CA-Top Secret®

Control Options Guide
Release 3.0
VSE

SP1

Second Edition, September 2000

Contents

About This Guide

Purpose

The *Control Options Guide* guide provides detailed instructions on how to use CA-Top Secret control options to control the CA-Top Secret security environment.

This guide provides you with detailed information about each control option and can be used as a quick reference aid.

Read and be familiar with the *User Guide* before using this guide.

Organization

Chapter	Description
1	Defines the purpose of control options, provides examples of the various methods used to enter the options, and explains how the options are processed by CA-Top Secret. Notation conventions used within this guide are also presented.
2	Provides a description of all Control Options. The description includes: format, default values, entry methods, and applicable operands. The General Information section explains how the option affects CA-Top Secret and how the option interacts with other Control Options or with other products that may be installed at the site. If required, this information is followed by one or more examples of how the option should be used.
Index	Provides an efficient way to locate specific material.

CA-Top Secret Publications

The following publications are supplied with CA-Top Secret:

Title	Contents
Installation Guide	CA-Top Secret installation for VSE, including: installation and maintenance steps, startup and shutdown considerations, backup and recovery procedures, and Security File conversion.
Command Functions Guide	Comprehensive reference to the TSS command and CA-Top Secret resources.
Control Options Guide	Comprehensive reference of CA-Top Secret control options.
Implementation: BATCH, STC and APPC Guide	Provides for setting up security in Batch, STC and APPC environments.
Implementation: CICS Guide	Provides for setting up security in a CICS environment.
Messages and Codes Guide	Provides all CA-Top Secret messages and codes.
Planning Guide	General guide for planning a successful CA-Top Secret security implementation and describing the latest enhancements to CA-Top Secret.
Report and Tracking Guide	Details the use of TSSUTIL, TSSTRACK, TSSAUDIT, TSSCFILE and TSSCPR and provides sample reports.
Troubleshooting Guide	Includes CA-Top Secret debugging options and facilities, information to be prepared prior to contacting Technical Support, and an explanation of customer support.
User Guide	Conceptual overview of CA-Top Secret architecture and capablilities. Also includes implementation instructions that span all facilities, including: implementation how to's, customization, and the CA-Top Secret utilities.

All guides are updated as required. Instructions accompany each update package.

Related Publications

The common component services formerly known as CA90s have been enhanced and renamed CA Common Infrastructure Services, CA-CIS. All the documentation for the services exists in the following publications supplied by Computer Associates:

Name	Contents
CA-CIS Administrator Guide	A guide for system administrators.
CA-CIS CAICCI User Guide	Describes how to use the communication protocols needed for cross-system communication.
CA-CIS Installation Guide	Tells how to install the CA-CIS.
CA-CIS Message Guide	Lists messages and codes for CA-CIS.
CA-CIS Reference Guide	Describes how to access and use the VSE common components.
CA-CIS Systems Programmer Guide	Details the programming requirements for command, security, and signon exits.

The following publications relate to CA-Top Secret and are available from Computer Associates:

Title	Operating System
CA-EARL Reference Guide	MVS/VM/VSE
CA-EARL User Guide	MVS/VM/VSE
CA-EARL Systems Programmer Guide	VSE
CA-EARL Examples Guide	MVS/VM/VSE

Command Notation

Enter the following exactly as they appear in command descriptions:

UPPERCASE	identifies commands, keywords, and keyword values which must be coded exactly as shown.
MIXEDcase	identifies acceptable command abbreviations. The UPPER-CASE letters represent the minimum abbreviation possible. The lowercase letters of the command may be entered for further clarification **Note:** In some cases, the command processor may require a more detailed abbreviation due to user-defined resource being the same as a command abbreviation. In these cases, either enter the complete command or code a national or numeric character in one of the first four positions of the user-defined resource.
underlining	identifies default operands. These operands do not need to be entered to take effect.
Symbols	"" / * # () , must be coded exactly as shown.

The following items clarify command syntax; do not type when they appear:

lowercase	indicates keyword values which you must supply.
[ ]	identifies optional keywords.
|	separates alternative keywords or values; choose one.
{ }	indicates that you must enter one of the keywords.
...	means the preceding value may be repeated more than once.

The following table indicates the appropriate command format.

Sample Command	Explanation
TSS PER(acid) DSN(dsname)	You must supply a value for the ACID and for the data set name.
MODE(DORM|IMPL|WARN|FAIL)	You must choose **only** one of the keywords.
TSS {ADDto } (acid) MCSAUTH {(INFO) } {REMove } {(MASTER)} {REPlace} {(SYS) } {(IO) } {(CONS) } {(ALL) }	You must select a command function, enter the name of an ACID, enter the MCSAUTH keyword, and select an operand from the list.

Chapter 1. Introduction

The overview defines the purpose of control options, and explains the various entry methods used to enable them. Security administrators without CA-Top Secret experience should read this overview before entering control options.

1.1 CA-Top Secret Control Options

Control options allow selected operators and security administrators to specify how CA-Top Secret will control security. In other words, the security administrator can use control options to perform several useful activities:

- Reset the security MODE. FAIL is the delivered default.
- Determine how CA-Top Secret will process normally and how it will process under specific security MODES and circumstances.
- Indicate what features, facilities, or products, are on the operating system, and how individual facilities will be handled by CA-Top Secret.
- Suspend suspicious users.
- Specify password selection rules and violation thresholds.
- Issue commands that force CA-Top Secret to reset after shutdown or reinitialize after installation of new CA-Top Secret maintenance.

1.2 Option Selection and Change

CA-Top Secret provides two methods for selecting and changing control options:

1. TSS MODIFY Command Function.
2. Parameter File at startup of CA-Top Secret

Each of these entry methods will be described in detail throughout the remainder of this chapter.

1.3 Entry Methods

The following table shows each of the three entry methods and an example of their use.

Table 1-1. Control Option Entry Methods

Entry Method:	When Used:	Example:
TSS MODIFY Command	To add or change options from online terminal	`TSS MODIFY('TAPE(OFF)')`

Parameter File	To specify a set of control options at startup of CA-Top Secret.	`*`
		`* control options`
		`*`
		`MODE(WARN)`
		`FAC(TSO=MODE=IMPL,LOG=(ALL)`
		`BACKUP(0400)`
		`NEWPW(MIN=5,MASK=CVCVC)`

TSS MODIFY Command	To add or change options from console reply	`reply id TAPE(OFF)`

1.3.1 Changing Options with TSS MODIFY Command

Control options may be entered via the TSS MODIFY command function. The administrator attempting to issue the command must have previously been granted CONSOLE authority. The format for entering control options with TSS MODIFY is:

Format

```
TSS MODIFY(control option[(suboption-list)])
```

If the administrator uses the FACILITY control option with the TSS MODIFY command, the following formats apply:

Examples

```
TSS MODIFY(FACILITY(BATCH=MODE=WARN))
TSS MODIFY(FACILITY(IMSPROD=DEFACID(X)))
TSS MODIFY SECTRACE(ACT,WTO)
TSS MODIFY STATUS
```

Refer to the TSS MODIFY command in the *Command Functions Guide* for detailed information.

1.3.2 Specifying Options in the Parameter File

The *Control Options Guide* lists control options and their default settings. An SCA may elect to change any default setting in order to tailor security for his environment during the security implementation phase.

The default for the MODE option is FAIL. Most security administrators will want to change this setting during the implementation phase.

1.3.2.1 Creating the Parameter File

During the installation of CA-Top Secret, a systems programmer creates a Parameter File that contains an initial set of control options selected by the MSCA.

The Parameter File is a standard sequential data set that may contain any number of records. Control options may be entered into the file without commas or separators. Titles and comment statements that describe the entries may also be entered. An asterisk is used to delimit a title or comment statement (see the following figure). The Parameter File entries should begin in column one.

```
*          SECURITY CONTROL OPTIONS FOR TEST MACHINE

MODE(WARN)                          * SELECT PROCESSING MODE
FAC(BATCH=MODE=IMPL,LOG=(ALL))      * BATCH IS DIFFERENT
BACKUP(0400)                        * 4 IN MORNING, PERFORM BACKUP
NEWPW(MIN=5,MASK=CVCVCV)            * NEW PASSWORD MASKING
```

Figure 1-1. Parameter File with Comment Asterisks

Control options such as FACILITY may contain a string of suboptions and values that will not fit on a single command line. The same option may be separated and entered as several options.

Example

```
FAC(TSO=MODE=IMPL,LOG=(ALL)) * BATCH DIFFERENCES
FAC(TSO=LOCKTIME=5)
FAC(BATCH=NOLUMSG,RNDPW)
```

1.3.2.2 Parameter File Becomes the Baseline

Once entered into the Parameter File, the initial options become a base or foundation. Although these options may be overridden, CA-Top Secret will revert to the options listed in the Parameter File when CA-Top Secret is restarted after a shutdown.

1.3.2.3 Sequential Processing

CA-Top Secret sequentially processes most of the control options in the Parameter File. Global entries must be entered before facility-specific entries to ensure that the facility-specific entries will take effect.

As an example, suppose CA-Top Secret was set in WARN mode with the entry shown on line **1**. Then, by entering the FAC option shown in **2**, you set BATCH to process in IMPL mode.

```
    *     SECURITY CONTROL OPTIONS FOR TEST MACHINE

1     MODE(WARN)                      * SELECT PROCESSING MODE
2   FAC(BATCH=MODE=IMPL,LOG=(ALL)) * BATCH IS DIFFERENT
    BACKUP(0400)                    * 4 IN MORNING
    NEWPW(MIN=5,MASK=CVCVCV)        * NEW PASSWORD MASKING
```

Figure 1-2. Sequential Processing Of Options.

If the FACILITY control option was specified before the MODE option, CA-Top Secret would process all requests under the WARN MODE, regardless of the facility from which the request was entered.

1.3.2.4 Altering Facility Names

If the name of a facility is changed via the NAME suboption of the FACILITY control option:

```
FAC(USER4=NAME=CICSA)
```

then all subsequent control option entries that will impact the newly named facility (CICSA) must contain the new facility name.

Correct Entry

To change name of USER4 to CICSA and force CICSA to process in the WARN mode, enter:

```
FAC(USER4=NAME=CICSA)
FAC(CICSA=MODE=WARN)
```

Incorrect Entry

The following entry will NOT affect the mode of the newly named facility:

```
FAC(USER4=NAME=CICSUSER)
FAC(USER4=MODE=WARN)
```

Control option changes made before a facility is renamed will remain in effect for the newly named facility.

Example

Given the entries:

```
FAC(USER4=MODE=WARN)
FAC(USER4=NOABEND)
FAC(USER4=NAME=CICSA)
```

the CICSA facility will process security in WARN mode and will have the NOABEND attribute. Of course any additional changes must be made to CICSA, not USER4.

1.4 Rules and Procedures

1.4.1 Authority to Enter Options

CA-Top Secret protects the most powerful control options against unauthorized entry and change. When a restricted option is changed or specified at the O/S console, CA-Top Secret will display message TSS9080A, which prompts the user for one of the following authorizations before allowing the change to take effect.

The person entering the option must either:

- Enter the MSCA's PREVIOUS password, or
- Enter an ACID that contains the CONSOLE attribute followed by the ACID's password in the format ACID/password.

This allows for emergency changes without compromising the MSCA's current password.

1.4.2 Restricted and Unrestricted Options

Any control option that **changes** the security environment is restricted. Most control options are restricted unless they only request CA-Top Secret status displays. These "unrestricted" control options are as follows:

DRC(nnn)
FACILITY(fac)
MSG(nnnn)
RPW(LIST)
ST
STATS
STATUS
VERSION

Note: If the option is entered via the TSS MODIFY command function, the ACID must have been granted CONSOLE authority.

1.4.3 Accountability for Entries

Only an MSCA or SCA should be allowed to select and change control options. Sometimes though, the MSCA may elect to allow an operations supervisor, or a divisional or departmental security administrator, to enter control options.

The authorized ACID/password combination will allow operations supervisors or CA-Top Secret administrators to specify control options, but it will also leave an audit trail that leads directly to the ACID under which the specification was made.

Rules for Use

Three basic rules must be followed to allow operators or administrators to enter control options and be held accountable for their entries.

1. ACID must be valid, and must have the CONSOLE attribute attached to it.
2. ACID cannot be expired or suspended at the time that the control option entry is made.
3. The PASSWORD must be correct and unexpired.

1.4.4 Hierarchy of Entry Methods

Control options such as MODE and LOG can be specified globally, by facility, or in the case of the MODE option, by user or profile. This fact, along with the flexibility of being able to specify options using different entry methods at different times, could result in confusion over which options are actually controlling security at the installation. This confusion might be eliminated by considering the following points.

- Options entered via the TSS MODIFY command will override similar options entered via any of the aforementioned entry methods, but are not retained.
- TSS commands that specify settings for a specific user will override any similar control option for that user.

Chapter 2. Specific Control Options

2.1 Control Options Summary

Option	Description
ADMINBY	controls the auditing of permits and facilities added to a user.
AUDIT(SWITCH)	forces an immediate switch to the top of the ATF or to the alternate ATF
AUTH	controls authorization checking
BACKUP	controls automatic Security File backup
BYPASS	specifies jobs and STCs that bypass security in an emergency
CACHE	specifies amount of virtual storage within the CA-Top Secret address space to be used for caching.
CANCEL	allows CA-Top Secret to be cancelled via the O/S CANCEL command
CMDNUM	determines the number of command processors initiated at startup of the CA-Top Secret address space.
CPF	controls startup of Command Propagation Facility
CPFNODES	identifies remote nodes to which TSS commands can be transmitted
CPFRCVUND	identifies whether or not the local node can receive commands transmitted from remote nodes that have not be defined to the CPFNODES list.
CPFTARGET	controls default for TSS command TARGET keyword
CPFWAIT	controls default for TSS command WAIT keyword
DATE	sets date display format
DEBUG	controls debuging feature use as directed by CA support
DIAGTRAP	controls diagnostic traps use as directed by CA support
DOWN	controls action taken when CA-Top Secret address space is inactive
DRC	modifies or lists particular DRC attributes
DUFPGM	identifies programs allowing for extraction or update of INSTDATA
DUMP	takes formatted dumps of CA-Top Secret address space
EXIT	controls installation exit (TSSINSTX)
EXPDAYS	Displays commands beyond the expiration date

FACILITY	controls facility processing
HPBPW	honors previous batch password
IBMCUST	specifies IBM customer #
IBMPASS	specifies IBM product license key
INACTIVE	controls users that have been inactive for a specified period
INSTDATA	alters global installation data field
IOTRACE	controls CA-Top Secret I/O trace
JOBACID	controls ACID identification for batch jobs
LIBRPROT	identifies access level for VSE library protection, and enables and disables VSE system library member level protection
LMPCHECK	verifies that a LMP encryption key is being used
LOG	controls incident recording for all facilities
LOGBUF	allows for the maximum number of in-core logging buffers to be used
MODE	controls processing mode for all facilities
MSG	alters characteristics of CA-Top Secret violation messages
MSUSPEND	allows MSCA to be suspended if password violation occurs
NEWPW	selects new password specification rules
NJEUSR	defines a default ACID to be used in the Store-and-Forward nodes
NPWRTHRESH	sets maximum threshold, from 0 to 99, for new passwords to be verified before complete logon sequence needs restarting
OPTIONS	replaces several optional apars
PTHRESH	specifies password violation threshold
PWEXP	specifies password expiration interval
PWHIST	specifies number of previous passwords to be maintained in history file
PWRNODE	indicates the name that the local node is known as by POWER
PWVIEW	controls display of passwords by administrators
RECOVER	controls change recovery
REFRESH	requests CA-SAF module reinitialization after maintenance
REINIT	requests module reinitialization after maintenance
RESETEOD	resets an "end-of day" shutdown condition
RESETSTATS	resets all statistics

RPW	modifies and lists contents of restricted password list
SDTTABLE	Reloads SDT record types into storage as a refresh
SECTRACE	controls security diagnostic trace
SHRFILE	specifies whether CA-Top Secret files will be shared
ST	generates combined STATS, STATUS, and VERSION display
STATS	generates CA-Top Secret statistics display
STATUS	generates CA-Top Secret status display
SUBACID	controls online job submission
SUSPEND	suspends an acid
SVCDUMP	produces a system dump of the CA-Top Secret system.
SYNCH	synchronizes global resource authorization tables
TAPE	controls tape processing
TEMPDS	controls temporary dataset protection
TEXTTSS	identifies up to 19 characters to replace the string 'CA-Top Secret SECURITY' in messages and reports
TIMER	selects timer control interval
TSS	allows use of TSS command at the VSE console
VERSION	displays CA-Top Secret version and maintenance level
VTHRESH	selects violation threshold and action

2.1.1 Control Option Default Values

Option	Default
AUTH	AUTH(OVERRIDE,ALLOVER)
BACKUP	BACKUP(0100)
CACHE	CACHE(OFF)
CPF	CPF(INACTIVE)
CPFRCVUND	CPFRCVUND(NO)
CPFTARGET	CPFTARGET(LOCAL)
CPFWAIT	CPFWAIT(YES)
DATE	DATE(MM/DD/YY)
DEBUG	DEBUG(OFF)
DIAGTRAP	DIAGTRAP(OFF)
DOWN	DOWN(BW,SB,TW,OW)
EXIT	EXIT(OFF)
HPBPW	HPBPW(0)
INACTIVE	INACTIVE(0)
INSTDATA	INSTDATA(0)
JOBACID	JOBACID(A,1,0)
LOG	LOG(MSG,SMF,INIT,SEC9)
LOGBUF	LOGBUF(32)
MODE	MODE(FAIL)
MSUSPEND	MSUSPEND(NO)
NEWPW	NEWPW(MIN=4,WARN=3,ID,RS,NR=0,TS,MINDAYS=1)
NJEUSR	N/A
NPWRTHRESH	NPWRTHRESH(2)
OPTIONS	N/A
PTHRESH	PTHRESH(4)
PWEXP	PWEXP(30)
PWHIST	PWHIST(3)
PWVIEW	PWVIEW(NO)
RECOVER	RECOVER(ON) if RECFILE DD statement is in CA-Top Secret started task procedure

SECTRACE	SECTRACE(OFF)
SHRFILE	SHRFILE(YES)
SUBACID	SUBACID(U,7)
TAPE	TAPE(OFF)
TEMPDS	TEMPDS(NO)
TEXTTSS	TEXTTSS(CA-TOP SECRET SECURITY)
TIMER	TIMER(15)
VTHRESH	VTHRESH(05,NOT)

2.2 ADMINBY

ADMINBY is used to enable the auditing of permits and facilities added to a user within the Security File. If this control option is used, then all new ADD( ) FACILITY( ) PERMIT( ) resource( ) to user ACIDs will have recorded the name of the administrator, the SYSID of the system on which they issued the command, and the date/time the command was issued. then

Format:	**Default:**	**Entry Method:**
ADMINBY	N/A	All

General Information This information is only maintained and listed if the ADMINBY control option is turned off. The information already on the system is no longer displayed, and no new information is maintained.

2.3 AUDIT(SWITCH)

The AUDIT(SWITCH) option allows the CA-Top Secret administrator to force a switch to the alternate Audit Tracking File if multiple files are being used. If only one ATF is being used it forces a wrap to the top of the file.

Format:	Default:	Entry Method:
AUDIT(SWITCH)	N/A	TSS MODIFY

2.3.1 General Information

The 256 byte Audit/Tracking File cannot be shared with pre-5.0 CA-Top Secret systems. If you wish to share Audit/Tracking Files between pre-5.0 and 5.0 systems you must use the 44 byte Audit/Tracking File format.

2.3.2 Examples

To wrap to the top of the alternate ATF when the primary ATF is full, the CA-Top Secret administrator enters:

```
TSS MODIFY AUDIT(SWITCH)
```

2.4 AUTH

AUTH indicates whether CA-Top Secret will merge the User, Profile, and ALL records for its access authorization search, or whether CA-Top Secret will search each record separately.

Format:	Default:	Entry Method:
AUTH(OVERRIDE[,ALLOVER])	OVERRIDE,ALLOVER	All
AUTH(MERGE[,ALLOVER|ALLMERGE])		

Operands **Description**

OVERRIDE Indicates that the User, Profile, and All records will be searched separately in the following manner:

User Record: CA-Top Secret will search an ACID's user record for the authorization to access a resource. If CA-Top Secret locates this authorization, it will continue its search of the entire user record, and grant access to the resource. If the system finds another authorization for the same resource, it will grant or deny access based on the PERMIT containing the resource prefix which most explicitly matches the resource being requested. Once this authorization is found in a user record, CA-Top Secret will not check profile records.

Profile Record: If the system cannot locate the authorization in the user record, it will search each profile in sequence. Again, CA-Top Secret will search the entire profile record. Once an authorization record is found in a profile, subsequent profiles are not searched. If more than one authorization is found for the same resource, it will grant or deny access using the PERMIT containing the resource prefix which most explicitly matches the resource being requested.

Note: OVERRIDE is mutually exclusive with MERGE and ALLMERGE. Also, OVERRIDE implies ALLOVER.

MERGE CA-Top Secret merges user and profile records, and searches this merged record for the requested authorization. The system will not make an access decision until it has searched the entire merged record.

ALLOVER Indicates that the ALL record should be searched if no authorization is found in the user or profile records.

Note: ALLOVER is mutually exclusive with ALLMERGE.

ALLMERGE
Indicates that the ALL record will be merged with user and profile records. ALLMERGE implies MERGE.

2.4.1 General Information

Authorization Algorithm

CA-Top Secret uses an Authorization Algorithm to determine whether or not to grant access to a resource. This algorithm is described in the *User Guide.*

2.5 BACKUP

BACKUP allows security administrators to:

- immediately back up the Security File
- select a time for an automatic daily backup
- deactivate the automatic backup.

Format:	Default:	Entry Method:
BACKUP	N/A	All
BACKUP(hhmm)	BACKUP(0100)	All
BACKUP(OFF)	N/A	All

Note: The MODIFY command will not override the entry in the Parameter File if BACKUP is set to OFF. Also, this option will only work if the Backup DD card is included in the start JCL. Refer to the *Installation Guide* for further information.

2.5.1 Operands

If You Enter:	And:	Then:
BACKUP	Backup DD statement is in the CA-Top Secret STC procedure	CA-Top Secret will immediately backup the Security File
BACKUP(hhmm)	Backup DD statement is in the CA-Top Secret STC procedure	CA-Top Secret will backup the the Security File at time specified
BACKUP(OFF)	N/A	CA-Top Secret will discontinue automatic backup of Security File. CA-Top Secret must be restarted to reset BACKUP(OFF).

2.5.2 General Information

Use Of BACKUP Option

Use of the BACKUP option is contingent on two factors:

1. BACKUP is available only if the CAIBKUP DLBL statement is entered into the CA-Top Secret startup procedure. Refer to the *Installation* guide for details.
2. The Backup File must be the exact size of the Security File. See your *Installation* guide for details.

When CA-Top Secret Won't Perform BACKUP

CA-Top Secret will not back up the Security File on the same day that CA-Top Secret is started, unless it is started BEFORE any scheduled backup time.

Multiple CPUs

It is only necessary to perform backup from one CPU in a multiple CPU environment. The site need only activate backup through one CPU's CA-Top Secret Parameter File or STC procedure. Multiple backups are redundant, and will not occur at the same time due to device locking.

Daily Procedures

The *Computer Operations* guide in the Appendix of *User Guide* contains daily backup and recovery procedures.

Recommended Use

Security administrators should use the automatic backup feature to protect the Security File. To use the backup feature, the security administrator or programmer must first create a backup file on an alternate DASD volume. This Backup File should be placed on a different string with a different control unit than the primary file. This will ensure that the Backup File will be available in the event of a hardware failure. This Backup File is a copy of the Security File, and as such it must be considered a sensitive, high-risk data set. The *Installation* guide contains the procedure for creating the Backup File.

2.5.3 Examples

To automatically back up the Security File for 2 am, enter the following in the Parameter File:

```
BACKUP(0200)
```

To immediately back up the File, enter:

```
TSS MODIFY BACKUP
```

2.6 BYPASS

BYPASS allows the MSCA to request emergency security bypass for a specific job or ACID. Whenever security is BYPASSed, CA-Top Secret writes an audit record and sends messages to the console indicating that security is being totally or selectively bypassed.

Format:	Default:	Entry Method:	Restrictions:
BYPASS(jobname) BYPASS(EVERYJOB)	N/A	Modify Commands	Requires Authorization
BYPASS(RESET)	N/A	Modify commands (see note below)	No Authorization

Operands Description

jobname Enter the name of the batch job, started-task procedure, or the ACID identifying the online session (or job), which will bypass security.

RESET Terminates security bypass for all jobnames or acidnames that were specified to bypass security.

EVERYJOB
Allows ALL jobs and online sessions to bypass security. USE WITH EXTREME CAUTION.

Note: To RESET security bypass for one specific job, you can use both O/S and TSS MODIFY commands. If BYPASS(EVERYJOB) is specified to RESET security bypass for all jobs and online sessions, only the modify command is valid.

2.6.1 General Information

Rules For Use:

- BYPASS takes effect in all modes.
- Only one jobname or ACID may be specified per option.
- Up to ten BYPASS options may be specified.
- TSS MODIFY may be used to bypass security for every job run. However, a TSS MODIFY - BYPASS(RESET) must be issued from the console to rescind the option. If a TSS MODIFY (BYPASS(RESET)) is attempted, the following message will result:

```
TSS0201E TOP SECRET IS NOT ACTIVE
```

- Any jobname or ACID with the BYPASS option specified can not use CA-Top Secret administrative features (such as the TSS PERMIT command) because password checking is bypassed.

2.6.2 Examples

The entry:

```
TSS MODIFY BYPASS(PAYRUN)
```

causes any job called PAYRUN, or any job run under the ACID 'PAYRUN', to bypass all security checking.

The entry:

```
TSS MODIFY BYPASS(RESET)
```

terminates security bypass for 'PAYRUN', and any other ACID or jobname that was specified to bypass security.

2.7 CACHE

CACHE allows CA-Top Secret to reduce I/O operations toward the Security File which improves the performance of CA-Top Secret and the system as a whole.

Format:	Default:	Entry Method:
CACHE (nnnn|CLEAR|STATUS|OFF)	CACHE(OFF)	ALL

Operands Description

nnnn Changes the threshold size of the amount of storage to be used by CACHE. **nnnn** is the maximum number of kilobytes that CA-Top Secret may use. A threshold size of 2000K is recommended as a starting point, if CACHE clears too often you may wish to increase the threshold size. You may specify any amount for CACHE but CA-Top Secret will limit the amount that is actually used to the size of the CA-Top Secret region minus a buffer needed to avoid storage constraints.

If CACHE was inactive, this command activates CACHE.

CLEAR Empties the CACHE. The CACHE will start to fill again as security records are requested by applications. Clear is also automatically performed when a CACHE request is issued that would cause the CURRENT SIZE to exceed the MAXSIZE.

STATUS Provides statistics on how much CACHE is used and how efficient CACHE is in avoiding extra I/O. If CACHE is not active, the following message is displayed:

```
TSS1303I CACHE IS OFF
```

If CACHE is active, the following statistics will be displayed:

```
TSS1304I ------ CACHE STATISTICS -----
TSS1305I MAXSIZE ( nnnnnnnnnK ) SIZE ( nnnnnnnnnK )
TSS1306I CALLS ( nnnnnnnnn ) SATISFIED ( nnnnnnnnn )
TSS1307I CLEARED ( nnnnnnnnn )
```

Where:

MAXSIZE Maximum number of kilobytes used by CACHE as the storage threshold.

SIZE Current number of kilobytes used.

CALLS Number of calls made to CACHE

SATISFIED Number of calls satisfied in CACHE

CLEARED How many times CACHE was clear for the life of this CA-Top Secret address space.

OFF Deactivates CACHE. The CACHE is emptied and will not be used until requested by a CACHE(nnnn) command.

2.7.1 General Information

CA-Top Secret uses virtual storage above the line within its address space as a method to keep commonly used records from the Security File.

As a default, CA-Top Secret comes with the CACHE option off, the TSS MODIFY control option must be used to activate CACHE.

The CACHE provides benefits in two areas. The first is that users commonly signon multiple times in a short duration of time. In some cases this is due to the logon mechanism as in TSO, or logon to multiple regions such as CICS. Secondly, the CACHE benefits profile sharing in allowing I/O performed on behalf of one user to benefit another user logging onto a different address space.

2.8 CANCEL

CANCEL allows security administrators to use the CANCEL command to bring the CA-Top Secret address space down. After specifying CANCEL, the CA-Top Secret address space will be eligible for cancellation.

Refer to the DOWN control option for a description of the various DOWN options that will take effect when the CA-Top Secret address space is deactivated.

Format:	**Default:**	**Entry Method:**
CANCEL	N/A	All

2.8.1 General Information

CANCEL should be used in emergency situations only. This option is not recommended as the normal shutdown method for CA-Top Secret. Use TSS SHUTDOWN as described under the heading, "Stopping the CA-Top Secret Started Task" in the "Overview."

If the VSE FLUSH Command is used, CA-Top Secret:

- cannot process the DOWN options
- must be restarted or IPLed to proceed
- will process in a very unpredictable manner.

2.9 CMDNUM

CMDNUM determines the number of command processors initiated at startup of the CA-Top Secret address space.

Format:	Default:	Entry Method:
CMDNUM(n)	2	Parameter File

Operands Description

n Specifies the number (from 2 to 10) of command procesors that CA-Top Secret initiates at startup.

2.9.1 Examples

The entry:

```
CMDNUM(5)
```

indicates that five command processors are initiated at startup.

2.9.2 General Information

The following messages, below, are displayed during a TSS MODIFY STATUS command. Only the number of processors started are shown.

```
TSS9610I  == Command Processor Workload Balance ==
TSS9611I  Total Commands Processed = 00000000
TSS9612I  CMD  01 = 000.00%          CMD  02 = 000.00%
TSS9612I  CMD  03 = 000.00%          CMD  04 = 000.00%
TSS9612I  CMD  05 = 000.00%          CMD  06 = 000.00%
TSS9612I  CMD  07 = 000.00%          CMD  08 = 000.00%
TSS9612I  CMD  09 = 000.00%          CMD  10 = 000.00%
Is there is an odd number of processors then the message becomes
TSS9613I  CMD  09 = 000.00%
```

Note: Although the minimum number of command processors is two, with the NT workstation and the higher number of commands being issued, there is a need for starting more processors.

2.10 CPF

CPF(ON|OFF|KILL) specifies whether the Command Propagation Facility (CPF) of CA-Top Secret will be activated at startup.

At least one of the CPF-related control options **must** be entered at CA-Top Secret startup to use the Command Propagation Facility. If not, CPF may not be activated until the next CA-Top Secret startup and no CPF control options are honored by CA-Top Secret until that time.

Format:	Default:	Entry Method:
CPF(ON|OFF|KILL)	CPF(INACTIVE)	All

Operands Description

ON Specifies that CPF support modules are loaded by CA-Top Secret into memory and command routing can commence as soon as CA-Top Secret startup is activated.

OFF Specifies that no TSS commands are transmitted by this node or received from other nodes until the operator sets CPF(ON) with the TSS MODIFY command (if any CPF-related control option was entered), or at the next startup of CA-Top Secret.

For example, an entry of

```
CPF(OFF)
```

indicates that a user does not wish to use the Command Propagation Facility.

Refer to the *User Guide* for further information on the use of this option.

KILL Terminates the CPF subtask and produces a dump. Once the subtask has been KILLed, it can later be reactivated using TSS MODIFY(CPF(ON)).

INACTIVE
Is an indicator that CPF has not been turned on.

2.11 CPFNODES

CPFNODES identifies remote CA-Top Secret nodes (one- to eight-characters) from and/or to which CPF can propagate commands.

Note: The word **node** when used in reference to the Command Propagation Facility, refers to the **unique identifier** that is assigned to a node when it is defined using CAICCI. For more information on defining a node, refer to the *CA-CIS Reference Guide*.

Format:	Default:	Entry Method:
CPFNODES(nodename1[(S|R)],...)	N/A	PARM File or Startup Parms

Operands Description

nodename Specifies remote CA-Top Secret nodes from and/or to which TSS commands will be transmitted. For example, an entry of:

```
CPFNODES(A1B2C3,D4E5F6)
```

identifies nodes A1B2C3 and D4E5F6 as potential targets of TSS commands.

(S) Specifies that the local node can only **send** commands to that particular remote node. For example, an entry of:

```
CPFNODES(CHI,NYC,PHIL(S))
```

indicates that the local node can send and receive commands from the CHI and NYC nodes, however, it can only send commands to the PHIL node.

(R) Specifies that the local node can only **receive** commands from that particular remote node. For example, an entry of:

```
CPFNODES(LA,NJ,NY(R))
```

indicates that the local node can send and receive commands from the LA and NJ nodes, however, it can only receive commands from the NY node.

Note: User password changes automatically propagate to all nodes designated by the CPFNODES option.

2.12 CPFRCVUND

CPFRCVUND indicates whether or not the local node can receive commands propagated from nodes which have not been defined to the CPFNODES list.

Format:	Default:	Entry Method:
CPFRCVUND(YES|NO)	NO	ALL

Operands Description

YES Indicates that CPFRCVUND is in effect. The local node will receive commands from defined as well as undefined remote nodes.

NO Indicates that CPFRCVUND is not in effect. Therefore, the local node will not accept commands transmitted from remote nodes that are not listed in the CPFNODES list. This is the default.

2.13 CPFTARGET

CPFTARGET(LOCAL|AUTO|*) sets a default value for the TSS command TARGET keyword.

At least one of the CPF-related control options **must** be entered at CA-Top Secret startup to use the Command Propagation Facility. If not, CPF may not be activated until the next CA-Top Secret startup and no CPF control options are accepted by CA-Top Secret until that time.

Format:	**Default:**	**Entry Method:**
CPFTARGET(LOCAL|AUTO|*)	CPFTARGET(LOCAL)	PARM File or Startup Parms

Operands **Description**

LOCAL Specifies that the default for the TARGET keyword will be to restrict command execution to the local node only.

AUTO Indicates default routing based upon the DEFNODES associated with the ACID. The user's default nodes are assigned implicitly on a TSS CREATE function or manually using the TSS ADD function. For more information on DEFNODES, refer to the *CA-Top Secret Command Functions Guide.*

***** Specifies that the default for the TARGET keyword will be to transmit the command to all nodes defined in the CPFNODES control option with the exception of those indicated as receive-only nodes.

The default may be overridden by the TARGET value on the individual TSS command.

Example

An entry of

```
CPFTARGET(*)
```

indicates that, by default, all TSS commands will be routed to all nodes defined in the CPFNODES control option.

2.14 CPFWAIT

CPFWAIT(YES|NO) sets a default value for the TSS command WAIT keyword.

At least one of the CPF-related control options **must** be entered at CA-Top Secret startup to use the Command Propagation Facility. If not, CPF may not be activated until the next CA-Top Secret startup and no CPF control options are accepted by CA-Top Secret until that time.

Note: If no journal file has been specified and if either WAIT(NO) is specified on the TSS Command or if the CPFWAIT control option is set to NO, then there is no way to view the output generated as the result of that command.

Format:	**Default:**	**Entry Method:**
CPFWAIT(YES|NO)	CPFWAIT(YES)	All

Operands **Description**

YES Specifies a default value for the TSS command WAIT keyword.

NO Specifies that no waiting will occur for messages.

Example

An entry of

```
CPFWAIT(NO)
```

indicates that when a TSS command is routed to a remote node, the issuer of the command will not wait for a response from that remote node before continuing.

Note: The value entered here may be overridden by the WAIT value on an individual TSS command.

2.15 DATE

This option specifies the format for dates displayed in listings. The DATE option accommodates various multinational date standards.

Format:	Default:	Entry Method:
DATE(xx/xx/xx)	DATE(MM/DD/YY)	All

Operands	Description
XX	Must be set to equal a combination of date characters, YY/DD/MM
YY	Year (90 . . .)
DD	Day (01 . . . 31)
MM	Month (01 . . . 12)
/	Slash will appear between date characters.
space	A blank space will appear between date characters.

Note: Any character, hyphen (-), period (.), comma(,) etc. may be used as a delimiter between the date fields.

2.15.1 Examples

Entering:	Will Produce:
DATE(YY/MM/DD)	90/04/01 for any listings produced on April 1, 1990.
DATE(MM-DD-YY)	04—01—90
DATE(DD MM YY)	01 04 90

2.16 DEBUG

DEBUG controls the production of debugging dumps used to determine the cause of abnormal error conditions.

Format:	Default:	Entry Method:
DEBUG(ON | OFF)	OFF	All

Operands Description

ON Produces a diagnostic dump. Use ONLY upon request of CA Technical Support.

OFF Deactivates the DEBUG feature.

2.16.1 General Information

DEBUG will be issued at the request of CA Technical Support to help determine the cause of specific abnormal events. Event output from this command will be written to the system console.

2.17 DIAGTRAP

DIAGTRAP is used, at the request of CA Technical Support, to produce a diagnostic dump. This is the CA-Top Secret equivalent to DUMP.

Format:	Default:	Entry Method:
DIAGTRAP(www,name,drc) DIAGTRAP(OFF)	(OFF)	Modify command

Operands **Description**

www Activates the trap in a particular location:

- **KER** trap within security kernel (TSSKERNL)
- **DB1** diagnostic location-1
- **DB2** diagnostic location-2
- **SFS** CA-Top Secret Security File services debugging.

name is the name of the job, user, or ACID that will trigger the dump. The "name" must match the logon ID that produced the error being diagnosed.

drc is the detailed violation reason code that must be produced to trigger the dump. The drc must be a decimal value which equals:

- **000** upon successful validation
- **001-254** to indicate a specific code.
- **255** to indicate any error condition

OFF deactivates the trap.

2.17.1 General Information

No examples will be provided in the documentation. CA will provide the specific parameters for use of the DIAGTRAP option.

2.18 DOWN

The DOWN option, which must be set while CA-Top Secret is active, determines how jobs are initiated and passwords changed when the CA-Top Secret address space is inactive.

Format:	Default:	Entry Method:
DOWN(fa,fa,...)	DOWN(BW,OW)	All

Operands **Description**

f(acility) identifies the system facility being affected by the DOWN action.

a(ction) identifies the action that CA-Top Secret will perform when its address space is down.

Operand	Must Equal:	To Indicate:
facility	B	BATCH Facility
facility	O	All other facilities
action	W	Wait for CA-Top Secret to be reactivated
action	B	Bypass security checking. Does not invoke CA-Top Secret until restarted.
action	F	Fail the request
action	N	Revert to native security (if any) until restarted.

2.18.1 General Information

DORMANT Mode

The DOWN options are ignored if CA-Top Secret is processing in global DORMANT mode.

2.18.2 Examples

The list below shows how the default DOWN(BW,OW) forces CA-Top Secret to process security when its address space is down.

Option **Indicates**

BW Batch jobs and password changes (B) will wait (W) for CA-Top Secret to be reactivated.

OW Online initiations and password changes (O) will wait (W) for CA-Top Secret to be reactivated.

The following table shows how DOWN actions will affect various CA-Top Secret processes.

PROCESS	WAIT	BYPASS	FAIL	NORMAL
Initiation or Logon	Initiations held and terminals locked	Security Ignored	Initiation Terminated	TSO UADS Password Required
Request for Password change	Initiations held and terminals locked	Wait	Wait	Wait
TSS Command	Failed	Failed	Failed	Failed
Data set in FAIL mode	Failed	BYPASS	Failed	Failed
Submit a permitted ACID	Job submitted without password	Job submitted without password	Job submitted without password	Job submitted without password
TAPE(DEF) processing (volume level)	Volume access denied	BYPASS	Volume access denied	Volume access denied
DUF update or extract	Failed	Failed	Failed	Failed

2.19 DRC

DRC allows security administrators to modify the characteristics of DRCs (Detailed Error Reason Codes). Refer to Detailed Violation Codes in *Messages and Codes* for a list of all DRCs.

Format:	Default:	Entry Method:
DRC(nnn,opt,opt...) DRC(nnn)	N/A	Parameter File or Modify Commands

Operands	Description
nnn	Is a three-digit decimal number from 001 to 159, which represents the DRC being modified or listed. Hexadecimal equivalents appear in many messages and on violation reports in TSSUTIL. Do not use these equivalents; refer to the *Messages and Codes* guide for the decimal format.
AUDIT	Violation event will be tagged with an audit attribute to allow TSSUTIL to select it with EVENT(AUDIT) as well as normal EVENT(VIOL).
NOAUDIT	Resets the AUDIT suboption.
FAIL	Violation causes CA-Top Secret to terminate the access attempt in ALL modes.
NOFAIL	Resets the FAIL suboption.
FAILWARN	Violation causes CA-Top Secret to terminate access attempts in WARN as well as FAIL or IMPL modes.

NOFAILWARN	Resets the FAILWARN option.
PW	Indicates that the violation is a password type violation, such as an invalid password entry, as opposed to an access violation such as an unauthorized resource access attempt.
NOPW	Resets the PW suboption.
NOVIOL	Do not treat event as a violation. Instead, flag the event, but do not FAIL the user.
VIOL	Resets the NOVIOL suboption.

2.19.1 Examples

The entry:

```
DRC(002,FAIL,AUDIT)
```

indicates that DRC 002: "Initiation failed by site exit" will terminate access attempts in all modes, including both DORMANT and WARN modes. CA-Top Secret will also write an Audit Record for this type of violation.

Displaying DRC Characteristics

To display the characteristics of DRC 002, enter:

```
TSS MODIFY DRC(002)
```

as an O/S Modify command.

2.19.2 General Information

Additional violation control may be performed in the installation exit via the VIOLATION call. Refer to the *User Guide* for details on the VIOLATION call.

2.20 DUFPGM

DUFPGM identifies up to five programs which allow for the extraction or update of the user installation data field (INSTDATA), bypassing the requirement that the ACID issuing the DUFXTR and/or DUFUPD call have the DUFXTR and/or DUFUPD ACID attribute.

Format:	Default:	Entry Method:
DUFPGM(pgm1,...|RESET)	N/A	All

Operands **Description**

pgm1 The programs (up to 5) that can be specified.

RESET Clears the entire program list.

2.20.1 Example

The entry:

```
DUFPGM(pgm1)
```

indicates the first program allowing for the extraction or update of the user installation data field. The entry:

```
DUFPGM(RESET)
```

indicates that the entire program list will be cleared.

2.20.2 General Information

If DUFPGM was changed using a TSS MODIFY command, the changes made remain in effect even if CA-Top Secret is restarted. Most control options revert to their default settings, the exceptions are DUFPGM, JESNODE and NJEUSR.

2.21 DUMP

DUMP is used to produce a diagnostic dump of control blocks within the CA-Top Secret address space and common system storage. Security administrators will only use this option when requested to do so by CA technical support.

Format:	Default:	Entry Method:
DUMP	N/A	TSS MODIFY commands

2.21.1 General Information

This option is protected by the Accountability feature as described in the Overview.

2.21.2 Examples

To use the DUMP option with the TSS MODIFY command enter:

```
TSS MODIFY(DUMP)
```

2.22 EXIT

EXIT activates and deactivates the installation exit.

Format:	Default:	Entry Method:
EXIT(ON | OFF)	EXIT(OFF)	All

Operands	Description
ON	Causes CA-Top Secret to call the installation exit module (TSSINSTX) at all exit control points.
OFF	Deactivates the installation exit.

2.22.1 General Information

Installation Exit

CA-Top Secret provides more than 17 control points at which systems programmers may write code to define security-checking procedures for initiation, volumes, and resources. This installation-unique code is housed in the TSSINSTX module, which resides in a link-listed library. CA-Top Secret accesses this module and performs all functions and validations. If the EXIT option is not specified, CA-Top Secret will assume EXIT(ON) provided that TSSINSTX exists. CA-Top Secret will ignore this option if no exit code exists.

If the exit abends, CA-Top Secret will automatically deactivate the exit and attempt to take a system dump.

Proper Installation Exit Format

The site must properly format and assemble the installation exit before it can be activated. A matrix within the exit will indicate the calls which the exit will accept. Refer to the *User Guide* for details.

2.23 EXPDAYS

EXPDAYS sets how many days TSS ADD or TSS PERMIT commands that are used with a FOR or UNTIL parameter are held in the Security File and displayed beyond its expiration date. Once these commands pass the expiration days, the adds or permissions are automatically removed from the user and the WHOHAS data for permits are also deleted.

Format:	Default:	Entry Method:
EXPDAYS(nn)	2	Parameter File

Operands Description

nn Specifies the number of days(from 01 to 30) a PERMIT or ADD is held in the Security File and displayed pass its expiration date.

If you set EXPDAYS to 00, the function is disabled.

2.23.1 Examples

The entry:

```
EXPDAYS(3)
```

indicates that the specific add or permit is held in the Security File and displayed three days beyond its expiration date.

Note: In order for the user to have the expired access again, a new TSS ADD or TSS PERMIT command needs to be issued for the resource, profile, etc.

2.24 FACILITY

FACILITY controls the processing of each system facility, or obtains the status of a facility. See "General Information" at the end of this section for a list of defaults for the FACILITY control option.

Format:	Entry Method:
FACILITY(facility|ALL)	All
FACILITY(facility=opt=value,opt,...)	All

Operands **Description**

facility Enter the full name of a single facility.

F TSS,FAC(TSO) causes CA-Top Secret to display status of TSO.

To use the FACILITY option with the TSS MODIFY command, use this format:

```
TSS MODIFY(control option(suboption=operand=value))
```

Example:

```
TSS MODIFY('FACILITY(BATCH=MODE=WARN)')
```

ALL Displays basic information about all facilities currently being used at an installation.

ABEND Resets the NOABEND suboption.

NOABEND A multiuser address space facility (such as CICS, IMS, CA-Roscoe etc.) will not abend if one user in the region causes a violation. This does not imply that the ACID used to define the Facility itself is immune from security abends during startup.

If NOABEND is set, CA-Top Secret will not cancel the user's activity--even if the violations exceed the violation's threshold (VTHRESH). CA-Top Secret will lock the user's terminal.

ACTIVE Reactivates a facility that was deactivated via the FAC(facility=INACT) command.

CA-Top Secret Status/Diagnostic Log listings will display "IN-USE" to indicate that a facility is active.

Example:

To allow signons to the IMSPROD facility, enter:

```
FAC(IMSPROD=ACTIVE)
```

ASUBM Indicates that CA-Top Secret-authorized job submission is being used for the given facility.

NOASUBM Resets the ASUBM suboption

AUDIT

Audits all activity for users who subseqently logon to the specified facility.

Example: To audit all user activity of a newly activated facility, enter:

```
FAC(IMSPROD=AUDIT)
```

NOAUDIT

Deactivates auditing of users who subsequently logon to the facility.

AUTHINIT Resets the NOAUTHINIT suboption.

NOAUTHINIT Indicates that the facility will issue a RACINIT in a problem state. Refer to the *User Guide* for details.

DEFACID(acid) Assigns a default ACID to be used for access to the specified facility by users who do not have defined ACIDs but require access to the facility. The TSS CREATE function must be used to define this default ACID. For example, a production CICS default ACID can be defined so that users who do not require specific security requirements are governed by the blanket requirements that are defined by the default ACID. To create this default ACID, enter:

```
FAC(CICSPROD=DEFACID(CICS1))
```

in the Parameter File and define the ACID as follows:

```
TSS CREATE(CICS1) DEPT(XXX) FAC(CICS)
    NAME('DEFAULT FOR CICS')
```

DEFACID(RDR*TERM)

Indicates that CA-Top Secret should derive the default ACID from the terminal or batch reader name, if the userid entered at signon is not defined as an ACID, or if the batch ACID is not supplied.

A default ACID for BATCH can be defined to handle RJE (Remote Job Entry) or NJE (Network Job Entry) job submission. If so defined, all jobs which are submitted will derive a default ACID associated with the NJE or RJE node. This will eliminate required JCL changes or possible viewing of passwords over the NJE or RJE lines.

A BATCH default ACID can also be defined for jobs submitted through a card reader. This will eliminate required JCL changes that would include coding of passwords on the job card.

To establish a default ACID for RJE remotes 1, 2, and 3, the security administrator would specify:

FACILITY(BATCH=DEFACID(RDR*TERM))

in the Parameter File. The security administrator would then create and define ACIDS for remote readers 1, 2, and 3. CA-Top Secret will use these ACIDS to derive the default ACIDS.

```
TSS CREATE(RM1) DEPT(XXX)
    FACILITY(BATCH) SOURCE(RM1)
    NAME('DEFAULT-FOR-SHOP-1')
```

The security administrator would continue to create ACIDS for readers 2 and 3. When a default ACID is assigned, the user receives message TSS7053I.

DEFACID(*NONE*)

Removes the default ACID for the facility specified.

Example:

```
FAC(BATCH=DEFACID(*NONE*))
```

Note: DEFACID should never be used with facility TSO.

DORMPW Honors password validation in DORMANT mode when specified for a facility. A DORMANT mode user must give the correct password to log on. For more details, see the discussion of the WARNPW sub-option.

Note: Message TSS7102E will only be issued for control type ACIDs (i.e., SCA, VCA, etc.).

NODORMPW Does not honor CA-Top Secret password validation in DORMANT mode.

DOWN=suboption

Controls how jobs are initiated and passwords changed for a facility when CA-Top Secret's address space is inactive. There are six sub-options associated with the DOWN option:

GLOBAL | *

Defaults to the setting defined by the DOWN control option. An asterisk (*) has the same meaning as GLOBAL. Refer to 2-29, for information on the DOWN control option.

WAIT Waits for CA-Top Secret to be restarted.

BYPASS Bypasses security checking, does not invoke CA-Top Secret until it is restarted.

FAIL Fails the request.

NORMAL Reverts to native security (if any) until CA-Top Secret is restarted.

EODINIT Indicates that a RACINIT can be performed for the facility after a TSS ZEOD has been issued. Required for JES and Console facilities.

NOEODINIT Indicates that a RACINIT cannot be performed for the facility after a TSS ZEOD has been issued.

ID= Equals either one or two alphanumeric characters that represents the facility for reporting purposes. This value is predefined in the Facilities Matrix Table and should not be changed unless defining or renaming a facility.

INACT Deactivates ability to sign on to the facility specified. Active users will continue normally.

Example: FAC(BATCH=INACT) prevents users from signing on to BATCH.

INSTDATA Allows installation data to be stored within a region of the specified facility. Refer to the *User Guide* for a description of INSTDATA.

Example:

```
FAC(BATCH=INSTDATA)
```

NOINSTDATA Prohibits storing of installation data in a facility region. Usually done to conserve space in large user regions.

IN-USE Indicates that the facility definition has been updated. It is used to determine if the facility should be displayed as a result of a TSS MODIFY, FAC(ALL) or a TSS MODIFY, STATUS command. FACILITIES will be marked as IN-USE as soon as a user signs on to them. Although it cannot be set directly, it is set by changing any option of the facility, either through the PARMFILE or via a TSS MODIFY command. IN-USE will be turned on even if the option is set to its default value.

KEY=n n may be set to equal the TCB protect key that the facility uses for storage. The default value is n=8.

LCFCMD Specifies that all LCF (Limited Command Facility) associated messages will refer to "Commands" in their text.

LCFTRANS Specifies that all LCF-associated messages will refer to "Transactions" in their text.

LOCKTIME=n Assigns a time after which a terminal connected to a specific facility will lock, if CA-Top Secret does not detect activity. Facility specific locktimes are overridden by a user's or profile's locktime.

Example:

```
FAC(CICSPROD=LOCKTIME=5)
```

indicates that terminals logged on to CICSPROD will lock if CA-Top Secret does not detect activity after five minutes.

LOG(log,log...) LOG indicates what types of security events CA-Top Secret will record, and where it will record them.

The LOG option allows this to be done for all facilities (global) while the LOG suboption allows LOG options to be specified for each facility. Facility-specific LOG options entered after any global LOG option will override the global option.

The security administrator may use the LOG suboption in one of three ways:

```
FAC(fac=LOG(ACTIVITY,ACCESS,SMF,INIT,MSG))
FAC(fac=LOG(NONE))
FAC(fac=LOG(ALL))
```

Example: To indicate that all events should be logged for CICS, enter:

```
FAC(CICSPROD=LOG(ALL))
```

Refer to the *Control Options* overview for a detailed discussion of the command hierarchy. Refer to the LOG option for definitions of its operands and examples of their use.

LUMSG Requests that the system display the "last-used" message when a user signs on to the specified facility. This operand only applies to USER type ACIDs.

Example:

```
FAC(CICSPROD=LUMSG)
```

NOLUMSG Terminates the last-used message display. Administrative type ACIDs will display "last-used" messages regardless of the setting of this operand.

MAXUSER=nnnn

Specifies the size of the ACID cross-reference table in any multi-user address space system. In order to increase the size of the cross-reference table, you must recycle the address space. In CICS, the MAXUSER value specified is also used to calculate necessary USCB allocation at startup.

The default is 3000.

MODE=mode Specifies a specific security mode for the facility:

DORM
FAIL
IMPL
WARN.

Modes specified by facility must be entered after global or system-wide mode selections. Thus, if the global mode is FAIL, but WARN is specified for the IMS facility, then all users initiating from IMS will operate in the WARN mode.

Refer to the *Control Options* overview for a detailed discussion of the command hierarchy. Refer to the MODE control option for a description of its operands.

MSGLC Indicates that user violation messages are to be issued in mixed case.

NOMSGLC Indicates that user violation messages are to be issued in upper case only.

MULTIUSER Used to indicate a multiuser address space.

A multiuser address space supports multiple users. Security is generally not handled by VSE. The following facilities are examples of multi-user address space facilities: CICS and CA-IDMS.

Example of a Multiuser Address Space:

```
FAC(CICSPROD=MULTIUSER)
```

NAME=fffff Changes the base name of a facility in the Facility matrix table. Once changed, the new facility name must always be used. To change a facility name from CICSPROD to CICSPAY, enter:

```
FAC(CICSPROD=NAME=CICSPAY)
```

NPWR Specifies whether a CICS facility supports password reverification. There is a default of two attempts for new passwords to be verified before complete logon sequence needs restarting. To set the threshold value for CICS, see the NPWRTHRESH control option for details. When a user logs on to a facility that has activated the NPWR sub-option of the FACILITY control option, and enters a new password, the following message is issued:

```
TSS7016A ENTER NEW PASSWORD AGAIN FOR REVERIFICATION
```

The user then enters the new password a second time for reverification. This ensures that the user correctly enters and remembers the new password. If the user enters an incorrect reverified password, he is prompted again. After the second attempt, if the reverified new password is still incorrect, the following message is issued:

```
TSS7111E NEW PASSWORD CHANGE INVALID - REVERIFICATION FAILED
```

and an accompanying DRC(015) is returned.

NONPWR Does not force password reverification.

PGM=xxx or xxxxxxxx

Supplies either all eight or just the first three characters of the program name issuing RACINIT SVC's. Online systems use RACINIT to support signon validation for individual users. This is the key to determining the (generic) facility. Refer to the *User Guide* for details on RACINIT.

Used together, PGM and MASTFAC can be used by an ACID to identify a Facility Matrix entry.

PRFT=nnnn Specifies the size of the shared profile table in increments of 256 entries. A single shared profile table is allocated at the start of a region if its facility has SHRPRF set.

A region's shared profile table must have enough entries to hold the highest number of unique profiles that can be allocated for use within the region at any time.

Example: a region supporting 250 users, each sharing 3 common profiles, where each user also has 1 unique profile, must have a shared profile table with no less than 253 entries: PRFT=1.

The default is PRFT=3. It supports profile sharing of up to 768 unique, active profiles with a region. If this value is changed via the TSS MODIFY command, the region must be recycled for the change to take effect.

NOPROMPT Deactivates the PROMPT suboption.

RES Used to allow storage of access authorizations for all resources within the online user region.

NORES Prevents the storage of permissions for maskable resources for users within this facility. Some examples of maskable resources are: DATASET, VSELIB, and VSEMEMBR. Any security checks against these resource classes will fail under this facility because the security permissions do not exist.

Prohibits the storage of data set, OPERCMDS, SDDSSF, VMMDISK, WRITER and volume authorizations within the online region. Usually done to conserve space.

Do not use this option for any facility that controls data set access. Examples are BATCH facilities. Security violations or 913 abends will result.

RNDPW Allows random password generation. CA-Top Secret offers two random password capabilities:

1. CICS users may enter RANDOM in the new password field at signon. These facilities will then generate a random password for the user. RNDPW must be set for the aforementioned facilities in order for this feature to work. RNDPW is set by default for CICS.

2. CA-Top Secret will automatically generate a new password when the user's current password expires. The RNDPW suboption must be in effect, and the NEWPW control option must specify the RN (random) suboption.

Before assigning the RNDPW attribute to a facility, test the option to ensure that the facility will display the randomly generated password. Some system facilities will randomly generate a password, but will not display the new password on the user's screen. This renders the RNDPW suboption useless, unless a systems programmer writes code to produce the display.

NORNDPW Cancels the RNDPW suboption.

SHRPRF Allows profile sharing in multiuser address space environments such as CICS where it is important to conserve storage. SHRPRF allows a copy of the profile to be shared by all users in the multiuser facility. Thus, storage is used efficiently. Of course, after a profile is updated, it is available to users when they sign on.

NOSHRPRF Prohibits profile sharing for the specified facility.

SIGN(M) Allows simultaneous logons with the same ACID for the specified facility.

SIGN(S) Disallows simultaneous logons with the same ACID for a multi-user region running under this facility.

If there are multiple regions running under one facility, an ACID can logon to any of these facilities - but only once.

STMSG Requests that the status message be displayed when a user signs on to the facility specified in the command. This operand only applies to USER type ACIDs.

NOSTMSG Terminates the display of status messages. Administrative type ACIDs receive a status message regardless of this operand.

SUAS Used to indicate a a single-user address space. For the purposes of CA-Top Secret, a single-user address space requests data sets directly from VSE. These facilities are single-user address spaces: BATCH.

TRACE Allows entire facility to be traced. Refer to 2.54, “SECTRACE” on page 2-106 for more information.

NOTRACE Deactivates the TRACE suboption.

TYPE When listing all facilities, a two-digit numerical value (ranging from 00 to 31) displays for the TYPE= parameter. This parameter should not be changed except when defining or renaming a new CICS facility. Then TYPE= must be specified as TYPE=CICS.

UIDACID=n Specifies that the first "n" characters of an online userid will be used to derive the ACID for the user.

WARNPW Forces defined users and jobs to use their correct passwords during the WARN mode. The default for the WARN mode would normally allow a job to process, even if the user omitted his password or entered it incorrectly.

If the user signs on with a security administrator's ACID, and omits or enters an invalid password, CA-Top Secret will FAIL the request regardless of the current security mode, or control option settings. CA-Top Secret will ignore the WARNPW option for undefined user ACIDS, and in DORMANT mode.

NOWARNPW Cancels the WARNPW suboption.

XDEF Indicates that transactions and commands are protected via LCF (Limited Command Facility). All transactions and commands must be defined to each user or profile through the LCF (Limited Command Facility) before the command or transaction can be used. This ensures protection of all commands and transactions used for the facility.

NOXDEF Indicates that transactions and commands need not be authorized through LCF before they can be used.

2.24.1 CICS-Related FACILITY Suboptions

The following suboptions are CICS specific and can be used when you have specified TYPE=CICS as the FACILITY option. For examples of how these CICS suboptions are used, refer to the *Implementation: CICS Guide.*

Suboption Description

BYPADD(resource)
Specifies CICS resources that will be added to the bypass list and **will not** be checked by CA-Top Secret security.

BYPLIST Lists CICS resources that are on the bypass list.

BYPREM(resource)
Specifies CICS resources that will be removed from the bypass list.

PROTADD(resource)
Specifies CICS resources that will be added to the protect list and will be checked by CA-Top Secret.

PROTREM(resource)
Specifies CICS resources that will be removed from the protect list.

Refer to the following resource list and the *Implementation: CICS Guide* for additional information.

2.24.1.1 CICS Resource Lists

Two lists of resources can be constructed using the Bypass and Protect suboptions listed above. Resources can be added to the bypass list to avoid checking by CA-Top Secret or to the protect list to be checked. If a resource is added to both lists the entry on the protect list will override the bypass list.

For example, if the following entry is made on the bypass list:

```
TSS MODIFY FAC(CICSTEST=BYPADD(TRANID=XY)
```

all transactions beginning with XY will avoid security checking. You can still check for security on transaction XYZ by entering:

```
TSS MODIFY FAC(CICSTEST=PROTADD(TRANID=XYZ)
```

The **PROTADD(TRANID=XYZ)** command overrides the **BYPADD(TRANID=XY)** command.

The following CICS resources can be used with the BYPADD, BYPREM, PROTADD, and PROTREM suboptions.

Note: This list is intended for a limited number of resources and should not be used as an alternative for the ALL Record.

CICS Resources:

Resource	Description
CEMT=action	Contains Extended Master Terminal Command actions, valid actions are: ADD, INQUIRE, PERFORM, REMOVE, and SET. For example, to bypass all CEMT INQUIRE commands, enter:

```
TSS MODIFY FAC(CICSTEST=BYPADD(CEMT=INQUIRE))
```

DCT=tdq	Contains transient data entries.
DSN=name	The entries in this list are not the actual dataset names, but the File Control Table entries associated with the datasets. The DSNCHECK= suboption must be set to YES.
FCT=ddname	Contains File Control Table entries. The DSNCHECK= suboption must be set to NO.

JCT=name Contains Journal Control Table entries.

LOCKTIME=(list)
Contains a single terminal or a list of terminal entries.

```
VTAM=Netname, TCAM=Terminal ID and BTAM=Terminal ID
```

For transactions, supply the tranid.

```
TSS MODIFY (fac(xxxxxxxx=PROTADD(LOCKTIME=yyyy)))
```

where:

x CICS facility name.

y Transaction.

PCT=tranid Contains interval control started transaction identifiers that will not be checked by CA-Top Secret.

PPT=name Contains program processing control entries that will not be checked by CA-Top Secret.

PSB=name Contains PSB entries.

SPI=action Contains a list of CICS command level application programming interface commands. Valid commands are: EXEC CICS SET and EXEC CICS INQUIRE. For example, to protect all EXEC CICS SET commands, enter:

```
TSS MODIFY FAC(CICSTEST=PROTADD(SPI=SET))
```

To bypass all EXEC CICS INQUIRE commands, enter:

```
TSS MODIFY FAC(CICSTEST=BYPADD(SPI=INQUIRE))
```

SYSID=sysid Contains system identification names of the CICS systems. SYSID= is only applicable to CICS 2.3 and below.

Note: If EXTSEC=NO is coded in either the DFHSIT parameter or the FACMATRX suboption, you must add SYSID to the bypass list.

TCT=(list) Contains a list of terminal entries.

```
VTAM=Netname, TCAM=Terminal ID and BTAM=Terminal ID
```

TRAN=tranid Contains transaction identifiers that will not be checked by CA-Top Secret.

TRANID=tranid

Contains transaction identifiers that will bypass all security checking for the transaction. When issuing a **TSS MODIFY(FAC(CICS facname))** command, the bypass list for TRANID will contain '...'. These periods represent CICS internal transactions whose names contain unprintable characters. These entries cannot be removed.

TRANID is different from TRAN in that TRANID uses all types of security checking (OTRAN, LCF, file, program, locktime). TRAN only uses OTRAN or LCF security checking.

```
TSS MODIFY FAC(CICS=BYPADD(TRANID=HELP))
```

Note: TRANID=TSS cannot be removed from the CICS Bypass List. It is always needed for LOCK/UNLOCK and nothing can be done with this transaction unless the ACID has the proper administrative authority.

TST=tsq Contains Temporary Storage entries.

DSNCHECK=YES|NO

Specifies whether individual dataset names or File Control Table entries will be checked. XFCT=YES is required for DSN checking if running CICS 2.3 or below. See FACMATRX suboption.

FACMATRX=YES|NO

Specifies whether the security related parameter in the DFHSIT will be used or the following FACILITY suboptions will be used.

The default is NO.

When using CA-ENF, CA-Top Secret processes calls based on the parameters set by your site. To improve performance, you can selectively disable calls for resources that are not protected by CA-Top Secret For more information on disabling CA-ENF calls when using XPARMS, refer to "Disabling ENF/CICS Intercepts" in the *Implementation: CICS Guide*.

Security can be set globally for CICS tables and transactions, or for individual tables or transactions by specifying one or more of the following operands.

Operand **Description**

EXTSEC=

where:

YES CA-Top Secret security **is** invoked for this region.

NO For CICS 2.3 and below:
CA-Top Secret security is inactive, but still present. CA-Top Secret is running in an inactive state. An entry has to be made to the SYSID bypass list if you are running in any mode except DORMANT.

For CICS TS 1.1 and above:
CA-Top Secret security is not present. No SYSID bypass list entry is necessary to inactivate security with this release.

EXTSEC= is only applicable to CICS 2.3 and below.

XAPPC= where:

YES Session security **can** be used.

NO Session security **cannot** be used. Only the BIND password (defined to CICS for the APPC connection) is checked.

XCMD= where:

YES EXEC CICS commands **are** checked by CA-Top Secret.

NO EXEC CICS commands **are not** checked by CA-Top Secret.

XDCT= where:

YES Transient data entries for this region **are** checked by CA-Top Secret.

NO Transient data entries for the region **are not** checked by CA-Top Secret.

XFCT= where:

YES File control entries for this region **are** checked by CA-Top Secret. Required for DSN checking.

NO File control entries for this region **are not** checked by CA-Top Secret. Deactivates DSN checking.

XJCT= where:

YES Journal entries for this region **are** checked by CA-Top Secret.

NO Journal entries for this region **are not** checked by CA-Top Secret.

XPCT= where:

YES EXEC-started transactions for this region **are** checked by CA-Top Secret.

NO EXEC-started transactions for this region **are not** checked by CA-Top Secret.

XPPT= where:

YES Program entries for this region **are** checked by CA-Top Secret.

NO Program entries for this region **are not** checked by CA-Top Secret.

XPSB= where:

YES PSB entries for this region **are** checked by CA-Top Secret.

NO PSB entries for this region **are not** checked by CA-Top Secret.

XTRAN= where:

YES Attached transaction entries for this region **are** checked by CA-Top Secret.

NO Attached transaction entries for this region **are not** checked by CA-Top Secret.

XTST= where:

YES Temporary storage entries for this region **are** checked by CA-Top Secret.

NO Temporary storage entries for this region **are not** checked by CA-Top Secret.

XUSER= where:

YES Surrogate user checking **will be** performed by CA-Top Secret.

NO Surrogate user checking **will not** be performed by CA-Top Secret.

RLP= where:

YES RLP processing **will be** activated by CA-Top Secret.

NO RLP processing **will not** be activated by CA-Top Secret.

SLP= where:

YES SLP processing **will be** activated by CA-Top Secret.

NO SLP processing **will not** be activated by CA-Top Secret.

LTLOGOFF=NO|YES

Specifies whether CA-Top Secret will log the user's terminal off when his locktime has expired for a second interval. The TSLO and TSSS transactions must be installed in the CICS region for LTLOGOFF to function properly. The default, NO, means that CA-Top Secret will not log the user off.

MAXSIGN=(nnn,RETRY|KILL)

Specifies the maximum number of concurrent signon/signoff requests that will be processed and the action to be performed on requests not processed. The default for nnn is 10, value can range from 1 to 50. RETRY, the default, requeues the signon/signoff request. Specifying KILL abends the signon/signoff transaction.

When coding MAXSIGN and MAXUSER in the CA-Top Secret PARM field, the MAXUSER option must be coded before MAXSIGN. If MAXUSER is not coded first, an invalid data error will occur during CA-Top Secret initialization.

MAXUSER=nnnn

Limits the amount of storage allocated by CA-Top Secret for user signon control blocks (USCB) which are getmained at CICS initialization. The MAXUSER value specified is used to calculate necessary USCB allocation.

The default is 3000, and the minimum value is 256.

PCTCMDSEC=HONOR|OVERRIDE

Specifies whether CA-Top Secret will honor the SIT parameter CMDSEC=. The default, OVERRIDE, means that CA-Top Secret will not honor the PCT CMDSEC= parameter and will force a security call.

Specifying HONOR, means that CA-Top Secret will honor the SIT parameter CMDSEC=.

PCTCMDSEC= is only applicable to CICS 2.3 and above.

PCTEXTSEC=HONOR|OVERRIDE

Specifies whether CA-Top Secret will honor the PCT parameters EXTSEC= and RSLC=. The default, OVERRIDE, means that CA-Top Secret will not honor the PCT EXTSEC= and RSLC= parameters and will force a security call.

Specifying HONOR, means that CA-Top Secret will honor the PCT parameters EXTSEC= and RSLC=.

PCTEXTSEC= is only applicable to CICS 2.3 and below.

PCTRESSEC=HONOR|OVERRIDE

Specifies whether CA-Top Secret will honor the SIT parameter RESSEC=. The default, OVERRIDE, means that CA-Top Secret will not honor the SIT RESSEC= parameter and will force a security call.

Specifying HONOR, means that CA-Top Secret will honor the SIT parameter RESSEC=.

PCTRESSEC= is only applicable to CICS/TS 1.1 and above.

2.24.2 General Information

BATCH:

```
INITPGM=$JOBACCT  ID=B   TYPE=01
ATTRIBUTES=IN-USE,ACTIVE,SHRPRF,NOASUBM,ABEND,SUAS,NOXDEF
ATTRIBUTES=LUMSG,STMSG,SIGN(M),INSTDATA,NORNDPW,AUTHINIT
ATTRIBUTES=NOPROMPT,NOAUDIT,RES,NOWARNPW,LCFCMD
ATTRIBUTES=MSGLC,NOTRACE,NODORMPW,NONPWR
MODE=FAIL  LOGGING=INIT,MSG,SEC9,SMF
UIDACID=8  LOCKTIME=000   DEFACID=*NONE*  KEY=8
```

CICSPROD

```
INITPGM=DFH    ID=C   TYPE=04
ATTRIBUTES=ACTIVE,SHRPRF,ASUBM,NOABEND,MULTIUSER,NOXDEF
ATTRIBUTES=LUMSG,STMSG,SIGN(M),INSTDATA,RNDPW,AUTHINIT
ATTRIBUTES=NOPROMPT,NOAUDIT,NORES,WARNPW,NOTSOC,LCFTRANS
ATTRIBUTES=MSGLC,NOTRACE,NODORMPW,NONPWR
MODE=FAIL  LOGGING=INIT,SMF,MSG,SEC9
UIDACID=8  LOCKTIME=000   DEFACID=*NONE*  KEY=8
FACMATRX=NO  EXTSEC=YES            RLP=NO     SLP=NO
XJCT=YES  XFCT=YES  XCMD=YES  XDCT=YES  XTRAN=YES
XTST=YES  XPSB=YES  XPCT=YES  XPPT=YES  XAPPC=NO
PCTEXTSEC=OVERRIDE   PCTCMDSEC=OVERRIDE
DSNCHECK=NO    LTLOGOFF=NO
MAXSIGN=050,KILL                MAXUSER=03000

BYPASS:  RESOURCE=TRANID   NAMES:   CAQP   CATD   CATP
         CAUT     CBRC     CCMF     CECS   CESF   CESN
         CLS1     CLS2     CMSG     CMPX   CNSE   CNPX
         CRDR     CQRY     CRSQ     CRSR   CRSY   CRSR
         CRTE     CRTR     CSAC     CSCY   CSGM   CSGX
         CSFU     CSIR     CSJC     CSKP   CSLG   CSMI
         CSM1     CSM2     CSM3     CSM4   CSM5   CSNC
         CSPG     CSPK     CSRK     CSPP   CSPQ   CSPS
         CSRS     CSSC     CSSF     CSSN   CSSX   CSSY
         CSTA     CSTB     CSTE     CSTT   CSXX   CVST
         CWTR     CWTO     CXCU     CXRE   TSSS   TSLO
         TSLA     TSLM     8888     9999   CLS3   CXRT
```

CICSTEST

```
INITPGM=DFH    ID=K   TYPE=04
ATTRIBUTES=ACTIVE,SHRPRF,ASUBM,NOABEND,MULTIUSER,NOXDEF
ATTRIBUTES=LUMSG,STMSG,SIGN(M),INSTDATA,RNDPW,AUTHINIT
ATTRIBUTES=NOPROMPT,NOAUDIT,NORES,WARNPW,NOTSOC,LCFTRANS
ATTRIBUTES=MSGLC,NOTRACE,NODORMPW,NONPWR
MODE=FAIL   LOGGING=INIT,SMF,MSG,SEC9
UIDACID=8      LOCKTIME=000   DEFACID=*NONE*    KEY=8
FACMATRX=NO         EXTSEC=YES        RLP=NO     SLP=NO
XJCT=YES   XFCT=YES   XCMD=YES   XDCT=YES  XTRAN=YES
XTST=YES   XPSB=YES   XPCT=YES   XPPT=YES  XAPPC=NO
PCTEXTSEC=OVERRIDE   PCTCMDSEC=OVERRIDE
DSNCHECK=NO       LTLOGOFF=NO
MAXSIGN=050,KILL                      MAXUSER=3000

BYPASS:  RESOURCE=TRANID   NAMES:   CAQP   CATD   CATP
         CAUT     CBRC     CCMF     CECS   CESF   CESN
         CRDR     CQRY     CRSQ     CRSR   CRSY   CRSR
         CRTE     CRTR     CSAC     CSCY   CSGM   CSGX
         CSFU     CSIR     CSJC     CSKP   CSLG   CSMI
         CSM1     CSM2     CSM3     CSM4   CSM5   CSNC
         CSPG     CSPK     CSRK     CSPP   CSPQ   CSPS
         CSRS     CSSC     CSSF     CSSN   CSSX   CSSY
         CSTA     CSTB     CSTE     CSTT   CSXX   CVST
         CWTR     CWTO     CXCU     CXRE   TSSS   TSLO
         TSLA     TSLM     8888     9999   CLS3   CXRT
```

IDMSPROD:

```
INITPGM=RHD    ID=M  TYPE=11
ATTRIBUTES=ACTIVE,SHRPRF,ASUBM,NOABEND,MULTIUSER,NOXDEF
ATTRIBUTES=LUMSG,STMSG,SIGN(M),INSTDATA,RNDPW,AUTHINIT
ATTRIBUTES=NOPROMPT,NOAUDIT,NORES,WARNPW,NOTSOC,LCFTRANS
ATTRIBUTES=MSGLC,NOTRACE,NODORMPW,NONPWR
MODE=FAIL  LOGGING=ACCESS,INIT,MSG,SEC9
UIDACID=8  LOCKTIME=000   DEFACID=*NONE*  KEY=8
```

IDMSTEST:

```
INITPGM=RHD    ID=Q  TYPE=11
ATTRIBUTES=ACTIVE,SHRPRF,ASUBM,NOABEND,MULTIUSER,NOXDEF
ATTRIBUTES=LUMSG,STMSG,SIGN(M),INSTDATA,RNDPW,AUTHINIT
ATTRIBUTES=NOPROMPT,NOAUDIT,NORES,WARNPW,NOTSOC,LCFTRANS
ATTRIBUTES=MSGLC,NOTRACE,NODORMPW,NONPWR
MODE=FAIL  LOGGING=INIT,MSG,SEC9
UIDACID=8  LOCKTIME=000   DEFACID=*NONE*  KEY=8
```

IMSPROD:

```
INITPGM=DFS    ID=I  TYPE=05
ATTRIBUTES=ACTIVE,SHRPRF,ASUBM,NOABEND,MULTIUSER,NOXDEF
ATTRIBUTES=LUMSG,STMSG,SIGN(M),INSTDATA,RNDPW,AUTHINIT
ATTRIBUTES=NOPROMPT,NOAUDIT,NORES,WARNPW,NOTSOC,LCFTRANS
ATTRIBUTES=MSGLC,NOTRACE,NODORMPW,NONPWR
MODE=FAIL  LOGGING=INIT,MSG,SEC9
UIDACID=8  LOCKTIME=000   DEFACID=*NONE*  KEY=8
```

USER0

```
INITPGM=000    ID=A TYPE=19
ATTRIBUTES=ACTIVE,SHRPRF,NOASUBM,ABEND,SUAS,NOXDEF
ATTRIBUTES=LUMSG,STMSG,SIGN(M),INSTDATA,NORNDPW,AUTHINIT,
ATTRIBUTES=NOPROMPT,NOAUDIT,RES,WARNPW,NOTSOC
ATTRIBUTES=NOTRACE,NODORMPW,NONPWR,MSGLC
MODE=FAIL  LOGGING=INIT,SMG,MSG
UIDACID=8  LOCKTIME=000   DEFACID=*NONE*  KEY=8
```

USER1:

```
INITPGM=111    ID=1 TYPE=31
ATTRIBUTES=ACTIVE,SHRPRF,NOASUBM,ABEND,SUAS,NOXDEF
ATTRIBUTES=LUMSG,STMSG,SIGN(M),INSTDATA,NORNDPW,AUTHINIT,
ATTRIBUTES=NOPROMPT,NOAUDIT,RES,NOWARNPW,NOTSOC
ATTRIBUTES=NOTRACE,NODORMPW,NONPWR,MSGLC
MODE=FAIL  LOGGING=INIT,SMF,MSG
UIDACID=8  LOCKTIME=000   DEFACID=*NONE*  KEY=8
```

USER2:

```
INITPGM=222    ID=2  TYPE=30
ATTRIBUTES=ACTIVE,SHRPRF,NOASUBM,ABEND,SUAS,NOXDEF
ATTRIBUTES=LUMSG,STMSG,SIGN(M),INSTDATA,NORNDPW,AUTHINIT,
ATTRIBUTES=NOPROMPT,NOAUDIT,RES,NOWARNPW,NOTSOC
ATTRIBUTES=NOTRACE,NODORMPW,NONPWR,MSGLC
MODE=FAIL  LOGGING=INIT,SMF,MSG
UIDACID=8  LOCKTIME=000   DEFACID=*NONE*  KEY=8
```

USER3:

```
INITPGM=333    ID=3  TYPE=29
ATTRIBUTES=ACTIVE,SHRPRF,NOASUBM,ABEND,SUAS,NOXDEF
ATTRIBUTES=LUMSG,STMSG,SIGN(M),INSTDATA,NORNDPW,AUTHINIT,
ATTRIBUTES=NOPROMPT,NOAUDIT,RES,NOWARNPW,NOTSOC
ATTRIBUTES=NOTRACE,NODORMPW,NONPWR,MSGLC
MODE=FAIL  LOGGING=INIT,SMF,MSG
UIDACID=8  LOCKTIME=000   DEFACID=*NONE*  KEY=8
```

USER4

```
INITPGM=444    ID=4  TYPE=28
ATTRIBUTES=ACTIVE,SHRPRF,NOASUBM,ABEND,SUAS,NOXDEF
ATTRIBUTES=LUMSG,STMSG,SIGN(M),INSTDATA,NORNDPW,AUTHINIT,
ATTRIBUTES=NOPROMPT,NOAUDIT,RES,NOWARNPW,NOTSOC
ATTRIBUTES=NOTRACE,NODORMPW,NONPWR,MSGLC
MODE=FAIL  LOGGING=INIT,SMF,MSG
UIDACID=8  LOCKTIME=000   DEFACID=*NONE*  KEY=8
```

VM:

```
INITPGM=TSS    ID=V  TYPE=08
ATTRIBUTES=ACTIVE,SHRPRF,NOASUBM,ABEND,SUAS,NOXDEF
ATTRIBUTES=NOLUMSG,NOSTMSG,SIGN(M),INSTDATA,RNDPW,AUTHINIT
ATTRIBUTES=NOPROMPT,NOAUDIT,RES,WARNPW,NOTSOC,LCFCMD
ATTRIBUTES=MSGLC,NOTRACE,NODORMPW,NONPWR
MODE=FAIL  LOGGING=INIT,MSG,SEC9
UIDACID=8  LOCKTIME=000   DEFACID=*NONE*  KEY=8
```

2.24.3 User Facilities

In addition to the pre-defined facility entries, 222 user-facility entries — with names of USER0 through USER221 — are available for site customization. Each facility entry has identical attributes (as shown below) with only the ID field unique to each.

Facilities	ID Field
USER0 - USER09	0 through 99
USER100 - USER109	A0 through A9
USER110 - USER119	B0 through B9
USER120 - USER129	C0 through C9
USER130 - USER139	D0 through D9
USER140 - USER149	E0 through E9
USER150 - USER159	F0 through F9
USER160 - USER169	G0 through G9
USER170 - USER179	H0 through H9
USER180 - USER189	I0 through I9
USER190 - USER199	J0 through J9
USER200 - USER209	K0 through K9
USER210 - USER219	L0 through L9
USER220 - USER221	M0 through M1

The ID field is the same as the numeric value of the USERnnn facility. For example, for facility USER0 the ID= will be 0, for facility USER23 the ID= will be 23, etc.

USERnnn:

```
INITPGM=********  ID=xx    TYPE=99
ATTRIBUTES=ACTIVE,SHRPRF,ASUBM,NOABEND,MULTIUSER,NOXDEF
ATTRIBUTES=LUMSG,STMSG,SIGN(M),INSTDATA,RNDPW,AUTHINIT
ATTRIBUTES=NOPROMPT,NOAUDIT,RES,WARNPW,LCFTRANS
ATTRIBUTES=MSGLC,NOTRACE,NODORMPW,NONPWR
MODE=FAIL  LOGGING=INIT,MSG,SEC9
UIDACID=8  LOCKTIME=000  DEFACID=*NONE*    KEY=8
```

2.25 HPBPW

HPBPW selects the maximum number of days that CA-Top Secret will honor an expired or previous password for batch jobs.

Format:	Default:	Entry Method:
HPBPW(n)	HPBPW(0)	All

Operands Description

n Must be a number from zero through nine. This number will represent the number of days that CA-Top Secret will honor an expired or previous password associated with a batch job.

2.25.1 General Information

CA-Top Secret will check the HPBPW setting if a user submits a job and changes his password prior to the job's initiation.

CA-Top Secret will check the HPBPW setting to determine if the job has initiated within the number of days specified. CA-Top Secret will honor the user's previous password if the job initiates within the HPBPW setting.

This option is useful if jobs are left on the hold queue for later execution.

2.25.2 Examples

An entry of:

```
HPBPW(1)
```

indicates that CA-Top Secret will honor a batch job's expired or previous password for one day. An entry of:

```
HPBPW(0)
```

deactivates the option.

2.26 IBMCUST

IBMCUST defines the IBM customer number, if the product was purchased from IBM. This option should not be used with LMPCHECK.

Format:	**Default:**	**Entry Method:**
IBMCUST (xxxx-xxx-xxxx)	N/A	Parameter file only

2.27 IBMPASS

IBMPASS defines the IBM product password.

Format:	Default:	Entry Method:
IBMPASS (xxxx-xxxx-xxxx-xxxx-xxxx)	N/A	Parameter file only

2.28 INACTIVE

INACTIVE selects the number of days before CA-Top Secret will deny an unused ACID access to the system after that ACID's password has expired.

Format:	Default:	Entry Method:
INACTIVE(0-255)	INACTIVE(0)	All

Operands	Description
Any number from 1 to 255	The number of days after which an ACID connected to an expired password will be prohibited from signing on.
0	Deactivates the INACTIVE option.

2.28.1 General Information

This option prohibits the use of ACIDS that have not been used for long periods of time. This "period of time" starts from the day that the ACID's password expired and continues through the number of days that the security administrator specified in the INACTIVE control option. If CA-Top Secret does not detect activity for an ACID within this time period, it will deny access to the system to any user or job using this ACID by SUSPENDing the ACID.

2.28.2 Examples

The SCA has entered the following into the Parameter File:

```
INACTIVE(5)
```

If an ACID is not used for five consecutive days after its password expires, CA-Top Secret would deny access to any user or job that attempts to access the system by using that ACID.

The user could avoid the situation described above by changing his password before the expiration date, or by changing his password within the five-day threshold specified in the INACTIVE control option.

The security administrator can reactivate an INACTIVE ACID by removing SUSPEND from user and replacing the password specifying the expiration interval or expire option.

```
TSS REMOVE(acid) SUSPEND
```

and

```
TSS REPLACE(acid) PASSWORD(xxx,030)
```

or

```
TSS REPLACE(acid) PASSWORD(xxx,,EXP)
```

2.29 INSTDATA

INSTDATA controls the value of the 8-byte global installation data area. This value is passed to the security exit developed at a particular site. INSTDATA is not related to the ACID INSTDATA area.

Format:	Default:	Entry Method:
INSTDATA(0)	INSTDATA(0)	All
INSTDATA(XXXX...)		

Operands	Description
0	Resets the field to zero.
XXXX	Alters the value to hexadecimal xx, where each xx is 1 to 4 pairs of hexadecimal digits.

2.30 IOTRACE

IOTRACE controls a diagnostic trace for use by CA technical support. The trace is produced on the TRACE/LOG data set.

Caution

Do not use this option unless requested to do so by CA technical support. This option will produce voluminous output.

Format:	Default:	Entry Method:
IOTRACE(ON | OFF)	N/A	All

Operands	Description
ON	Activates an input/output.
OFF	Deactivates the trace.

2.31 JOBACID

JOBACID identifies the field on every batch job card from which the ACID will be derived when the source of the submission cannot be identified and if no USER= field is present on the job card.

If a value for the USER= parameter is coded on the jobcard, this value will override any JOBACID option.

Format:	**Default:**	**Entry Method:**
JOBACID(Field,Position [,Start])	JOBACID(U,7)	All

2.31.1 Operands

Field Prefix:	**Field Name:**	**Operand:**	**Position Name & Meaning:**
A	Accounting	Digit from 1-8	Parameter within the field becomes the ACID, optionally starting in the nth position within that field.
P	Programmer Name	Digit from 1-8	Parameter within the field becomes the ACID, optionally starting in the nth position within that field.
U	User keyword	Digit from 1-7	First n characters become the ACID, optionally starting in the nth position.
J	Job Name	Digit from 1-8	First n characters become the ACID.
R	Reader Name	Digit from 1-8	First n characters become the ACID.

2.31.2 General Information

Batch Jobs

All batch jobs must be identified with an ACID and password in the FAIL mode, unless default ACIDS are assigned.

The security administrator may use the JOBACID control option to indicate which field on the JOB card should be used as the ACID. Thus the:

```
JOBACID(A,1)
```

indicates that the first parameter of the Accounting field should be used as the ACID:

```
//JOB JOBA ADMIN
```

The ADMIN parameter will be used as the ACID.

Sub-Accounting

For installations that use "sub-accounting," CA-Top Secret will treat the slash '/' and dash '-' as delimiters of an accounting number that is used as an ACID.

2.31.3 Examples

When JOBACID(A,1) is used, the ACID is ADM200 in the following account specifications:

```
ADM200-SMYTHE

ADM200/JUN82
```

JOBACID(U,3)

Indicates that the first three characters of the USER field will be used as the ACID.

Note: USER is restricted to a maximum of seven characters by VSE JCL rules.

```
* $$ JOB USER=CST5NG
```

JOBACID(P,2)

Indicates that the second parameter of the Programmer Name will be used as the ACID.

```
* $$ JOB PROGR='JOE SMITH'
```

JOBACID(J,5)

Indicates that the first five characters of the job name should be used as the ACID.

```
// JOB BUDGET
```

JOBACID(R,8)

Indicates that the entire reader name (other than INTRDR) will be used as the ACID.

JOBACID(U,4,3)

Indicates that the USER field will be used as the ACID, for a length of four characters starting at the third position.

```
//EXAMPLED JOB 123,USER=ABCDEF
ACID = CDEF
```

2.32 LIBRPROT

LIBPROT is used to identify the access level for protection of VSE system libraries. It is also used to enable or disable VSE system library member level protection.

Format:	Default:	Entry Method:
LIBRPROT(OFF) LIBRPROT(LIBRARY |SUBLIBR|MEMBER)	LIBRPROT (MEMBER)	TSS Parameter

Operands	Description
OFF	Disables VSE library protection for all libraries.
LIBRARY	Enables VSE library protection for access at the primary library level.
SUBLIBR	Enables VSE Library protection for access at the primary library and sub-library level.
MEMBER	Enables VSE Library protection for access at the primary library, sub-library level, and member level.

2.33 LMPCHECK

LMPCHECK verifies that the correct License Management Program (LMP) encryption key is being used for this system.

Format:	**Default:**	**Entry Method:**
LMPCHECK	N/A	O/S command only

2.33.1 General Information

If you do not issue this command, CA-Top Secret will perform a check of the encryption key every 30 minutes until LMP verifies the key. If an invalid key is found, CA-Top Secret will be placed in WARN mode. Once LMP verifies the encryption key, normal CA-Top Secret processing will be restored. CA-Top Secret will return to the mode that was in effect before it placed itself in WARN mode. Refer to the *Installation Guide* and the *CA-CIS Installation Guide* for more information about LMP keys.

This option cannot be used with IBMCUST.

2.34 LOG

LOG identifies the types of events that CA-Top Secret will log and specifies whether the events will be logged onto the ATF (Audit Tracking File). This option also specifies if the violation message will be displayed.

The LOG option affects all facilities. A Global LOG command can be overridden by a LOG operand entered as a suboption for a specific facility. Refer to the FACILITY control option for details.

Format:	Default:	Entry Method:
LOG(ACTIVITY,ACCESS, SMF,SEC9,INIT,MSG)	LOG(SMF,INIT, SEC9, MSG)	All
LOG(NONE)		
LOG(ALL)		

Operands Description

ACTIVITY
Logs all activity for all facilities to the SMF. This is the same as specifying:

```
LOG(ACCESS,INIT)
```

SMF Events will be written to the SMF file in addition to the ATF if applicable.

ACCESS Logs all resource access.

Note: Access to the following resources is not logged:

DBD
FCT
JCT
LCF
OTRAN
PPT
PROGRAM
PSB

SEC9 Routes violation summary messages:

TSS7100E
TSS7220E
TSS7200E
TSS7250E

to the security console via route code 9.

INIT Logs all job/session initiations and terminations.

MSG Violation messages are displayed for batch jobs, started tasks, or at the online user's terminal.

For users in FAIL mode, violation messages will always appear. Password violations will also always appear.

ALL Selects all log options for all facilities.

NONE Deactivates all ATF logging, except for violations and audited events to the ATF.

If the user facility is in DORMANT mode, no logging takes place unless the resource permitted is specified with ACTION(FAIL).

2.34.1 General Information

CA-Top Secret uses SMF type 80 format records. A DSECT (Dummy Control Section) for these records is documented in the installation exit (TSSINSTX) source code.

LOG(ACCESS), LOG(ACTIVITY), and LOG(ALL) are primarily diagnostic tools for CA technical support people. Because each option produces a large number of records, dumping such a large volume of records on the Audit/Tracking File, may cause excessive wrapping of the File, which, in turn, means you need a larger File. In short, limit your use of these three options.

Protection Of Option

The LOG option is protected by the operator accountability feature. CA-Top Secret will prompt the person entering the command for the proper ACID/password combination before processing the LOG option. CA-Top Secret will also create an audit trail identifying the ACID under which the LOG specification was made.

Recording Violations

If the CAIAUD1 DLBL statement is entered into the CA-Top Secret start procedure, then the recording of violations into the ATF will always occur. Violations are always written to available files. Violation recording cannot be prevented (in all modes except DORMANT), even if LOG(NONE) is entered. Refer to the DRC and MSG control options for instructions on how to tailor and/or suppress violation messages.

Use Of Report Utilities

An important prerequisite to the reporting and tracking of security events is the correct specification of log options. TSSUTIL and TSSTRACK can be used to build reports, but only based on data that is stored in the ATF. Refer to the *Report and Tracking* guide for details.

2.35 LOGBUF

LOGBUF allows the maximum number of in-core logging buffers to be used by CA-Top Secret. The buffers are 8k in size under VSE/ESA.

Format:	Default:	Entry Method:
LOGBUF(nn)	LOGBUF(32)	Parameter File (first CA-Top Secret startup only) or Modify Command

Operands Description

nn A two digit number representing the number of logging buffers to be used by CA-Top Secret.

2.36 MODE

MODE selects the security mode in which CA-Top Secret will operate for all facilities.

The MODE option is used to set a global mode. Modes may be assigned to a specific subsystem facility, permitted to a specific ACID, or assigned by the ACTION keyword on a permission. The order of the search for MODE is as follows:

1. ACTION on a permission
2. Subsystem facility (i.e., DB2FAC)
3. User mode permission
4. Facility
5. Global

Refer to the following:

- FACILITY control option for details on how to assign a MODE to a facility.
- DB2FAC for details on how to assign a facility to a DB2 subsystem.
- ACTION keyword for details on how to assign a mode for a specific resource permission.

Format:	**Default:**	**Entry Method:**
MODE(DORMANT|WARN |FAIL|IMPL)	FAIL	All

Modes	**Description**
DORMANT	CA-Top Secret will not perform security validation for normal users (everyone except security administrators). Normal users will enter their current signon and password, not a CA-Top Secret password. CA-Top Secret will always perform password validation for Security Control ACIDS (security administrators). Security administrators who sign on with their security control ACID, will be prompted for their CA-Top Secret password. CA-Top Secret will also always perform password validation for those users whose UADS data fields are being managed by CA-Top Secret. Exceptions may be specified via the DRC control option, or via the TSS PERMIT ACTION(FAIL) command.
WARN	CA-Top Secret will perform security validations for all access attempts. Users who are guilty of security violations will receive a message indicating that they have violated security, but will not be denied access to the resource unless exceptions have been specified. All specified LOG options are in effect.

Exceptions may be specified via the DRC control option, or via the TSS PERMIT ACTION(FAIL) command.

IMPL This mode is referred to as a gradual implementation mode since it will fully protect defined resources, and monitor all access requests made by defined users. Defined resources are protected and violations result in denied access. This mode will, however, allow undefined users uninhibited access to undefined resources. Thus, security can be gradually applied to selected users and resources with little or no impact.

FAIL CA-Top Secret will deny all unauthorized facility or resource access unconditionally. All users must be defined.

2.36.1 General Information

The MODE option is protected by the operator accountability feature. CA-Top Secret will prompt the person entering the command for the proper ACID/password combination before processing the MODE option. CA-Top Secret also creates an audit trail that identifies the ACID under which the MODE was specified.

2.37 MSG

MSG allows the site to modify the characteristics of certain CA-Top Secret violation messages that are contained in the CA-Top Secret Message Table. The site may alter the characteristics of the message, such as when and how the message is issued or suppressed, but not the text of the message.

Format:	Default:	Entry Method:
MSG(nnnn(opt,opt,...)	N/A	Parameter File or Modify Command
MSG(nnnn)		

Operands	Description
nnnn	Enter the four-digit CA-Top Secret message number that corresponds to the message being listed or modified.
SEC9	Indicates that the message is a violation summary that is sent to the security console by using WTO route code 9.
NOSEC9	Cancels the SEC9 suboption.
USER	Indicates that the message is directed to the user.
NOUSER	Cancels the USER suboption.
FORCE	Message must always be issued, even if the LOG option does not include the MSG suboption.
NOFORCE	Cancels the FORCE suboption.
DSN	Message is associated with data set name indicator message TSS7230I.
NODSN	Cancels the DSN suboption.
SWARN	Suppress message display if user is in WARN mode.
NOSWARN	Cancels the SWARN suboption.
SIMPL	Suppress the message display if user is in the IMPL mode.
NOSIMPL	Cancels the SIMPL suboption.
SDEF	Suppress the message display for defined users.
NOSDEF	Cancels the SDEF suboption.
SUNDEF	Suppress the message display for undefined users.
NOSUNDEF	Cancels the SUNDEF suboption.

SBATCH	Suppress message display if user is using BATCH processing.
NOSBATCH	Cancels the SBATCH suboption.
SONLINE	Suppress the message display for online users (CICS, IMS etc).
NOSONLINE	Cancels the SONLINE suboption.
SUPPRESS	Suppress the message display at all times for all users.
NOSUPPRESS	Cancels the SUPPRESS suboption.

2.37.1 General Information

Displaying MSG Characteristics

To display the characteristics of a specific MSG or MSGs, enter:

```
TSS MODIFY,MSG(nnnn)
```

Modification Restrictions

MSG modifications may be made to CA-Top Secret messages in the range of 7000 to 7999.

Additional Modifications

Additional message editing may be performed in the installation exit via the MESSAGE EDIT call. Refer to the *User Guide* for details.

Valid Message Suppression

Suppressions are in effect only if all suppress conditions are valid, i.e. "AND" logic is used.

2.37.2 Examples

The entry:

```
TSS MODIFY,MSG(7205,SBATCH,SUNDEF,SIMPL)
```

indicates that message TSS7205 will be suppressed for undefined batch jobs in the IMPL mode only.

To determine the characteristics of message TSS7003W, enter the following modify command:

```
TSS MODIFY,MSG(7003)
```

Entry Into Parameter File

```
*
* CONTROL OPTIONS
*
MODE(WARN)
MSG(7003,SBATCH,SUNDEF,SIMPL)
```

2.38 MSUSPEND

MSUSPEND allows the MSCA's ACID to be suspended automatically if the password violation threshold set via the PTHRESH option is exceeded. This will prevent a user from making an unlimited number of guess attempts to determine the MSCA's password.

This option is ignored for BATCH or STC use.

Format:	Default:	Entry Method:
MSUSPEND(YES | NO)	NO	All

Operands Description

YES MSCA's ACID will be suspended if the password violation threshold is exceeded.

NO Cancels the MSUSPEND option.

2.38.1 General Information

If a suspended MSCA signs on and enters the password correctly, CA-Top Secret will prompt the master console via message:

```
TSS7186I  SUSPENDED CONTROL SECURITY ADMINISTRATOR ATTEMPTING
SIGNON

TSS7187A SPECIFY <Y> TO CONFIRM SIGNON, <N> TO DENY USE OF MSCA
ACID
```

To remove the SUSPEND attribute, refer to Chapter 3 of the *Command Functions Guide.*

2.38.2 Examples

To protect the MSCA's password from password-guessing attempts, enter:

```
F TSS,MSUSPEND(YES)
```

2.39 NEWPW

NEWPW specifies the rules that CA-Top Secret will apply when a user selects a new password. Valid operands are described below. When modifying the NEWPW control option, you *must specify* all selected operands except MIN, MINDAYS, and WARN. Any changes to existing operands replace the previous selections.

Format:	**Default:**	**Entry Method:**
NEWPW(opr,opr,...)	NEWPW(MIN=4, WARN=03, MINDAYS=01, NR=0, ID, TS, RS)	All

Operands Description

MIN=n Selects the minimum length of a password, or minimum length of the mask used to generate random passwords. **n** must equal a number from 3 thru 8.

MINDAYS=nn

Sets the number of days after a password has been changed that a user will not be allowed to change his password again.

MINDAYS=00 deactivates MINDAYS processing altogether.

For example, an entry of:

```
NEWPW(MINDAYS=5)
```

indicates that a user must wait five full days (day six) to change his password again.

Note:

- MINDAYS is only applicable for USER type acids.
- This operand does not apply to Administrative ACIDs.
- MINDAYS is not applicable to users who have a non-expiring password.

ID Prevents a user from specifying a new password that contains his ACID, or a new password whose first four characters are equal to part of his name.

For example, a user named PERCY SNORTHAMMER would be prohibited from entering new passwords like SNORT or PERC56.

NM Indicates that only numbers may appear in a new password.

NO Indicates that only the MIN= and MINDAYS= suboptions will apply to new passwords.

NR=n Specifies the number of pairs of repeating characters in a new password. NR or NR=0 indicates that no characters may be repeated in succession. Specifying:

```
NEWPW(NR=1)
```

would allow a password of RABBIT (one pair of repeating characters: 'BB') but would prevent new passwords of RABBITT (two pairs of repeating characters: 'BB' and 'TT') and RABBBIT ('BBB' is considered to be two pairs).

NU Prevents ACID TYPE(USER) from changing their passwords.

NV Indicates that vowels (A,E,I,O,U) cannot appear in a new password.

RN CA-Top Secret randomly generates a password for users when their password expires.

Note: If the FACILITY control option contains RNDPW and NEWPW(RN) is set, CA-Top Secret will automatically generate a random password for the user whose password has expired. However, if the NEWPW option does not have RN set, a user can still specify a random password by typing the word RANDOM in the new password field at logon. CA-Top Secret will generate a random password for that user.

If the FACILITY control option does not contain RNDPW, CA-Top Secret ignores this option.

Refer to the FACILITY control option for details. STC and BATCH facilities do not properly support this feature.

RS Prevents the user from specifying a new password that is on the restricted passwords list. Refer to the RPW control option.

SW Requires that the new password contain a national character ($,@,#) between the first and last position. For example:

```
BIG$RED, I$AM@ME
```

The use of SW (split word) control will make the LOGON Reconnect feature of TSO unusable since LOGON Reconnect is not capable of processing passwords containing national characters.

TS Prevents users from specifying a password too similar to their previous password. A new password is considered to be too similar if:

- The first three characters are identical
- The second three characters are identical
- The last three characters are identical

New passwords that are identical to previous passwords are always rejected, regardless of the NEWPW setting.

WARN=nn

nn must be set to equal the interval, in days, that CA-Top Secret issues messages TSS7003W and TSS7004W, which warn users that their passwords or ACIDs are about to expire.

MASK=mask

Allows the security administrator to create a "mask," which dictates the type of character that will be accepted for each position in a password. CA-Top Secret will apply this mask to user initiated and randomly generated password changes. Character types used in the mask are:

a any alphabetic character

c consonant

v vowel

n numeric character

x non-vowel

? any character

Note: The only valid characters for a user changing his password are alphabetic, numeric, and special characters, such as @, #, $,], », and Œ. Characters such as %, !, and (do not apply.

An entry of MASK=vnvn could generate password: A5I6.
The mask will override the NV and NM suboptions.

2.40 NJEUSR

NJEUSR is used to define a default ACID to be used for NJE Store-and-Forward nodes where no other userid can be identified. This control option is used to specify the userid when building a default token in response to a verify SESSION=TKNUNKWN request.

Format:	Default:	Entry Method:
NJEUSR(acidname)	N/A	Parameter File TSS MODIFY Command

Operands Description

acidname The ACID that will be used in the VERIFYX call.

2.40.1 General Information

- This ACID will be used for the owner of the JOB or SYSLST data on the Store-and-Forward node and it will have no effect on the userid on the execution node.
- This control option can be included in the startup parms for CA-Top Secret. It needs to be set on the intermediate node where the job or output is being lost, and should be a valid ACID for that node, as well as having access to JES and BATCH. However, no checking is done at the time the NJEUSR is set to make certain that the ACID specified is valid.
- If NJEUSR was changed using a TSS MODIFY command, the changes made remain in effect even if CA-Top Secret is restarted. Most control options revert to their default settings, the exceptions are DUFPGM, PWRNODE and NJEUSR.

2.40.2 Examples

To set the NJEUSR ACID using the TSS MODIFY command enter:

```
TSS MODIFY(NJEUSR(acidname))
```

2.41 NPWRTHRESH

Sets the threshold value for the number of attempts allowed for new password reverification before complete logon sequence needs restarting.

This option is applicable to CICS only.

Format:	Default:	Entry Method:
NPWRTHRESH(nn)	NPWRTHRESH(2) (see Note below)	Parameter of START command or TSS MODIFY command

Operands Description

nn Sets the maximum number, 1 to 99, of retry attempts the user is allowed when attempting new password reverification before complete logon sequence needs restarting.

2.41.1 General Information

Note: NPWRTHRESH control option will not take effect unless the NPWR suboption of the FACILITY control option is added to the TSO or CICS facilities. See the FACILITY control option for details.

2.41.2 Examples

To set the retry password threshold to one using the TSS MODIFY command enter:

```
TSS MODIFY('NPWRTHRESH(1)')
```

2.42 OPTIONS

The OPTIONS control option replaces several optional apars in releases of CA-Top Secret prior to VSE Release 3.0. Any combination of the options listed below can be set by using the appropriate numbers, as indicated. This option can be used only at startup. Multiple OPTIONS statements in the parameter file are supported.

Format:	**Default:**	**Entry Method:**
OPTIONS(n,n)	NONE	Parameter File

Where: **n** represents any number listed below.

Operands	**Description**	**5.0 Fix Number**
1	Honor facility options NOLUMSG and NOSTMSG for administrator ACIDs.	LS11840
2	Do not update LASTUSED information on the security file.	LS38929
3	Disable inbound CPF old/new password verification. This allows gradual implementation of security file synchronization.	LS04865
4	Disable STC PASSCHK=YES. This allows STC's to be defined with passwords without forcing operators to supply a password when the STC is started.	GS81598
5	Allow TSS WHOOWNS without SCOPE checking.	GS95314
6	Suppress the delay after displaying the CA-Top Secret message (for TSO sessions) that can occur before the '***' are displayed.	LS11824
7	Truncate JOBACID at the period. For example, a job from R3.RD1 would be assigned ACID R3 even with JOBACID(R,3).	GS88723
8	For a job from R3.RD1, for example, the ACID used will be R3 instead of R3@RD1.	GS89207
9	Do not abend CA-11 with S913 abend when VTHRESH is reached.	GS89315
10	Stop jobcard scan at col 68 if CA-7 is the submitter.	GS89316

Operands	Description	5.0 Fix Number
11	WTOs are not done under certain facilities. This option allows WTOs to take place if the facility is CICS. Summary messages TSS7100 and TSS7101 will be written to the SYSLOG.	LS33429
12	Make message TSS9208I deletable and rollable on the console.	LS00838
13	Disable implied FETCH access to database in the LIB() keyword of a permit.	GS89920
14	Allow PRIVPGM from any library when no LIB() keyword is on the permit.	LS11835
15	Make message TSS9209I deletable and rollable on the console.	LS00838
16	Support lower case letters, enabling Icelandic and Hebrew characters in the NAME, INSTDATA, and PHYSKEY fields.	LS19775
17	Require operator accountability on ZEOD shutdown of CA-Top Secret.	LS26244
18	Ensure the CICS region ACID is used for all job submit authorizations unless one is supplied through SPOOLWRITE or TRANSIENT DATA interfaces.	LS26245
19	Honor MRO options for IMS regions.	LS26647 LS26644
20	Assign CICS facility DFLTACID for ATS sign on from undefined terminal.	LS33432
21	WTOs are not done under certain facilities. This option allows WTOs to take place if the facility is IMS. Summary messages TSS7100 and TSS7101 will be written to the SYSLOG.	LS33433
22	Force logging if using 4.1 plist for TSSAL.	LS33985
23	Do not do any translation on a TSSUTIL report.	LS34770
24	Audit entire session if terminal is audited.	LS38930
25	Issue abend for invalid control option setting during initialization of CA-Top Secret.	LS26246
26	Disable ACID XAUTH check out of CA-Roscoe exit TSSRXOUT.	LS19963
27	Treat IMS TIMS resource class checks as LCF.	LS38964

Operands	Description	5.0 Fix Number
28	CICS: Use session-life caching.	GS68190/ LS27865
29	CICS: Lock terminal during TSS messages.	GS99164
30	CICS: Last-used stats for ATS.	LS34319
31	CICS: Use LUname on APPL verify signon.	LS34320
41	CICS: Return to CICS Good Morning Transaction after Timeout FORCE.	(VSE Only)

Example: This entry honors facility options NOLUMSG and NOSTMSG for administrator ACIDs and also ignores scope checking on TSS WHOOWNS.

```
OPTIONS(1,5)
```

2.43 PTHRESH

PTHRESH selects a maximum password violation threshold. If the user exceeds the specified threshold by entering the wrong password too many times, CA-Top Secret suspends the ACID.

Format:	Default:	Entry Method:
PTHRESH(nn)	PTHRESH(4)	All

Operands Description

1 to 254 How this number is set determines the number of incorrect passwords a user can enter before CA-Top Secret suspends him.

0 Deactivates password thresholding.

2.43.1 General Information

Rules For Use:

1. Password thresholding only pertains to incorrect passwords. It does not pertain to missing passwords, or new-password specification violations.
2. Each user ACID has an associated invalid password counter.
3. CA-Top Secret counts invalid password attempts from the last valid signon.

2.43.2 Examples

The entry:

```
TSS MODIFY,PTHRESH(2)
```

will produce the RESULT shown below based on the following action.

A user enters an invalid password twice in succession, but successfully signs on on their third attempt.

As a result, CA-Top Secret will reset the counter to 0. If, however, the user enters an invalid password for the third straight time, CA-Top Secret will suspend this user after his third violation.

2.44 PWEXP

PWEXP allows a site to specify a password expiration interval.

Format:	Default:	Entry Method:
PWEXP(nn)	PWEXP(30)	All

Operands	Description
1 to 255	This number will represent the number of days before passwords expire.
0	Implies that the passwords for all new users would never expire.

2.44.1 General Information

- PWEXP is modifiable during CA-Top Secret execution and requires console authority.
- Changing the expiration interval would have no effect on current users; only on ones who have been created after the change.

2.44.2 Examples

The entry:

```
TSS MODIFY,PWEXP(50)
```

would set the default password expiration interval for new ACIDs to 50 days.

2.45 PWHIST

PWHIST specifies the number of previous passwords to be maintained as part of an ACID's password history file. The purpose of the password history is to prevent users from reusing old passwords when their current password expires. CA-Top Secret will always reject new passwords which are identical to any previous password.

Format:	Default:	Entry Method:
PWHIST(nn)	PWHIST(3)	All

Operands Description

nn This number represents the number of past passwords to be maintained for each ACID. It must be a numeric value from 1 to 64.

2.45.1 Examples

The entry:

```
TSS MODIFY,PWHIST(5)
```

would set the number of previous passwords to be maintained for each ACID to five.

2.46 PWRNODE

PWRNODE is used to indicate the name that the local node is known as by POWER. This allows jobs and SYSLST where the submitting node is the local node to be treated differently from NJE jobs and SYSLST originating from other nodes.

Format	Default	Entry Method
PWRNODE(nodename)	N/A	All

Operands Description

nodename Indicates the name of the local POWER node.

2.46.1 General Information

If PWRNODE was changed using a TSS MODIFY command, the changes made remain in effect even if CA-Top Secret is restarted. Most control options revert to their default settings, the exceptions are DUFPGM, PWRNODE and NJEUSR.

2.47 PWVIEW

PWVIEW allows a site to suppress the viewing of users' passwords.

Format:	Default:	Entry Method:
PWVIEW(YES|NO)	PWVIEW(NO)	Parameter File

Operands	Description
YES	Allows the display of passwords if the administrator has the required authority.
NO	No user is allowed to view any passwords.

2.47.1 General Information

- The administrator must have the PWVIEW authority level specified in the DATA parameter of the TSS ADMIN command function.
- This control option must be set separately on every CPU using the CA-Top Secret Security Files.
- PWVIEW can only be set the first time CA-Top Secret is initialized after an IPL. It cannot be reset using the REINIT or MODIFY commands.

2.47.2 Examples

The entry:

```
TSS MODIFY,PWVIEW(YES)
```

will allow an administrator to view the users' passwords within his scope, provided he has been given the PWVIEW-ADMIN authority level.

2.48 RECOVER

Recover indicates whether CA-Top Secret will record changes made to the Security Database onto the Recovery File. Changes include those made automatically by CA-Top Secret (automatic volume ownerships, password changes) and those made by security administrators via the TSS command.

If this option is omitted at CA-Top Secret startup, RECOVER(ON) will be in effect if the CAIRCVF DLBL statement is in the CA-Top Secret started task.

Format:	Default:	Entry Method:
RECOVER(ON | OFF)	RECOVER(ON) If CAIRCVF DLBL statement is in CA-Top Secret start procedure	All

Operands Description

ON Activates the Recovery File. Indicates that changes made to the Security Database will be recorded onto the Recovery File.

OFF Deactivates the Recovery File. Turn Recovery OFF when running the TSSRECVR utility to prevent double recording of changes.

2.49 REFRESH

REFRESH requests that CA-Top Secret reinitialize all CA-SAF modules. Use this option only after new maintenance is applied to the CA-SAF modules.

Format:	Default:	Entry Method:
REFRESH	N/A	ALL

2.49.1 General Information

The REFRESH control option is protected by the Operator Accountability feature. CA-Top Secret will prompt the person entering the command for the proper ACID and password before processing the REFRESH request.

2.50 RESETEOD

RESETEOD allows CA-Top Secret to be restarted, without IPLing, after it has been brought down (accidentally) at the end of a day with a 'Z' stop. Refer to the *Installation* guide for additional information.

Format:	Default:	Entry Method:
RESETEOD	N/A	Console commands only

2.50.1 General Information

End-of-day shutdown prohibits new initiations in all modes. No new users can sign on to any facility, and no new batch jobs can start. When CA-Top Secret is restarted, all control options show up in error, and the system defaults (including the default FAIL mode) are automatically restored.

2.50.2 Examples

To restart CA-Top Secret after an accidental end-of-day shutdown, enter the following series of commands:

```
S TSS

F TSS,RESETEOD

P TSS

S TSS,,,REINIT
```

2.51 RESETSTATS

RESETSTATS is used to reset all counters displayed by the STATS control option to zero.

Format:	Default:	Entry Method:
RESETSTATS	N/A	All

2.51.1 Examples

To reset all counters displayed by the STATS control option, enter the following Modify command:

```
TSS MODIFY,RESETSTATS
```

2.52 RPW

RPW allows the site to modify and list the contents of the Restricted Password list. This allows the site to prevent the use of obvious passwords such as company names, titles, month names, etc.

Format:	Default:	Entry Method:
RPW(LIST) RPW(RESET) RPW(ADD,password,...) RPW(REMOVE,password,..)	See list below	Parameter File or Modify commands

Operands	Description
ADD	Adds one or more password prefix(es) to the restricted password list.
REMOVE	Removes one or more password prefix(es) from restricted password list.
RESET	Removes all password prefixes currently in the restricted password list.
password	One to seven character password prefix.
LIST	Causes CA-Top Secret to display contents of restricted password list. This operand is not protected since it does not alter security.

2.52.1 General Information

The Restricted Password List

TOP SECRET provides a list of a maximum 133 password prefixes, which cannot be used as new passwords. Of the 133 password prefixes, 33 are default entries; 100 entries may be added up to a total of 133. This list is only in effect for NEW passwords that are entered while the NEWPW(RS) control option is in effect.

Refer to the NEWPW control option for details.

Restricted Passwords and Password Prefixes

```
APPL     IBM      PASS
APR      JAN      ROS
ASDF     JUL      SEP
AUG      JUN      SIGN
BASIC    LOG      SYS
CADAM    MAR      TEST
DEC      MAY      TSO
DEMO     NET      VALID
FEB      NEW      VTAM
FOCUS    NOV      XXX
GAME     OCT      1234
```

Capacity of the List

The Table provided by CA may contain up to 133 password prefixes (including the 33 default password prefixes). The site may specify as many RPW control option entries as required.

Protection

Use of the RPW control option is protected by the Accountability Feature. CA-Top Secret will prompt the person entering the command for the authorized ACID/password combination before processing the command.

2.52.2 Examples

To indicate that CA-Top Secret should not accept a set of new passwords if specified by users, enter:

```
TSS MODIFY,RPW(ADD,STAFF1,BATMAN,MYPASSW,MGRPASS)
```

The passwords shown above will no longer be able to be specified as new passwords. Users who are currently using these passwords will function normally.

To remove a password from the list, enter:

```
TSS MODIFY,RPW(REMOVE,BATMAN)
```

BATMAN may now be selected as a new password.

To determine the current contents of the restricted password list, enter:

```
MODIFY(RPW (LIST))
```

2.53 SDTTABLE

SDTTABLE instructs the system to reload either all SDT record types, or only the specified record type, into storage as a refresh.

Format:	**Default:**	**Entry Method:**
SDTTABLE SDTTABLE(type)	N/A	TSS MODIFY commands

The valid record types are:

CALENDAR

MAP

MASK

RLP

SELECT

TIME

2.53.1 General Information

This command is used to refresh tables that have been modified by an administrator.

See the *Command Functions Guide* for more details on the SDT.

2.54 SECTRACE

SECTRACE activates a diagnostic security trace on the activities of all defined users or of specific users.

Format:	Default:	Entry Method:
SECTRACE(WTO|WTL|OFF) SECTRACE(ACT,WTO|WTL)	OFF	All

The following operands will trace the jobs of ALL defined users.

Operands Description

WTO Activates the trace, and routes messages to the master console for all users and events.

WTL Activates the trace and routes messages to the SYSLOG (system log). Use with the ACT operand.

ON Activates global trace.

OFF Deactivates diagnostic tracing. This is an installation default. OFF is only used as a default when a command is not specified in the parmlib.

ACT Activates the trace for users that have the TRACE attribute attached to their ACIDs. Refer to the TSS ADDTO command for for instructions on how to add the TRACE attribute. ACT must be specified with WTL or WTO in this format:

```
SECTRACE(ACT,WTL|WTO)
```

Destinations of Trace Messages: in TSO, trace information always goes to both the terminal and SYSLOG.

The following operands indicate the possible destinations of the trace messages.

Operands Description

WTO To the master console

WTL To SYSLOG

2.54.1 General Information

The SECTRACE control option is usually issued at the request of CA Technical Support.

TRACE messages use the following prefixes:

TSS-I for initiations.
TSS-E for terminations.
TSS-C access validation done through RACHECK.
TSS-D access validation done through RACDEF.
TSS-F access validation done through FRACHECK.
TSS-T TSS command.
TSS-V PWR Early Verify Password support.

2.55 SHRFILE

SHRFILE specifies whether files used by CA-Top Secret are shared among other operating systems and/or CPUs.

Format:	Default:	Entry Method:
SHRFILE(YES|NO|SECURITY)	SHRFILE(YES)	All

Operands	Description
YES	Specifies that all of the files used by CA-Top Secret will be shared among other operating systems and/or CPUs.
NO	Specifies that no files will be shared between CA-Top Secret and other operating systems and/or CPUs. The LOCK records on the Security and Audit Files are obtained at startup and never released, totally eliminating all I/O required for lock record processing in a single CPU environment.
SECURITY	Specifies that CA-Top Secret will perform lock processing on the Security File (and subsequently on the Recovery File), but will not perform lock processing on the Audit File. Audit File processing will be handled as if SHRFILE(NO) had been specified. If a user starts sharing either the Security or Audit File without changing the control option, then any other CPU will not be able to obtain that File's lock, thereby eliminating accidental file corruption. Example:

```
SHRFILE(YES)
```

indicates that all of the files used by CA-Top Secret will be shared among other operating systems and/or CPUs.

2.56 ST

ST produces a display that combines the information produced for the VERSION, STATUS, and STATS control options.

Format:	Default:	Entry Method:
ST	N/A	TSS MODIFY

There are no operands for the ST control option.

2.56.1 General Information

Refer to the VERSION, STATUS, and STATS control options, for examples of information displayed in response to the ST command.

2.56.2 Examples

To determine complete information about the security control status at his installation, the SCA would enter:

```
TSS MODIFY(ST)
```

from an online terminal.

2.57 STATS

STATS displays numeric counts concerning CA-Top Secret security processing.

Format:	Default:	Entry Method:
STATS	N/A	O/S or TSS MODIFY commands only

2.57.1 General Information

STATS generates a console display identified by messages in the TSS95xxI series.

STATS produces a display showing the number of:

- Job initiations validated.
- Cross-memory requests processed.
- Security calls processed.
- SMF security records logged.
- Program executions validated.
- CACHE statistics processed.
- Changes made to the Security File.
- Changes saved in the Recovery File.
- Security File input requests made.
- Security File output operations since IPL on this CPU.
- Audit events recorded in the Audit/Tracking File.

2.58 STATUS

STATUS provides the current settings of various control options. You can specify which option you would like to display when you enter a TSS MODIFY(STATUS) command. Since only one option at a time is entered, the options are listed in the sequence in which you specify them. The default is STATUS(BASE,JES,PASSWORD,FACMODE,CPF)

Format:	Default:	Entry Method:
STATUS(option)	(see default above)	ALL

Operands	Description
BASE	Shows bases systrem and miscellaneous control options.
VERSION	Includes the system version in the output.
FACMODE	Shows facility modes.
PASSWORD	Shows password-related control options.
CPF	Shows CPF-related control options.

Note: The CPF option will display everything that the CPFSTAT control option formerly provided.

2.58.1 General Information

The options listed in the STATUS control option can be in any order, and the output will be presented in the order used in the control option.

The TSS MODIFY(STATUS) command can now include a single option to display only that information requested, or to acquire information not set in the STATUS control option. For example, the TSS MODI(STATUS(CPR)) will show the CPR information.

The output of the TSS MODIFY(STATUS) command has headers in both upper and mixed case. Any header in mixed case denotes information not set by a control option but rather derived from the system.

2.58.2 Examples

To determine complete information about the various CPF control options, as well as the current status of CPF and the nodes defined to it, the SCA would enter:

```
TSS MODIFY(STATUS(CPF))
```

2.59 SUBACID

SUBACID indicates how CA-Top Secret will derive an ACID for batch jobs that are submitted by the following methods:

- through an online terminal
- from another batch job
- from a started task.

Format:	Default:	Entry Method:
SUBACID(J,n) SUBACID(U,n)	SUBACID(U,7)	All

Operands **Description**

SUBACID(J,n) Indicates that the first 'n' characters of the jobname parameter on the job card will be used as the ACID, unless 'USER=acid' is present.

Specifying SUBACID(J,7) will cause restriction of jobnames to the user's userid plus one character. This will occur unless the user is explicitly PERMITted to submit other ACIDS.

SUBACID(U,n) Indicates that the first 'n' characters of the logged on user's ACID, or of the ACID associated with the started task, will be used as the ACID for the batch job.

2.59.1 General Information

Application of SUBACID

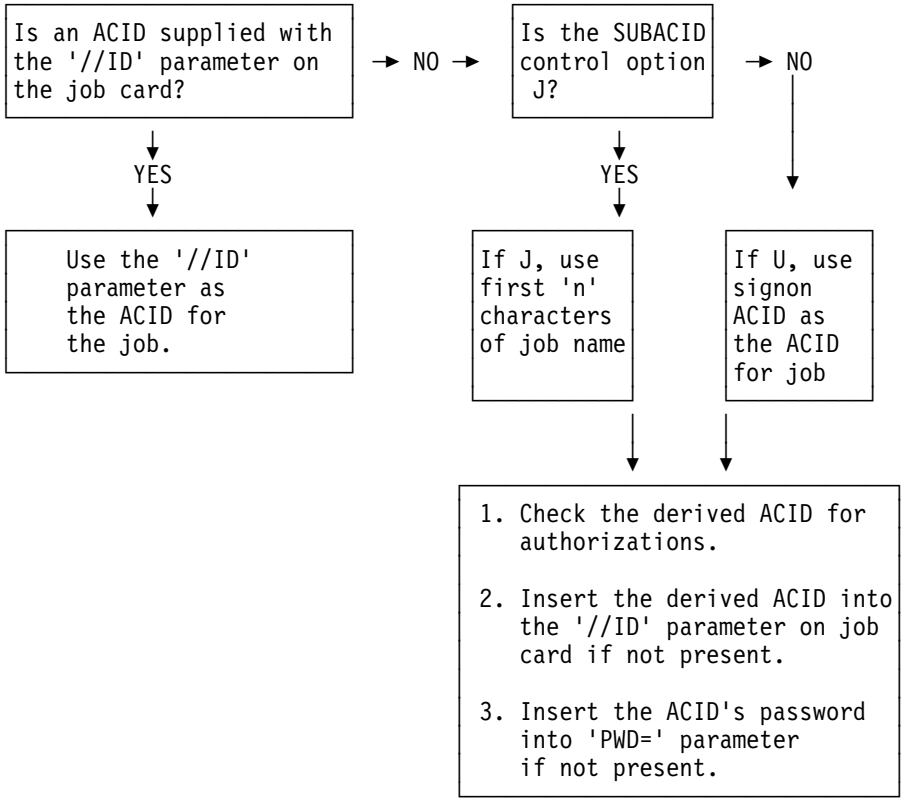
SUBACID only applies to jobs issued through an internal reader. It does NOT apply to jobs submitted via remotes, nodes, or local readers.

CA-Top Secret uses settings for the JOBACID and DEFACID control options to derive ACIDS for jobs issued from physical card readers or NJE and RJE remote readers. Refer to the JOBACID control option or the DEFACID suboption of the FACILITY control option for details.

SUBACID Algorithm

The following algorithm assumes that the JES control option is set to JES(NOVERIFY).

This indicates that the JES Early Verify feature is not in effect. In FAIL mode, all jobs must have an ACID in order to be processed by CA-Top Secret. CA-Top Secret uses the algorithm shown in the figure that follows to derive an ACID for a batch job received through an internal reader.



CA-Top Secret algorithm for jobs.

2.60 SUSPEND

SUSPEND allows an operator to suspend any ACID, thus preventing a user from gaining access to the system.

Format:	Default:	Entry Method:
SUSPEND(acid)	N/A	TSS MODIFY commands only

Operands	Description
acid	The ACID being suspended.

2.60.1 General Information

The SUSPEND option may be used whenever a particular user is suspected of subversive activity. The operations staff may then act quickly to suspend a suspicious user, without waiting for a security administrator to issue the option.

The user must still be cancelled from the system, but once cancelled, the user's ACID is invalid until unsuspended.

The SUSPEND option cannot be used to unsuspend a user.

2.61 SVCDUMP

SVCDUMP produces a system dump of the CA-Top Secret region.

Format:	Default:	Entry Method:
SVCDUMP	N/A	TSS MODIFY commands only

2.61.1 General Information

The SVCDUMP option is primarily provided to aid in CA-Top Secret problem determination. An unformatted dump of the CA-Top Secret region is written to an available SYS1.DUMPxx data set.

2.62 SYNCH

SYNCH requests immediate synchronization of global in-memory tables (ALL, AUDIT, RDT, STC) with the Security File.

SYNCH is usually only required for processors in global DORMANT mode.

Format:	Default:	Entry Method:
SYNCH	N/A	O/S or TSS MODIFY commands only.

There are no operands for the SYNCH control option.

2.62.1 Examples

To synchronize in-memory tables (ALL, STC, AUDIT) with the security file, enter the modify TSS command:

```
TSS MODIFY(SYNCH)
```

2.63 TAPE

TAPE specifies the type of tape protection (if any) in effect at the installation.

Format:	Default:	Entry Method:
TAPE(OFF|DSN)	TAPE(OFF)	All

Operands	Description
OFF	VSE will not invoke CA-Top Secret to validate a tape access request. TAPE(OFF) is used to indicate the use of external tape management packages such as CA-DYNAM/T.
DSN	CA-Top Secret will perform data set name checking using the full data set name supplied on the DSN keyword of the JCL.

2.63.1 General Information

Appropriate Settings for TAPE Option

- Set TAPE(OFF) for CA-DYNAM/T
- Set TAPE(DSN) for CA-EPIC or CA-Tape Manager.

Refer to the *User Guide* for detailed descriptions of volume security, and tape data set security.

2.63.2 Examples

Enter:	To:
TAPE(DSN)	Use CA-Top Secret to protect tape data sets
TAPE(OFF)	To indicate the use of a DYNAM interface
TAPE(DSN)	To use CA-EPIC or CA-Tape Manager

2.64 TEMPDS

TEMPDS allows an installation to determine whether or not temporary data sets will be protected.

Format:	Default:	Entry Method:
TEMPDS(YES|NO)	NO	All

Operands Description

YES Indicates that temporary data sets are treated like any other data set and users must be permitted to access them. For example:

```
TSS PER(ALL)  DSN(SYS9++++.T++++++.RA) ACC(ALL)
```

authorizes users to have ALL access to temporary data sets with the prefix SYS in the ALL Record. These data sets can be audited.

NO Indicates that temporary data sets are not protected, and cannot be audited.

2.64.1 Examples

The entry:

```
TSS MODIFY(TEMPDS=NO)
```

indicates that temporary data sets are not protected and, consequently, cannot be audited.

2.65 TEXTTSS

TEXTTSS allows for replacement of the string 'CA-Top Secret SECURITY' in reports and messages. Any string up to 19 characters may be used.

Format:	Default:	Entry Method:
TEXTTSS(replacement text)	CA-Top Secret SECURITY	All

Operands **Description**

replacement text

The 19 character string which will replace the words "CA-Top Secret SECURITY" in reports and messages.

Note: This is the only control option that allows spaces between words.

2.65.1 Examples

An entry in the parameter file such as:

```
*
* sample control options
*
TSS MODIFY('TEXTTSS(CAI ACCESS CONTROL)')
```

would cause startup message TSS9000I to be displayed as:

```
TSS9000I CAI ACCESS CONTROL INITIALIZATION COMPLETE.
```

2.66 TIMER

TIMER controls the interval at which data is written from CA-Top Secret buffers to the AUDIT/TRACKING file. This includes writing IMS and CICS transaction events to SMF.

Format:	Default:	Entry Method:
TIMER(nnn)	TIMER(15)	All

Operands Description

nnn Time interval from 10 seconds to 300 seconds.

2.66.1 Examples

To force CA-Top Secret to write from CA-Top Secret buffers every 45 seconds, enter:

```
TSS MODIFY,TIMER(45)
```

2.67 TNGMON

TNGMON is used to set and activate error messages sent to a Unicenter console.

Format:	Default:	Entry Method:
TNGMON (ON|OFF) TNGMON (ADD|REMOVE, ip address[,DEBUG]),	NONE	All

Operands **Description**

ON Enables the TNG monitor to send error messages to a Unicenter console.

If the monitor is on, and there are no TNG monitor table entries, the monitor does not process any data. The same is true, if the table has entries but monitor is off.

OFF Disables the TNG monitor from sending error messages to a Unicenter console.

ADD Indicates that a new IP address will be added to the TNG monitor table.

CA-Top Secret will not allow duplicate entries to the TNG monitor table. If an entry is added that already exists, CA-Top Secret recognizes its existence and returns a MODIFY FUNCTION SUCCESSFUL.

REM Indicates that an IP address will be removed from the TNG monitor table.

If you remove the last entry in the TNG monitor table, and the internal-used entry count is set to zero, the TNG monitor is placed in an off status, automatically.

Note: The REM function used with DEBUG, only removes the DEBUG function but not the IP address.

ip address Identifies the PC address for which CA-Top Secret violations are sent.

DEBUG Enables the the TNGMON control option to perform troubleshooting diagnostics. This function should only be used when requested by CA Technical Support.

If the IP address is already in the TNG monitor table without the DEBUG function, you may add it with the following command:

```
TNGMON(ADD,ip address,DEBUG)
```

2.67.1 General Information

You can identify one or many Windows NT machines as Unicenter TNG monitors. However, you can also identify other Unicenter TNG monitors from within Unicenter TNG.

There are advantages and disadvantages to both methods. Here are some important considerations:

- Sending error messages to multiple Unicenter monitors affects the performance of your system and increases work traffic. Identifying multiple Unicenter TNG monitors ensures that you will always have at least one Unicenter TNG monitor up and running.
- Identifying additional Unicenter monitors from within Unicenter TNG is easy, and it lets you create filters and calendars to route error messages more efficiently. For more details, refer to the *Getting Started Guide* for CA-Top Secret/WS.

2.68 TSS

CA-Top Secret allows the security administrator to enter TSS commands at the console. Refer to the CA-Top Secret *Command Functions* guide for a description of all TSS command functions and keywords.

Format:	Default:	Entry Method:
TSS	N/A	TSS MODIFY

2.68.1 General Information

Protection

The TSS control option is protected by a special prompt for the MSCA's previous password. A record of the event will be recorded to provide an audit trail.

TSS Command Format

TSS commands may be entered in free format. Output is restricted to 50 lines so as not to flood the console with a long output response.

2.68.2 Examples

To enter a TSS command function at the O/S console, use the following procedure:

1. Enter F TSS, TSS
2. The system will display:

```
TSS9691A ENTER TSS COMMAND PASSWORD
```

3. Enter the MSCA's previous password:

```
xx, password
```

4. If this password is correct, the system will display:

```
TSS9690A ENTER <TSS COMMAND> OR <END>
```

5. Enter the TSS command function as shown below:

```
xx, TSS COMMAND(acid) KEYWORD(operand)
```

6. Ensure that TSS is included in the command entry:

```
TSS ADD(USER01) DSN(ABC.DEF)
```

2.69 VERSION

VERSION displays CA-Top Secret's version.

Format:	Default:	Entry Method:
VERSION	N/A	O/S or TSS MODIFY commands only

2.69.1 Examples

Entering:

```
F TSS,VERSION
```

will result in the following message:

```
TSS9660I VERSION=50yymmAKOnn
```

where 50 is the Release, yymm is the CA-Top Secret Genlevel, KO is the Product Code and nn is the version.

2.70 VSAMCAT

CA-Top Secret offers a control option that allows sites to bypass user catalog volume checks on VSAM data set creation.

During VSAM data set creation, VSE passes the volume number of the user catalog, rather than the volume(s) where the data set is going to be located. This necessitates permitting CREATE access to the user catalog volume although the data set will not be placed there.

Specifying VSAMCAT(NO) will skip the volume checking; data set checking will occur unchanged. This setting eliminates the need to grant users the authority to create data sets on the catalog volume. Specifying the default VSAMCAT(YES) will continue to enforce checking the user for CREATE access to the user catalog.

2.71 VTHRESH

VTHRESH performs two functions. This option selects an access violation threshold for online users, batch jobs, and started tasks, and selects the action that CA-Top Secret will take when the threshold is reached.

Format:	Default:	Entry Method:
VTHRESH(nn,[NOT],[CAN],[WARN]) [SUS] [CAN],[WARN] [RES]	(5,NOT)	All

Operands Description

nn Sets the maximum number, from 0 to 254, of resource access violations that a user may accumulate during an online session or job execution. This operand must be specified when changing any of the action operands. Specifying a value of 0, signifies that no violation threshold processing will be performed.

NOT CA-Top Secret issues a message at the security console and the user's terminal to notify the security administrator of a security violation.

For online sessions: CA-Top Secret will prevent further access of any kind by locking the terminal. This forces the user to sign off.

CA-Top Secret will issue the message:

```
TSS7192E SESSIONL LOCKED - EXCESSIVE VIOLATIONS: SIGNOFF
```

For CICS online sessions, CA-Top Secret will cancel the session and issue the following messages:

```
TSS7191E JOB/SESSION CANCELLED EXCESSIVE VIOLATIONS
TSS7192E SESSIONL LOCKED - EXCESSIVE VIOLATIONS: SIGNOFF
```

SUS For online sessions: CA-Top Secret will prevent further access of any kind. This forces the user to sign off.

RES Resets actions SUS, CAN or WARN to NOT.

CAN CA-Top Secret will prevent further access of any kind by locking the terminal. This forces the user to sign off. CA-Top Secret issues the message:

TSS7192E SESSIONL LOCKED - EXCESSIVE VIOLATIONS: SIGNOFF

For CICS online sessions: CA-Top Secret will cancel the session and issue following messages:

TSS7191E JOB/SESSION CANCELLED EXCESSIVE VIOLATIONS
TSS7192E SESSION LOCKED - EXCESSIVE VIOLATIONS: SIGNOFF

WARN Indicates that CAN and SUS will be enforced for users operating in WARN mode as well as in FAIL or IMPL.

2.71.1 General Information

The VTHRESH option is in effect during WARN, FAIL, and IMPL modes. CA-Top Secret will not, however, SUSpend or CANcel violators during WARN mode unless VTHRESH(WARN) is set.

TSO users who reach the VTHRESH limit while in ISPF browse or edit will not be suspended or cancelled until they leave the screen. VTHRESH operands are not in effect when TSS LOCK is active. You must specify TSS UNLOCK first. Then the VTHRESH options take effect after the next user action. If you want to change the SUSPEND suboption to CANCEL, you must specify the RES suboption first. This resets SUS and CAN actions to NOT.

2.71.2 Examples

To suspend the ACID of any user who logs 3 or more violations enter:

```
TSS MODIFY,VTHRESH(3,SUS)
```

To change the number of resource access violations to 6, but keep everything else the same, enter:

```
TSS MODIFY,VTHRESH(06)
```

Index

R

S

T

U

V

User Registration Form

If you are interested in registering as a user of Computer Associates software, please complete the information below. Send it to the following address:

Computer Associates International, Inc.
ATTN: User Registration
One Computer Associates Plaza
Islandia, NY 11749

Registration entitles you to receive such items as:

- newsletters
- product release announcements
- information about User Groups
- information about CA conferences
- client questionnaires

You *do not* have to be the primary contact for CA software within your company or organization. All you have to be is interested in CA software, how it is used, and where it is headed.

Product(s): _____

_____

_____

_____

Site ID: _____
(Enter UNKNOWN if you do not know your Site ID.)

Name: _____

Position: _____

Company or organization: _____

Address: _____

Address: _____

Phone No.: _____

Date: _____

I would like additional information on: _____

Demand Analysis Request Form

Please use this form to make suggestions for product improvement. Send it to the following address.

Computer Associates International, Inc.
ATTN: Demand Analysis Requests
One Computer Associates Plaza
Islandia, NY 11749

Be sure to print your name and address below if you would like a reply.

Name: _____

Position: _____

Company or organization: _____

Address: _____

Address: _____

Phone No.: _____

Date: _____

Is DAR from a User Group? (Yes/No) ___ User Group ID: _____

Priority: _____

Description of Requested Item:

_____

_____

_____

_____

_____

_____

_____

_____

_____

CA Account Manager:	CA Office:
Input by:	Date:

Reader Comment Form

CA-Top Secret Control Options Guide

Release 3.0 VSE

Document Number: R101TS30COE

Please use this form to tell us how you use this manual and to make suggestions for improvement. Send it to the following address. (To request additional publications, call 1-800-841-8743 or check the CA home page (http://www.cai.com) on the Internet. To ask questions about the functionality of CA products, contact your CA representative.)

Computer Associates International, Inc.
ATTN: Reader Comment Form
One Computer Associates Plaza
Islandia, NY 11749

Be sure to print your name and address below if you would like a reply.

Name: _____

Position: _____

Company or organization: _____

Address: _____

Address: _____

Phone No.: _____

Date: _____

Years of experience with this CA product: _____

Overall Rating

	Good	Fair	Poor	Why?
Accuracy				
Organization				
Clarity				

Reference Aids

	Good	Fair	Poor	Why?
Contents				
Index				
Glossary				
Reference to Other Manuals				

Clarity

	Good	Fair	Poor	Why?
Instructions and Procedures				
Examples				
Graphics				

How Manual Is Used:

How do you use this manual in your job?

How often do you use this manual in a week?

Suggestions:

What do you like about this manual?

What do you dislike about this manual?

What would you like us to change?

Additional Comments: