SYS DISK* 0000000 12 PUBLIC C *PRIVILEGED USER* *NONE 00000 9 M 1014 (C0B0L74) PRIV 0 C0B0L74 0300000 12 PUBLIC C *PRIVILEGED USER* *NONE 00000 9 M N <td></td> <td>0588</td> <td>(CLH)</td> <td>DMS</td> <td>Ō</td> <td>*SYS DISK*</td> <td>0000000</td> <td>12</td> <td>PUBLIC</td> <td>Ć</td> <td>*PRIVILEGED USER*</td> <td></td> <td>*NONE</td> <td>00000</td> <td></td>		0588	(CLH)	DMS	Ō	*SYS DISK*	0000000	12	PUBLIC	Ć	*PRIVILEGED USER*		*NONE	00000	
1014 (COBOL74) PRIV C COBOL74 0300000 12 PUBLIC G *PRIVILEGED USER* *NONE 00000 9 MT 0024 (CON) CLH G *SYS DISK* 0300000 12 PUBLIC G *PRIVILEGED USER* *NONE 00000 9 MT 0844 (CONTROL) PATCH G PATCH80 0000000 12 PUBLIC *PRIVILEGED USER* *NONE 00000 0 MT MONE 00000 MT MONE 00000 MT MT MONE 000000 MT MONE <t< td=""><td></td><td>0132</td><td>(COBIN)</td><td>DARRYL</td><td>0</td><td>*SYS DISK*</td><td>0000000</td><td>12</td><td>PUBLIC</td><td>C</td><td>*PRIVILEGED USER*</td><td></td><td>*NONE</td><td>00000</td><td></td></t<>		0132	(COBIN)	DARRYL	0	*SYS DISK*	0000000	12	PUBLIC	C	*PRIVILEGED USER*		*NONE	00000	
0024 (CON) CLH C *SYS DISK* 0000000 12 PUBLIC C *PRIVILEGED USER* *NONE 000000 000000 12 PUBLIC C *PRIVILEGED USER* *NONE 000000 000000 12 PUBLIC C *PRIVILEGED USER* *NONE 000000 000000 12 PUBLIC C *PRIVILEGED USER* *NONE 000000 12 PUBLIC C *PRIVILEGED USER* *NONE 000000 12 PUBLIC C *PRIVILEGED USER* *NONE 00000 12 PUBLIC C *PRIVILEGED USER* *NONE 00000 12 PUBLIC C *PRIVILEGED USER* *NONE 00000 NC 22 PUBLIC C *PRIVILEGED USER* *NONE 000		1014	(COBOL74)	PRIV	C	COBOL74	000000	12	PUBLIC	C	*PRIVILEGED USER*		*NONE	00000	v m z
0884 (CONTROL) PATCH 0 PATCH8.0 000000 12 PUBLIC 0 *PRIVILEGED USER* *NONE 00000 PME 0335 (CP) CP 0 X 000000 12 PUBLIC 0 *PRIVILEGED USER* *NONE 00000 PME 0905 (CRN) KLEIN 0 *SYS DISK* 000000 12 PUBLIC 0 *PRIVILEGED USER* *NONE 00000 Cmm Cmm 00000 Cmm Cmm 00000 Cmm Cmm 00000 Cmm Cmm 00000 Cmm PUBLIC *PRIVILEGED USER* *NONE 00000 Cmm Cmm Cmm 00000 Cmm		0024	(CON)	CLH	С	*SYS DISK*	0000000	12	PUBLIC	C	*PRIVILEGED USER*		*NONE	00000	
0335 C(P) CP 0 X 0000000 12 PUBLIC 0 *PRIVILEGED USER* *NONE 000000 D D D 000000 D *PRIVILEGED USER* *NONE 000000 D D D D 000000 D PUBLIC 0 *PRIVILEGED USER* *NONE 00000 D PUBLIC 0 *PRIVILEGED USER* *NONE D </td <td></td> <td>0884</td> <td>(CONTROL)</td> <td>PATCH</td> <td>C</td> <td>PATCH8.0</td> <td>0000000</td> <td>12</td> <td>PUBLIC</td> <td>C</td> <td>*PRIVILEGED USER*</td> <td></td> <td>*NONE</td> <td>00000</td> <td>O S H</td>		0884	(CONTROL)	PATCH	C	PATCH8.0	0000000	12	PUBLIC	C	*PRIVILEGED USER*		*NONE	00000	O S H
0905 (CRIN) RLEIN 0 *SYS 0300000 12 PUBLIC 0 *PRIVILEGED USER* *NONE 00000 NC NC 0346 (CS) 0 *SYS DISK* 000000 15 PRIVILE *PRIVILEGED USER* *NONE 00000 NC NC 0509 (CURNY) SAWYER 0 *SYS DISK* 000000 12 PUBLIC C *PRIVILEGED USER* *NONE 00000 NC NO 0509 (CURNY) SAWYER 0 *SYS DISK* 000000 12 PUBLIC *PRIVILEGED USER* *NONE 00000 NC NO NO <td></td> <td>0335</td> <td>(40)</td> <td>CP</td> <td>0</td> <td>X</td> <td>0000000</td> <td>12</td> <td>PUBLIC</td> <td>0</td> <td>*PRIVILEGED USER*</td> <td></td> <td>*NONE</td> <td>00000</td> <td>H M C</td>		0335	(40)	CP	0	X	0000000	12	PUBLIC	0	*PRIVILEGED USER*		*NONE	00000	H M C
0346 CCSJ 0 *STS DISK* 0000000 15 PRIVALE *PRIVILEGED *NONE 000000 NO NO 0509 (CURRY) SAWYER 0 *SYS DISK* 600000 12 PUBLIC *PRIVILEGED USER* *NONE 00000 NO		0905	(CRIN)	KLEIN	U	*SYS DISK*	0000000	12	PUBLIC	0	*PRIVILEGED USER*		*NUNE	00000	S C E
0009 CURRTJ SANTER 0 *STS 01518* 000000 12 PUBLIC C *PRIVILEGED USER* *NONE 00000 DUDU 1013 (C74DR) PRIV 0 CCB0L74 000000 12 PUBLIC C *PRIVILEGED USER* *NONE 00000 DUDU 0569 (DA) BP 0 *SYS DISK* 0000000 12 PUBLIC 0 *PRIVILEGED USER* *NONE 00000 DUDU DU		0346	(05)		0	*SYS DISK*	00000000	15	PRIVATE	0	*PRIVILEGED USER*		=NUNE	00000	
1013 CCF4UR7 FR1V G CCBUL74 000000 12 PUBLIC C #PRIVILEGED USER* #NONE 00000 D D 0569 (DA) BP 0 *SYS DISK* 0000000 12 PUBLIC 0 *PRIVILEGED USER* *NONE 00000 D		0509	(CZ(20)	SANYER	U	*515 DISK*	0000000	12	PUBLIC	U c	*LATAITECED NELD*			00000	
0503 (DAA) 0 +5YS DISK* 0000000 12 PUBLIC 0 +PRIVILEGED USER* +NONE 000000 0503 (DAA) DAA 0 +SYS DISK* 0000000 12 PUBLIC 0 +PRIVILEGED USER* +NONE 00000 0426 (DAH) DCNNA C DATACONH 0000000 12 PUBLIC 0 +PRIVILEGED USER* +NONE 00000 0124 (DASOL) DGN C 0ASOL 0000000 12 PUBLIC C +PRIVILEGED USER* +NONE 00000 0124 (DASOL) DGN C 0ASOL 0000000 12 PUBLIC C +PRIVILEGED USER* +NONE 00000 0124 (DAV) SYS C +SYS DTSK* 0000000 12 PUBLIC C +PRIVILEGED USER* +NONE 00000 0125 C +SYS DTSK* 0000000 12 PUBLIC +PRIVILEGED USER* +NONE 00000		1013	1043	3" K L V 19 17	U A	ACVC DICER	0000000	12	PUDLEC	0	*POTATIEDEN AGEN*			00000	5 - >
0305 0305 0305 12 FUBLIC 0 FRIVILEGED 0307 0426 0404 DCNA C DATACONN 000000 12 PUBLIC 0 *PRIVILEGED USER* *NONE 00000 0124 (DASDL) DGN C 0ASEL 00000000 12 PUBLIC C *PRIVILEGED USER* *NONE 00000 0124 (DASDL) DGN C 0ASEL 0000000 12 PUBLIC C *PRIVILEGED USER* *NONE 00000 0124 (DASDL) DGN C 0ASEL 00000000 12 PUBLIC C *PRIVILEGED USER* *NONE 00000 0124 (DASDL) DGN C >SYS DTSK* 300000 12 PUBLIC C *PRIVILEGED USER* *NONE 00000 04/25 CDAVEN SYS DTSK* 300000 12 PUBLIC *PRIVILEGED USER* *NONE 00000		0503	(DAL)	រា។ រា៖ ត		- 319 DT2V+	0000000	12	FUDLIC	0	*POTVILLUED USEN=			00000	じょう
0124 (DASDLJ DEN C DASEL 0003030 12 PUBLIC C «PRIVILEGED USER» NONE 00000 0124 (DASDLJ DEN C DASEL 0003030 12 PUBLIC C «PRIVILEGED USER» NONE 00000 04/5 (DAVE) C #SSC C #SSC DISK# 3004000 12 PUBLIC C #PRIVILEGED USER* *NONE 00000		0,00,0	(DAH)	DENKA	о г	-212 DIJV#	00000000	12	PUBLIC	ñ	*PRTVTIEGED USEN=		*NONF	00000	
		0020	(DASD) 1	DUNN	c c	DASPI	0000000	12	PUBLIC	č	APRIVILEGED BSERM		ANONE	00000	
		0175	COAVES	cyc	ř	* 2 Y 2 D ¥ C K *	00000000	12	PUPI 10	ē,	APRTVILLEURD USERA		ANNAF	00000	

N

COMPANY CONFIDENTIAL B1800/B1700 FILE SECURITY P.S. 2219 0102 (G)

Notes:

0V:

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 cisk 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 CDT execution would involve:

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

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

COMPANY CONFIDENTIAL B1800/B1700 FILE SECURITY P.S. 2219 0102 (G)

SARD READER EXECUTION

The system usercode file can be created from a card deck preserted 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.

AUIOMATIC EEAIURES

If a card file named "NEW/USER.COCES" 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", CEX 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 selfexplaratory 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 IERMINATION

SYSTEM/MAKEUSER may be normally terminated by an END or EOJ commard. (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-

COMPANY CONFIDENTIAL B1800/B1700 FILE SECURITY P.S. 2219 0102 (G)

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 RESIRICIIONS

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 cr 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.

COMPANY CONFIDENTIAL B1800/B1700 FILE SECURITY P.S. 2219 0102 (G)

ADD

Syntax: 1< ACD ----- (1*\----- US ------ <name> -----1-- = -->1 1--/1±\---- PW ---- <name> --->1 |-- = -->| I--/1\----- PACK ---->1 |-- = -->|-I--/1\----- CHG ----- <integer> -I 1-- = -->1 -/1\----- PRI----- <integer> -| 1-- = -->1 --/1\----- SL --------- <integer> -1 1-- = -->1 1--/1\---- *PRIV -----1-- *NONPRIV --1 --/1\----- PUBLIC -----I-- PRIVATE ---I ----- MAXTIME ----- <integer> ->1 -- = -->1 I---- HOSTNAME ------ <identifier> ->1 1- = ->1 1---- *ANY ----1 1---- +NONE ----1

Semantics:

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

COMPANY CONFIDENTIAL B1800/B1700 FILE SECURITY P.S. 2219 0102 (G)

attritutes 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		Ncrprivileged 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="" PFI 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 % means atl 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

COMPANY CONFIDENTIAL B1800/B1700 FILE SECURITY P.S. 2219 0102 (G)

CHANGE

Syntax:

>-- CHANGE ----- <usercode specifier> ---- TO ------->>

----- PW ----- <rame> ----->>---|-- = -->|1--/1\-- PACK ------ <name> -----|-- = -->| I--/1\-- CHG ------ <integer> -----1-- = -->1 1--/1\-- PRI ----->1 1-- = -->1 I--/1\-- SL ------ <integer> -----|-- = -->| 1--/1\-- PUBLIC -----I-- PRIVATE ---->I I-- +NONPRIV --->I ----- MAXTIME ----- <integer>->1 1 |-- = -->| ----- HOSTNANE ----- <identifier> ->1 1 11 |- = ->| |---- $\pm ANY$ ----| 1---- *NONE ----1

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:

COMPANY CONFIDENTIAL B1800/B1700 FILE SECURITY P.S. 2219 0102 (G)

Option Attribute _____ ---------PW Password PACK Pack specification CHG Charge number PRI Lisiting 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 *AXTIME=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 running.

should not be used while other programs are

2-16

BURROUGHS CORPORATION Computer Systems Group Santa Barbara Plant

COMPANY CONFIDENTIAL B1800/B1700 FILE SECURITY P.S. 2219 0102 (G)

CREAIE

Syntax:

>

1						
1-	> <input< th=""><th>file</th><th>rame></th><th></th><th>>1</th><th></th></input<>	file	rame>		>1	
1			1		· · · · · ·	
1	•		1	> DISK	>1	
1					1	

Semantics:

The CREATE command allows the user to create a new (SYSTEM)/USER-CODE file. The user is allowed to specify the input file name, which is assumed to be a card file unless the keyword DISK is presert 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 GDT 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.

2-17

BURROUGHS CORPORATION Computer systems group Santa Barbara plant

COMPANY CONFIDENTIAL B1800/B1700 FILE SECURITY P.S. 2219 0102 (G)

CEBUG

Syntax:

>	DEBUG	
e.,		> ON>
		> OFF> I

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 attritute 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

COMPANY CONFIDENTIAL B1800/B1700 FILE SECURITY P.S. 2219 0102 (G)

CELEIE

Syntax:

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

Semantics:

The CELETE 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/""

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

BURROUGHS CORPORATION COMPUTER SYSTEMS GROUP SANTA BARBARA PLANT

COMPANY CONFIDENTIAL B1800/B1700 FILE SECURITY P.S. 2219 0102 (G)

DISPLAY

Syntax:



code or usercodes are displayed. The *PRIV option allows the displaying of only privileged usercoces.

<job=number>AX DISPLAY HARRY/= *NONPFIV % Display on ODT those usercode/

<job-number>AX DISPLAY *PRIV HOST *ANY % Display only those entries

% password pairs of HARRY which % are nonprivileged.

% 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) before its normal completion then % merely enter the next command.

COMPANY CONFIDENTIAL B1800/B1700 FILE SECURITY P.S. 2219 0102 (G)

END

Syntax:

Semantics:

The END command allows the user to terminate the program.

Example:

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

2-21

BURROLGHS CORPORATION Computer systems group Santa Barbara plant

COMPANY CONFIDENTIAL B1800/B1700 FILE SECURITY P.S. 2219 0102 (G)

EQJ

Syntax:

Semantics:

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

Example:

<job=number>AX E0J % ALTERNATIVE TO "END"

COMPANY CONFIDENTIAL B1800/B1700 FILE SECURITY P.S. 2219 0102 (G)

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 opticr allows the listing of only privileged usercodes.

Examples:

<job~number>AX LIST <job=number>AX LIST JOE/JOESPASS <job-number>AX LIS JOE/= <iob-number>AX LIS JOE/"" <job=number>AX LIS #PRIV <job-number>AX LIST HOSTNAME HUB % lists only entries which are X 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". <iob-number>AX LIST HOSTNAME *NONE % List only those entries for 7 which all remote access is % invalid. <job=number>AX LIST *NONPRIV HOSTNAME USER3 % list only those entries % which are NON PRIVILEGED

COMPANY CONFIDENTIAL B1800/B1700 FILE SECURITY P.S. 2219 0102 (G)

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

COMPANY CONFIDENTIAL B1800/B1700 FILE SECURITY P.S. 2219 0102 (G)

PUNCH

Syntax:

>-- PUNCH -

| |----- <usercode specifier> ----->| | |----- *PRIV ----->|

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 PROERAM 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

--->#

COMPANY CONFIDENTIAL B1800/B1700 FILE SECURITY P.S. 2219 0102 (G)

OUIPUI ODI 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:

"LNKNOWN 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."

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

"FARAMETER 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 CISK, COMMAND IGNORED." "NO USERCOCE 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 CEFAULT."

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

COMPANY CONFIDENTIAL B1800/B1700 FILE SECURITY P.S. 2219 0102 (G)

"CHANGE TO SECURITY REQUIRES ""<usercode>/=""." "CANNOT CHANGE ALL PASSWORDS." "CANNOT SPECIFY BOTH PUBLIC AND FRIVATE." "CANNOT SPECIFY BOTH *PRIV AND *NONPRIV." "REMOTE EXECUTION DENIED." "ILLEGAL USERCODE." BURROUGHS CORPORATION COMPUTER SYSTEMS GROUP SANTA BARBARA PLANT COMPANY CONFIDENTIAL B1800/B1700 FILE SECURITY P.S. 2219 0102 (G)

CREAIING SECURE FILES

BAICH MODE

Once the system's usercode file has been established, secure files can be created by programs executed under a valid userccde/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, ore 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 % for 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 showr 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 COELL program, then it does this in the FD section by stating:

COMPANY CONFIDENTIAL B1800/B1700 FILE SECURITY P.S. 2219 0102 (G)

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 equater e.g.r

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-r

US PAYROLL/ACCT MH CHECKS SEC PUBLIC

3. SYSTEM/MAKEUSER has an option whereby all files created by a specific usercode can be made PLBLIC. 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.

CONIROL 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 (PAYRCLL)/CHECKS is a PUBLIC read-orly file, then the program Y running under the usercode/password pair FINANCE/VP can read this file but cannot write into it.

COMPANY CONFIDENTIAL B1800/B1700 FILE SECURITY P.S. 2219 0102 (G)

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

SECURITYUSE OLTPUT 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 reac/write.

2. By modification of the file header:

US	PAYROLL/ACCT	MH	CHECKS	SEC	PUBLIC	SUS	INPUT OUTPUT
			2				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

t. 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-Ιf 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 usercoce file, or create a new file called NEW/INFO. Privileged userccde/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

COMPANY CONFIDENTIAL B1800/B1700 FILE SECURITY P.S. 2219 0102 (G)

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 nonsecure file. A secure file may be created or system disk either by using a usercode/password with a ro 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 ICENTIFIERS.

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 cr system disk.

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

The ron-privileged user may access a non-secure file with a multifile-id which is not its own but cannot create a file with any cther mulfifile-id than its cwn. Thus, PROGRAM/X may read OLD/INFO but cannot create (NEW)/INFC 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 userccde's default pack. If the file naming convention is overriden 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 The only control exercised over file idenfile is not created. tifiers is in the file-name. The operating system supplies the pack-id and the multifile-id; consecuently, non-privileged users must not attempt to write and close files with file identifiers cther 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.

CEFAULI IDENIIFIERS

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.

COMPANY CONFIDENTIAL B1800/B1700 FILE SECURITY P.S. 2219 0102 (G)

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 lcck a new file without their own usercode as the sulfifile-id), this means that the file is saved on system disk or a specifiec 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 CCBOL statement above will cause the MCP to create a file named P/(PAYROLL)/CHECKS, irrespective of the default pack id.

If ir 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 defired (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 (PAYRCLL)/CHECKS. The "*" is therefore a way of overriding the default pack designation and/or default multifile-id designation.

BURROUGHS CORPORATION COMPUTER SYSTEMS GROUP SANTA BARBARA PLANT

COMPANY CONFIDENTIAL B1800/B1700 FILE SECURITY P.S. 2219 0102 (G)

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 O 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 Level can "EX CMPALL" or "COMPILE PROG WITH COBOL TO security However, a usercode with a security level of 2 cannot "EX LI". (USERB)/PROG1" unless the usercode indentifier 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

Userccdes which are designated as privileged are allowed to access or create secure files with xultifile-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.

1	Usercode	1	PRIV		Filename Accessed	1	Access	
11. 12. 13. 14.	(PAYROLL) (PAYROLL) (PAYROLL) (PAYROLL)] { { !	YES YES YES YES	1	<pre><dp>/(PAYRGLL)/A <dp>/(USERA)/A #(A)/B <pre><pre>ck=id>/A/B</pre></pre></dp></dp></pre>	1 8 1	Allowed Allowed Allowed Allowed	1
11. 12. 13. 14.	(LSERA) (USERA) (USERA) (LSERA)	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	N 0 N 0 N 0 N 0	 	<pre><dp>/(USERA)/A <dp) #(a)="" (payrcll)="" <pack="id" a="" b="">/A/B</dp)></dp></pre>	9 1 1	Allowed Denied Denied Allowed	

Table 3.1 Comparative Access Privileges

Table 3.1 presumes the following conventions:

names the default pack associated with the usercode in the $\langle dp \rangle$ 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

3-6

COMPANY CONFIDENTIAL B1800/B1700 FILE SECURITY P.S. 2219 0102 (G)

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

used to override the default rack-id and/or multifile-id designation. If the file is rot 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 YS- NON-PRIV

1	Usercode	1	PRIV	1	Filename Created	1	Approval	1
11.	(PAYROLL)	1	YES	1	<dp>/(PAYRCLL)/A</dp>	1	Allowed	1
12.	(PAYROLL)	. 1	YES	1.	<dp>/(USERA)/A</dp>	1	Allowed	. 1
13.	(PAYROLL)	ł	YES	1	*(A)/B	1	Allowed	1
14.	(PAYROLL)		YES	-1	<pack-id>///B</pack-id>	1	Allowed	
I	*****	e m '455				-	eran anno 4040 4060 4060 arras 4060 4060 4060 4060 4060 4	1
11.	(LSERA)	1	NO	1	<dp>/(USERA)/A</dp>	1	Allowed	1
12.	CUSERAD	1	NO	1 I.	<dp) (payrcll)="" a<="" td=""><td>1</td><td>Denied</td><td>. 1</td></dp)>	1	Denied	. 1
13.	(USERA)	1	NO	1	*(A)/B	1	Denied	1
14.	(USERA)	1	NO	· . •	<pack=id>///B</pack=id>	1	Denied	1

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

COMPANY CONFIDENTIAL B1800/B1700 FILE SECURITY P.S. 2219 0102 (G)

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

COMPANY CONFIDENTIAL B1800/B1700 FILE SECURITY P.S. 2219 0102 (G)

PREEIXED ODI 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, QF, RB, RE, RF

Examples:

EX	(INVEN)/A			% Invalid command
CH	(INVEN)/A	TO	X	7 Invalid command
USER	INVEN/TORY	CH	A TO *X	% Invalid command
USER	INVEN/TORY	ΕX	CINVEN)//	% Valid command
USER	INVEN/TORY	ΕX	F	% Valid command
USER	INVEN/TORY	CH	A TO X	% Valid command
USER	EL/ZAPPO	СН	(INVEN)/# to *X	X Valid command if
				2 EL/ZAPPO is a
÷				7 privileged user.

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

KA	(INVEN)/A	2	is	OK
KP	(INVEN)/A	2	is	OK
KA	(INVEN)/=	2	is	0 K

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 V US INVEN PD A

LSERCODE BACKUP FILES

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

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

.

<default pack for PAYROLL>/(PAYROLL)/%<integer>% punch

or

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

COMPANY CONFIDENTIAL B1800/B1700 FILE SECURITY P.S. 2219 0102 (G)

REMOIE 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/CCNTROLLER 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 access the secure file of another user and is not attempts to privileged to do so will be denied access to that file. The job either not scheduled or DS-ed, depending upon the state at is 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 nonsecure 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 userccdes in the (SYSTEM)/USERCODE

COMPANY CONFIDENTIAL B1800/B1700 FILE SECURITY P.S. 2219 0102 (G)

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 orcinarily does not run under a secure usercode yet supports security checking for those programs which require it to do so.

JOB SPANNING

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 lcck 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 HANCLING

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.

SYSIEM DISPLAYS

Job security inhibits certain MCP cisplays 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.
- **3MO -- modifies only the files of the particular**, active user.

BACKUP EILES

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>.

COMPANY CONFIDENTIAL B1800/B1700 FILE SECURITY P.S. 2219 0102 (G)

DISK PACK DEFAULIS

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	<pre><default pack=""></default></pre>	(UC)	A
A/8	<default pack=""></default>	· A	B
A/E ON C	С	A	В
CUCJ/A	<default pack=""></default>	(UC)	Α
CUCJ/A ON C	C	(UC)	· A
+(UC)/A	**SYSTEM DISK**	(UC)	Α.
±A	**SYSTEM DISK**	A characteristics	
*A ON C	С	• A	

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

Since remote users are usually required to sign on to applications programs through usercode/password combinations, all files saved (locked on 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 Thus, a user signed on as UC/PW under someone else's usercode. cannot save a file with the command SAVE AS *(ANOTHER)/A; the command SAVE AS *A saves a file as (LC)/A on system disk. Α commard such as SAVE AS A will put the file on disk as <default pack>/(UC)/A.

COMPANY CONFIDENTIAL B1800/B1700 FILE SECURITY P.S. 2219 0102 (G)

DEFINITIONS AND JABLES

EILE 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.PROTEC-TION. If it is zero (default), then DFH.PROTECTION is set to PUBLIC if the MULTI.FILE.ID does not cortain a USERCODE. However, if the MULTI.FILE.ID does contain a USERCODE, FPB.PRO-TECTION will be set to the security attribute of the usercode, i.e., PUBLIC or PRIVATE. If FPB.PROTECTION is not equal to zero, DFH.PFOTECTION 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. fields in the cisk file header.

These are used to set the

COMPANY CONFIDENTIAL B1800/B1700 FILE SECURITY P.S. 2219 0102 (G)

FPE-PROTECTION

BIT (2)

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

FPE-PROTECTION-10

BIT (2)

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

Two file attributes can set these FPE fields.

SEC or	DEFAULT		SUS or	I.O
SECURITYTYPE	PUBLIC		SECURITYUSE	INPUT
	PRIVATE		•	OUTPUT
	GUARD	28	A	

ACCESSZOPEN IABLE

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

8. 1

ν.		* * * * * * * * * * * * * * * *	****
		* JOB RUNNING *	* JOB RUNNING
		* WITH A *	* WITHOUT A #
		* USERCODE *	* USERCODE *
		*********	*****
****	*******	*** NEW * OLD *	* NEW * OLD
* MULII.FILE.ID	* PACK-IU	* FILE * FILE *	
************		*******	*****
*****	***********	*****	*****
2 (A) 2 🛣	* BLANK	* A * B *	* OPEN * C
+ ELANK	*******	********	*********
* 3	* _ PRESENT	* G * K *	* OPEN * C
***********	****	*********	**********
********	**********	******	****
	* BLANK	* U * I *	* U * E
* USERCUDE	* PRESENT		$+ \qquad \qquad$
*******	********	****	***
************	**********	*******	******
* ASTERISK IN	* BLANK	. * L * ¥ *	* J * N
* FIRST	*********	********	*****
* PCSITION	* PRESENT	± L ± M *	★ J ★ N
********	************	****	****
************	******************	**************************************	
- DDECENT		- r - L -	
- FNEJENI	+ PRESENT		* NPEN * C
-		- 1	

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.
 - 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.

4-3

i Ç

COMPANY CONFIDENTIAL B1800/B1700 FILE SECURITY P.S. 2219 0102 (G)

4-4

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.
 - Set the PACK.ID from the USERCODE table using the USERCODE in the MULTI-FILE.ID.
 - 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 cirectory.
 - 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 MULII.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. 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 MLLTI.PACK.ID.

2. Search the directory.

3. If the file is present proceed to Step S-

Clear the PACK.ID.
 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.

f	BURR Comp Sant	OUGH Uter A ba	S CORPORATION SYSTEMS GROUP RBARA PLANT COMPANY CONFIDENTIAL B1800/81700 FILE SECURITY P.S. 2219 0102 (G)
	× K.	1 .	Set the MULTI-FILE-ID with the usercode under which the
			program is running.
	n de la composition de la comp	2 .	Search the directory.
	N., 1	3.0	If the file is present allow the OPEN to proceed.
	i) All	4 .	Clear the MULTI.FILE.ID.
		5.	Proceed to Step C.
	Lo	1.	Remove the asterisk and shift the name left one position.
		20	If the resultant name is a USERCODE proceed to Step F.
		2.0	Allow the OPEN to proceed.
		4.	At CLOSE time proceed to Step U.
	Me	1.	Remove the asterisk and shift the name left one position.
	•	2.0	If the resultant name is a LSERCODE proceed to Step H.
5			Proceed to Step C.
	N e	1.0	Remove the asterisk and shift the name left one position.
		20	Proceed to Step C.
	0		
	U.	1.	Set the PACK-ID from the USERCODE table using the USERCODE
		9	in the MULII.FILE.ID.
		6. *	Proceed to Step W.
	D		After the ODEN
	Fo	10 9	ALLOW THE UPEN TO PROCEED.
		К. Ф	we cruse time proceed to step V.
	0_	1	Dicolar security opposite process
		2	Hand Reserve NO FILF
		4.0	Hang program no rillo
	R	1	If the APEN violator file accurity and the
		2	Allow NPEN to proceed to Step Q.
	S.	1.	If the USERCODE in the MILLY'S EVEC TO
		2.0	USERCODE under which the sprence is superior the
	•		OPEN to proceed.
		2.	Proceed to Step R.
	T.	1.	If the program is attempting to look the file into the
			directory and the MIII TT_FTIF_TD comparing a disconner and
			proceed to Step V.
		2.0	Allow the CLOSE to proceed.
1	· .		

0

Ŧ

4-5

COMPANY CONFIDENTIAL B1800/B1700 FILE SECURITY P.S. 2219 0102 (G)

- U. 1. If the MULTI-FILE.ID does not contain the USERCODE under which this program is running 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.
- N. 1. Allow the OPEN to proceed.
 2. Proceed to Step T.

BURROUGHS CORPORATION COMPUTER SYSTEMS GROUP SANTA BARBARA PLANT

COMPANY CONFIDENTIAL B1800/B1700 FILE SECURITY P.S. 2219 0102 (G)

INDEX

*NONPFIV 2-5 *PRIV 2-5

.

+ to h

ACCESS/OPEN TABLE 4-2 ACCESS: PRIV VS. NON-PRIV 3-6 ADD 2-11 APPENCED USERCODES 3-7 AUTOMATIC FEATURES 2-9

BACKUP FILES 3-11 BATCH MODE 3-1

CARD READER EXECUTION 2-9 CHANGE 2-13 2-5 CHG COMMAND RESTRICTIONS 2-10 COMMANDS 2-9 CONSOLE KEYBOARD EXECUTION 2-8 CONTROL OF I/O 3-2 CONVERSION TO SECURE FILES 3-3 COPY 2-15 CREATE 2-16 CREATING SECURE FILES 3-1

DEBUG 2-17 DEFALLI IDENTIFIERS 3-4 DEFINITION OF TERMS 2-2 DEFINITIONS AND TABLES 4-1 DELETE 2-18 DISK PACK DEFAULTS 3-12 DISPLAY 2-19

END 2-20 EOJ 2-21

FILE HANDLING 3-11 FILE SECURITY 1-1 FILE SECURITY IMPLEMENTATION 4-1

INFORMATIONAL MESSAGES 2-9 INTROCUCTION 1-1

JOB SPAWNING 3-11

LINE PRINTER OUTPUT 2-6 LIST 2-22 LOCK: PRIV VS. NON-PRIV 3-7

a - 1

2 B

COMPANY CONFIDENTIAL B1800/B1700 FILE SECURITY P.S. 2219 0102 (G)

LOG-ON/SIGN-ON 3-10

OUTPUT ODT ERROR MESSAGES 2-25

PACK 2-5 PREFIXED ODT COMMANDS 3-9 PRI 2-5 PRIVATE 2-5 PROGRAM EXECUTION 2-8 PROGRAM TERMINATION 2-9 PUBLIC 2-5 PUBLIC FILES 3-2 PUNCH 2-24 PW 2-5

READ-ONLY FILES 3-3 RELATED DOCUMENTATION 1-2 REMOTE MODE 3-10 RESTRICTIONS 2-6

SECURE FILE IDENTIFIERS 1-1 SECURITY LEVELS 3-6 SYNTAX DIAGRAM CONVENTIONS 2-1 SYSTEM DISPLAYS 3-11 SYSTEM/MAKEUSER 2-1

US 2-5 USERCODE ATTRIBUTES 2-4 USERCODE BACKUP FILES 3-9

DISTRIBUTION LIST

B1800/B1700 SOFTWARE PRODUCT SPECIFICATIONS

DEIROII

- S. M. Roberson Prod. Mgmt. P. Gonzales - Prod. Ngmt. 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)

SANTA BARBARA PLANT

S. C. Schmidt J. Hale R. Shobe K. Meyers A. van der Linden T. Cardona R. Bauerle 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)

- J. Henige
- E. Yardi
- D. Stover
- L. Sweeney 2
- G. Hammond 3
- J. Morrison 6

Distribution list current as of 01/21/81