

CA-Top Secret[®]

Messages and Codes Guide
Release 3.0
VSE



This documentation and related computer software program (hereinafter referred to as the "Documentation") is for the end user's informational purposes only and is subject to change or withdrawal by Computer Associates International, Inc. ("CA") at any time.

THIS DOCUMENTATION MAY NOT BE COPIED, TRANSFERRED, REPRODUCED, DISCLOSED, OR DUPLICATED, IN WHOLE OR IN PART, WITHOUT THE PRIOR WRITTEN CONSENT OF CA. THIS DOCUMENTATION IS PROPRIETARY INFORMATION OF CA AND PROTECTED BY THE COPYRIGHT LAWS OF THE UNITED STATES AND INTERNATIONAL TREATIES.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENTATION "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO THE END USER OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED OF SUCH LOSS OR DAMAGE.

THE USE OF ANY PRODUCT REFERENCED IN THIS DOCUMENTATION AND THIS DOCUMENTATION IS GOVERNED BY THE END USER'S APPLICABLE LICENSE AGREEMENT.

The manufacturer of this documentation is Computer Associates International, Inc.

Provided with "Restricted Rights" as set forth in 48 C.F.R. Section 12.212, 48 C.F.R. Sections 52.227-19(c)(1) and (2) or DFARS Section 252.227.7013(c)(1)(ii) or applicable successor provisions.

Second Edition, September 2000

©1985-2000 Computer Associates International, Inc.
One Computer Associates Plaza, Islandia, NY 11749
All rights reserved.

All trademarks, trade names, service marks, or logos referenced herein belong to their respective companies.

Contents

About This Guide	v
Chapter 1. TSS Messages	1-1
1.1 CA-Top Secret Messages	1-2
Chapter 2. CAS Messages	2-1
2.1 CAS20 System Authorization Facility (SAF) Messages	2-2
2.1.1 Security Initialization Routine	2-3
2.2 CAS22 SAF Common Service Routines	2-4
2.3 CAS3 Common Record-Level Protection Routines	2-10
Chapter 3. Codes	3-1
3.1 Detailed Reason Codes	3-2
3.1.1 Reserved DRCs	3-2
3.1.2 Conventions	3-2
3.1.3 Detailed Reason Codes	3-3
3.1.4 DRC To Message Cross-Reference	3-17
3.2 TSSMAINT Abend Codes	3-24
3.2.1 TSSUTIL Abend Codes	3-25
3.2.2 TSSRECVR Abend Codes	3-26
3.2.3 TSSTRACK Abend Codes	3-26
3.2.4 TSSAUDIT Abend Codes	3-27
3.2.5 TSSCHART Abend Codes	3-27
3.2.6 TSSXTEND Abend Codes	3-28
3.2.7 TSSFAR Abend Codes	3-29
3.2.8 CICS Abend Codes	3-31
3.2.9 IBM CICS Abend Codes	3-33
User Registration Form	-URF-1
Demand Analysis Request Form	-DAR-1
Reader Comment Form	-RCF-1

About This Guide

Purpose

This guide defines all abend codes, error codes, and information messages that may be encountered while using CA-Top Secret.

The majority of *Messages and Codes* can be understood by all users. Some explanations, however, may contain terminology familiar only to system programmers.

Organization

Chapter	Description
1	Contains all CA-Top Secret messages.
2	Provides the System Authorization Facility (SAF) messages.
3	Describes all detailed reason codes, CA-Top Secret abend codes, operating system messages and abend codes, and miscellaneous IBM messages and codes.

CA-Top Secret Publications

The following publications are supplied with CA-Top Secret:

Title	Contents
<i>Installation Guide</i>	CA-Top Secret installation for VSE, including: installation and maintenance steps, startup and shutdown considerations, backup and recovery procedures, and Security File conversion.
<i>Command Functions Guide</i>	Comprehensive reference to the TSS command and CA-Top Secret resources.
<i>Control Options Guide</i>	Comprehensive reference of CA-Top Secret control options.
<i>Implementation: BATCH, STC and APPC Guide</i>	Provides for setting up security in Batch, STC and APPC environments.
<i>Implementation: CICS Guide</i>	Provides for setting up security in a CICS environment.
<i>Messages and Codes Guide</i>	Provides all CA-Top Secret messages and codes.
<i>Planning Guide</i>	General guide for planning a successful CA-Top Secret security implementation and describing the latest enhancements to CA-Top Secret.
<i>Report and Tracking Guide</i>	Details the use of TSSUTIL, TSSTRACK, TSSAUDIT, TSSCFE and TSSCPR and provides sample reports.
<i>Troubleshooting Guide</i>	Includes CA-Top Secret debugging options and facilities, information to be prepared prior to contacting Technical Support, and an explanation of customer support.
<i>User Guide</i>	Conceptual overview of CA-Top Secret architecture and capabilities. 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
<i>CA-EARL Reference Guide</i>	MVS/VM/VSE
<i>CA-EARL User Guide</i>	MVS/VM/VSE
<i>CA-EARL Systems Programmer Guide</i>	VSE
<i>CA-EARL Examples Guide</i>	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.
<u>underlining</u>	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.

Message Conventions

For the sake of organization and clarity, messages and codes explained in this guide follow certain conventions and abbreviations.

- CA-Top Secret message numbers have three main components:



Where:

- 1** The CA-Top Secret message prefix
- 2** The message number
- 3** The message suffix letters. One of these letters is given at the end of each message to indicate the type of message:
 - I** Informational messages
 - E** Error messages, issued if CA-Top Secret is in FAIL mode.
 - W** Warning messages, issued if CA-Top Secret is in WARN mode.
 - A** Action messages, which indicate the user must perform some action as indicated in the message text.

- The text of the messages is in all capital letters, except for places where CA-Top Secret supplies information. Lowercase words (such as resource, acid, and so on) indicate that CA-Top Secret will fill in the appropriate information.
- Numbered messages are listed in numerical order.
- Unless it is self-explanatory, each message lists the reason the violation or warning was issued, along with any applicable corrective action.
- A vertical bar indicates that one of the listed options is displayed in the message.
- Characters enclosed by the less-than sign, <, and the greater-than sign, >, indicate a necessary user response.

For example, the message

TSS7187A REPLY <Y> TO CONFIRM LOGON. ELSE <N> TO DENY USE OF MSCA ACID.

indicates that the user must enter "Y" or "N."

Note: The SAF SECTRACE Reporter messages (TSS41022 through TSS9C000) differ from the standard CA-Top Secret message convention in that they do not have a suffix letter.

Abbreviations

The following abbreviations may appear in the text of messages and codes shown in this guide:

acid	A CA-Top Secret accessor id
alevel	Access level requested by the user
cicsresource	A CICS resource class
cmd	Command
d	DOWN option
dsname	Data set name
drc	Detailed Reason Code
f	Name of facility
hh	Hour (as in time)
level	An access level, that is, READ, UPDATE, CREATE, etc.
mm	Minutes (as in time)
nn	Numeric value
pgmname	Program name
reader	The logical name of a reader
resclass	The resource class
resname	The actual name of the resource
ss	Seconds (as in time)
stc	Specific started task
tssfunc	A CA-Top Secret function or command
userid	A logon/signon user id
volser	Volume name or serial number
XACTN	A transaction

Chapter 1. TSS Messages

This guide lists all the CA-Top Secret VSE messages. CA-Top Secret violation and warning messages appear only if the LOG/MSG Control Option is in effect.

1.1 CA-Top Secret Messages

TSS0000I CA-Top Secret is Activating

Reason: The CA-Top Secret address space is activating.

Action: None.

TSS0001I TSS CVT loaded at xxxxxxxx

Reason: Informs Operator where the CA-Top Secret Control Vector table has been loaded.

Action: None. The information is useful for debugging purposes.

TSS0010I Stating Security File Services (SFS)

Reason: The CA-Top Secret I/O subsystem is initiating.

Action: None.

TSS0017I Recovery file wrapped around

Reason: The Security Recovery file has wrapped around, causing oldest recovery records to be lost.

Action: This is a normal event, if the message appears more often than the system backup, then the recovery file should be expanded.

TSS0024I Security file serialization has been delayed

Reason: During startup of the I/O subsystem, CA-Top Secret attempts to lock the Database. Something caused the lock to wait more than 1 second to succeed.

Action: None. This can happen on a I/O intensive system or during periods of high cpu useage.

TSS0025I Enqueue table full - enqueue waiting

Reason: Too many tasks have queued up for enqueue of the CA-Top Secret database.

Action: None. The system will clear the situation out and resume operation.

TSS0040W Security file encryption unavailable

Reason: CA-Top Secret was unable to locate a valid security key in TSSKPTRC.

Action: Apply a new encryption key, using the TSSKEY.Z copybook.

TSS00041E Customer key required to unlock file

Reason: The CA-Top Secret database is locked by another system, and CA-Top Secret was unable to find a valid encryption key in TSSKTPRC.

Action: Apply a new encryption key using TSSKEY.Z copybook, or enter a temporary key.

TSS0042A Specify <ABORT>; Else 16 hex digit key

Reason: TSS was unable to locate a valid key in TSSKTRPC and now wants to know what action to take.

Action: Either ABORT the job, or enter a valid Temporary 16 Hex Digit key, such as 1111111222222222.

TSS0043W Key is temporary - Zap required

Reason: A temporary encryption key was entered and needs to be made permanent.

Action: Enter the same key in TSSKEY.Z copybook and zap module TSSKTPRC with it.

TSS0044E Invalid Hex digit in key

Reason: Parts of the key entered was not in hexadecimal format (Between value 1 and F).

Action: Enter a new key using valid hexadecimal numbers.

TSS0050E Security file services (SFS) failed

Reason: The CA-Top Secret I/O subsystem failed to initiate properly.

Action: See following messages, or contact CA-Top Secret Technical Support.

TSS0090I Taskid; xxxxx Cancel-Code: xxxxx

Reason: Issued as a part of subsystem cancel, listing what task canceled and the cancel code.

Action: Report to CA-Top Secret Technical Support Center.

TSS0091I PSW: xxxxxxxx xxxxxxxx

Reason: Program status word (PSW) of failing program.

Action: Report to CA-Top Secret Technical Support staff.

TSS0092I Regs xx - xx xxxxxxxx xxxxxxxx xxxxxxxx xxxxxxxx

Reason: Register values of failing program.

Action: Report to CA-Top Secret Technical Support staff.

TSS0100I SFS is starting (TID=xxx EP=xxxxxxxxx)

Reason: Informs operator about the Taskid and Entry point address of I/O subsystem.

Action: None. Useful for possible debugging.

TSS0101I SFS resident tables build

Reason: The I/O subsystem has completed reading and building various incore tables.

Action: None. Informational only.

TSS0102I SFS I/O queue is open

Reason: The I/O subsystem is now ready to accept work.

Action: None.

TSS0103I SFS is active

Reason: The I/O subsystem is now completely initialized

Action: None.

TSS0110E SFS is already active

Reason: An attempt was made to start an additional I/O subsystem.

Action: System will fail second startup attempt. If error occurs and no other CA-Top Secret tasks are active, then system must be replied to clear possible corrupt storage buffers.

TSS0111E SFS unable to obtain storage for RSAs

Reason: Insufficient Partition getvis or system getvis storage is available.

Action: Increase allocated sizes and reattempt to start CA-Top Secret.

TSS0112E SFS unable to obtain storage for WS

Reason: Insufficient partition getvis storage.

Action: Increase storage size allocated to CA-Top Secret address space and/or correct EXEC size.

TSS0113E SFS file initialization failed

Reason: Some other event caused I/O system to fail.

Action: See previously issues error messages, correct problem and re start, contact CA-Top Secret Technical Support.

TSS0114E SFS I/O request queue initialization failed

Reason: I/O subsystem was unable to initialize its command queues.

Action: Check other Error messages, check sufficient Getvis and/or SVA storage availability, contact CA-Top Secret Technical Support.

TSS0115E SFS recursive QGET failures

Reason: Possible corruption of I/O subsystem request queue.

Action: Dump SVA and CA-Top Secret address space to tape or cart using DUMP command. Contact CA-Top Secret Technical Support.

TSS0116E Abend occurred in QGET

Reason: Possible coding logic error or storage corruption in I/O sub system.

Action: Collect produced dumps and contact CA-Top Secret Technical Support.

TSS0117E SFS error in function xxxxxxxx, RC=xx

Reason: Severe logic error occurred in I/O subsystem.

Action: Collect possible dump and output, contact CA-Top Secret Technical Support.

TSS0118I SFS found label for xxxxxxxx on volume xxxxxxxx.

Reason: Informs Operator where CA-Top Secret databases are located and what DASD volumes they reside on.

Action: Useful information used to check that DLBL or STDLABEL area points to correct datasets.

TSS0119E SFS label information missing for xxxxxxxx

Reason: I/O subsystem attempted to locate needed dataset, but did not find it.

Action: Correct STDLABEL or DLBL statements ensure files are initialized with TSSMAINT or other utility.

TSS0120E SFS device error on volume xxxxxx

Reason: I/O subsystem detected error on specific device.

Action: Restart CA-Top Secret and check if hardware is malfunctioning; contact CA-Top Secret Technical Support.

TSS0121E GETAREA failed building xxxxxxxxxx

Reason: Insufficient Partition of getvis or SVA storage during the build of table xxxxxxxx caused the build to fail.

Action: Increase storage, contact CA support for information about what storage area table XXXXXXXX would be located in.

TSS0122E QGET error - zero pointer to QDCB

Reason: Internal error in I/O subsystem command processor queue.

Action: Dump the System and SVA, contact CA-Top Secret Technical Support personnel.

TSS0123I Deleting current RDT record

Reason: CA-Top Secret is in the process of rebuilding the RDT and deletes the current table first.

Action: None, this is a normal process.

TSS0124I Building default RDT/FDT record

Reason: CA-Top Secret is creating a new RDT/FDT record in the database.

Action: None, this is a normal process.

TSS0125I Open processing successful for XXXXXXXX

Reason: CA-Top Secret successfully opened a dataset called XXXXXXXX.

Action: None.

TSS0126E Open processing failed for XXXXXXXX

Reason: CA-Top Secret was unable to open dataset XXXXXXXX.

Action: Check if file has been created with the TSSMAINT utility or allocated on the specified DASD. Contact CA-Top Secret Technical Support personnel.

TSS0127I Close processing completed for XXXXXXXX

Reason: CA-Top Secret successfully closed dataset XXXXXXXX.

Action: None.

TSS0128E ESTAE failed - RC=xxxxxxxx

Reason: Internal abend handler routine failed with RC.

Action: Contact CA-Top Secret Technical Support personnel about RC.

TSS0129W Waiting for system getvis storage

Reason: Insufficient System getvis storage, system is waiting for storage to be released or available.

Action: Increase System getvis area.

TSS0190E Fatal Error occurred in program XXXXXXXX

Reason: A program check or other error occurred in program XXXXXXXX.

Action: Collect Dumps, console output and contact CA-Top Secret Technical Support.

TSS0198I SFS shutdown was requested

Reason: I/O subsystem has been posted to shutdown processing.

Action: Normal during shutdown of CA-Top Secret address space.

TSS0199I SFS has terminated

Reason: I/O subsystem has completed its shutdown.

Action: None. Normal processing.

TSS0200E TSS COMMAND ENVIRONMENT ERROR

Reason: The TSS command cannot be initiated due to an VSE environment error. Two common reasons for an VSE environment error are insufficient storage for the LOAD and the TSS command is contained in a non-APF authorized library.

Action: You should increase your storage size.

TSS0201E CA-TOP SECRET IS NOT ACTIVE

Reason: TSS commands cannot be processed if the CA-Top Secret address space is inactive.

Action: Determine why the CA-Top Secret address space has not been initialized. To start CA-Top Secret, use the EXEC PROC=TSS command.

TSS0202E YOU ARE NOT AUTHORIZED TO USE THE TSS COMMAND

Reason: An undefined user attempted to issue a TSS command.

Action: No action required.

TSS0203E YOU ARE NOT AUTHORIZED FOR THIS TSS FUNCTION

Reason: You do not have authority to use the entered CA-Top Secret function.

Another possible reason for this message is with the use of an invalid parameter on the create statement as when a DCA or VCA incorrectly specifies the Department or Division on the create statement.

Action: No action required.

TSS0204E FUNCTION KEYWORD MISSING OR INVALID

Reason: An invalid function was entered for a TSS command.

Action: Refer to the *Command Functions Guide*.

**TSS0204I CREATE,DELETE,ADD,REPLACE,RENAME,REMOVE,
PERMIT,REVOKE,WHOOWNS,WHOHAS,HELP,LIST,LOCK,
UNLOCK,WHOAMI,MODIFY,ADMIN,DEADMIN,MOVE**

Reason: The TSS HELP command was issued. A list of valid TSS HELP keywords was provided.

Action: For a complete explanation of the functions, refer to the *Command Functions Guide*.

TSS0205E YOU DO NOT YOURSELF HAVE THIS AUTHORITY

Reason: An administrator must possess an authority before he can grant/remove that authority to/from another user.

Action: No action required.

TSS0206E TYPE = function

Reason: Displays the function for which a user does not have authority.

Action: No action required.

TSS0207E INSUFFICIENT AUTHORITY FOR FUNCTION

Reason: The user does not have authority to use the entered function.

Action: No action required.

TSS0208E TYPE = function, AUTHORITY = authority

Reason: Displays the specific function and the authority level at which the user is not authorized. See message TSS0207E. You should note that authority to administer a specific resource class overrides authority to administer the general RESOURCE class.

Action: No action required.

TSS0210E INVALID ACCESS KEYWORD

Reason: An unrecognizable ACCESS level was specified, or the specified ACCESS level is not valid for the resource type.

Action: For the correct access levels, refer to the ACCESS keyword in the *Command Functions Guide*. For installation-defined resources, the ACCESS level must match one of the ACLST levels listed in the TSS ADD(RDT) command that added the resource.

TSS0211E ACCESSOR-ID MISSING OR INVALID

Reason: A CA-Top Secret function was specified without the ACID operand.

Action: Reenter the function in the correct format.

TSS0212E INVALID DATA LIST KEYWORD

Reason: An invalid option was specified for the DATA keyword of the LIST function.

Action: Reenter the LIST function using a valid DATA keyword.

TSS0213E INVALID DAYS KEYWORD

Reason: An invalid option was specified for the DAYS keyword of the PERMIT function.

Action: Reenter the PERMIT function using a valid DAYS keyword.

TSS0214E INVALID DATASET NAME/PREFIX

Reason: A data set or data set prefix was incorrectly specified. The:

- incorrect data set masking (valid only for PERMIT & REVOKE) was used,
- entry contains invalid characters,
- entry is too short, or
- LIBRARY keyword is not specified correctly.

Action: Correct the data set format and reenter the request.

TSS0215E INVALID EXPIRATION

Reason: The expiration date in a FOR or UNTIL keyword parameter is incorrect. Both FOR and UNTIL were specified for a single ACID or resource, or an incorrect keyword was used with an ADD or REMOVE or SUSPEND.

Action: Enter the date in the format specified by the DATE control option, or use the appropriate SUSPEND or SUSPEND FOR/UNTIL keywords.

TSS0216E FACILITY KEYWORD MISSING OR INVALID

Reason: An invalid facility name was specified for the FACILITY keyword. There are three other possible reasons:

1. FACILITY keyword of the COMMANDS or XCOMMANDS function is missing or invalid, or,
2. the MASTFAC value is incorrect, or,
3. the Facility parameter of the LOCKTIME or SITRAN keywords is incorrect.

Action: Determine if the facility was specified correctly. If it was, ensure the facility is properly defined to CA-Top Secret (see the *Implementation* guides).

TSS0217E INVALID FOR KEYWORD DAYS COUNT

Reason: The number of days specified by the FOR keyword exceeds the maximum of 255 days.

Action: Correct the number of days and reenter the command.

TSS0218E INVALID LCF COMMAND

Reason: A command or transaction specified on either the COMMANDS or XCOMMANDS function contains more than 8 characters or invalid characters.

Action: Correct the command or transaction specification and reenter the function.

TSS0219E DATASET MASKING NOT ALLOWED FOR LIBRARIES

Reason: Data set masking cannot be used in the LIBRARIES keyword to specify program libraries. However, full data set names can be specified by entering them in quotation marks.

Action: You may specify full data set names by entering them in quotation marks.

TSS0220E INVALID ACTION KEYWORD

Reason: An unrecognizable ACTION keyword was specified.

Action: See the *Command Functions Guide* for a complete list of ACTION keyword parameters.

TSS0221E OWNER'S NAME REQUIRED.

Reason: When creating an ACID, you did not enter the NAME keyword. The NAME keyword is used for identification and reporting and must be entered when using the CREATE function.

Action: Reenter the TSS CREATE command including the NAME keyword parameter.

TSS0222E RESOURCE LENGTH INVALID FOR FUNCTION

Reason: A prefix resource longer than 26 bytes, or a general resource longer than 8 bytes was specified for either the ADD, REMOVE, or WHOOWNS functions. Longer resources are only valid for PERMIT, REVOKE, and WHOHAS functions.

Action: Correct the resource name and reenter the function command.

TSS0223E PROFILE CANNOT HAVE PROFILES

Reason: Users can be defined to as many as 254 Profiles. Profiles, however, cannot be added to other Profiles.

Action: See the explanation of a PROFILE in the *User Guide*.

TSS0224E PASSWORD KEYWORD REQUIRED

Reason: The PASSWORD keyword was not specified for a CREATE of a new ACID, or the ADD of a facility for an ACID having multiple passwords.

Action: Reenter the command including the PASSWORD parameter.

TSS0226E REQUEST FAILED BY INSTALLATION EXIT

Reason: An installation exit written by your own installation has failed the request.

Action: Contact your Central Security Group to determine the function of the exit.

TSS0227E INVALID VOLUME SERIAL

Reason: The volume specification either:

- contains less than 2 characters,
- contains more than 6 characters, or
- contains invalid characters.

Action: Correct the volume serial specification and reenter the function.

TSS0228E INVALID VOLUME ATTRIBUTES

Reason: The attributes of a volume are incorrectly specified. Typical causes are invalid attribute combinations, such as both D (DASD) and T (TAPE) being specified.

Action: Refer to the *Command Functions Guide*, for the correct format of specifying VOLUME attributes.

TSS0229E INVALID TIMES VALUES

Reason: The TIMES keyword contains invalid hour specifications. The hours of permitted access to a resource must be represented as two numerical values from 00 to 24. Both the starting and the ending hours must be entered.

Action: Refer to the *Command Functions Guide* for the correct TIMES format. Reenter the Command.

TSS0230E AT LEAST 1 RESOURCE KEYWORD REQUIRED

Reason: The PERMIT, REVOKE, WHOOWNS or WHOHAS functions require that a resource keyword--i.e., VOLUMES or PROGRAMS--is specified.

Action: Refer to the *Command Functions Guide* for the correct command function.

TSS0231E ONLY 1 RESOURCE MAY BE SPECIFIED

Reason: The WHOOWNS or WHOHAS function was specified with more than one resource.

Action: Reenter the function, specifying one resource at a time.

TSS0233E INVALID CICS SCTYKEY

Reason: A CICS security key greater than 64 was specified. Valid security keys are 0-64.

Action: Enter a valid key.

TSS0234E INVALID TIME ZONE

Reason: An invalid time zone displacement was specified. Valid time zones are -12 to 12.

Action: See the *Command Functions Guide* for a complete explanation of the TZONE keyword parameter (used with the ADD or CREATE function).

TSS0235E INVALID CICS OPCLASS

Reason: A CICS operator class greater than 24 was specified. Valid classes are 0-24.

Action: Enter a valid class.

TSS0236E INVALID CICS OPPRTY

Reason: A CICS operator priority greater than 255 was specified. Valid priority is 0-255.

Action: Enter the proper priority.

TSS0237E INVALID LOCK TIME TERMINAL

Reason: A terminal lock time greater than 120 minutes was specified. Valid lock times are 0-120 minutes.

Action: Reenter the terminal lock time with a valid minute specification.

TSS0238E USER CLASS NAME MISSING OR INVALID

Reason: An invalid user class was specified for UR1 or UR2. The user class must be a single character or digit.

Action: Refer to the *Command Functions Guide*, for a complete description of UR1 and UR2.

TSS0239E INVALID ADMINISTRATION AUTHORITY

Reason: A specified administration authority is invalid or unknown.

Action: Refer to the *Command Functions Guide*, for valid ADMIN/DEADMIN authorities.

TSS0240E INVALID RESOURCE NAME

Reason: A minidisk or minidisk prefix was incorrectly specified. Either masking was used incorrectly, the entry contains invalid characters, or the entry is too short.

Action: No action required.

TSS0241E INVALID DIAGNOSE RESOURCE

Reason: An invalid diagnose response was specified. Valid diagnose resources are hexadecimal values ranging from 0 to FFFF.

Action: No action required.

TSS0242E UNKNOWN KEYWORD

Reason: The command processor could not recognize the entered keyword

Action: Reenter the TSS command, using the correct spelling of the keyword.

TSS0243E INVALID SUBFIELD DATA

Reason: The format of the subfield did not conform to the format as required by the keyword.

Action: Reenter the TSS command, using correct subfield format

TSS0244E INVALID SUBFIELD LENGTH FOR KEYWORD

Reason: The text of the subfield was longer than the allowable length as determined by the keyword.

Action: Reenter the TSS command, using a valid subfield length.

TSS0245E INVALID INTEGER VALUE

Reason: The text of the subfield was not 0-9 characters.

Action: Reenter the TSS command, using integer characters.

TSS0246E SUBFIELD CONTAINS INVALID CHARACTER(S)

Reason: The text of the subfield as required by the keyword should have been one of the following but was not:

ALPHABETIC
ALPHANUMERICS
NUMERIC

Action: Reenter the TSS command, using the characters required by the keyword.

TSS0247E DUPLICATE KEYWORD SPECIFICATION

Reason: The same keyword was entered more than once.

Action: Reenter the TSS command, using each keyword only once.

TSS0248E REQUIRED SUBFIELD MISSING FOR KEYWORD keyword

Reason: You need a subfield for this keyword.

Action: Reenter the TSS command, with the appropriate subfield.

TSS0249E STATEMENT CONTAINS UNBALANCED PARENTHESIS

Reason: The TSS command is missing one of its parentheses.

TSS0250E INVALID HEX VALUE

Reason: The text of the subfield was not 0-9 or A-F characters.

Action: Reenter the TSS command, using valid hex characters.

TSS0251E KEYWORD <keyword> DOES NOT SUPPORT SUBFIELDS

Reason: A subfield was entered for a keyword that does not require a subfield.

Action: Reenter the TSS command, using valid syntax.

TSS0252E KEYWORD NOT DISCERNIBLE keyword

Reason: An abbreviated form of a keyword was specified, however, it was too short to identify one full keyword name. For example, if you use "PA" as a password, TSS cannot discern whether it stands for PAssword or PAnel.

Action: Reenter the TSS command using a valid keyword.

TSS0253I NOTHING TO REFRESH. ACID/JOBNAME NOT FOUND

Reason: The requested ACID could not be found and logged-on in either the current or named address space.

Action: Check ACID/JOBNAME entered.

TSS0254I REFRESH ALREADY IN PROGRESS. RETRY LATER

Reason: A TSS REFRESH request is currently being processed for the named ACID.

Action: If required, retry the command at a later time.

TSS0257E PRIVPGM INVALID FOR THIS RESOURCE CLASS

Reason: PRIVPGM was entered as a keyword on a TSS PERMIT command and PRIVPGM is not valid for the resource class being permitted.

Action: Remove the PRIVPGM keyword from the PERMIT or if it is a user-defined resource class, add the PRIVPGM attribute to the RDT entry for resource class and reissue TSS PERMIT.

TSS0258E MISSING OR INVALID LINKID VALUE

Reason: The linkid value specified was missing or invalid.

Action: Correct the linkid specified.

TSS0259E INVALID CONVSEC VALUE

Reason: An incorrect value was specified for Conversation Security

Action: Specify a maximum of eight characters.

TSS0260E INVALID INTERVAL VALUE

Reason: An incorrect or too high of a value was specified.

Action: Specify a value that does not exceed 99999.

TSS0261E MORE THAN 5 ACIDS

Reason: A maximum of 5 acids can be specified in a single TSS command; however, the TSS command can be repeated an unlimited amount of times.

Action: Reenter the TSS command, specifying 5 or less acids per command entry.

TSS0262E ACID IS ASUSPENDED

Reason: A TSS REMOVE(SUSPEND) command was issued for an ACID that was administratively suspended.

Action: Issue the TSS REMOVE(ASUSPEND) command.

TSS0263E MORE THAN 8 DATASETS OR LIBRARIES

Reason: A maximum of 8 data sets or libraries can be specified in a single TSS command; however, the TSS command can be repeated an unlimited amount of times.

Action: Reenter the TSS command specifying 8 or less data sets or libraries per command entry.

TSS0264E MORE THAN 30 ENTRIES IN LIST

Reason: A maximum of 30 commands can be specified in a LCF list of a single TSS command; however, the TSS command can be repeated an unlimited amount of times.

Action: Reenter the TSS command, specifying 30 or less commands in the LCF list per command entry.

TSS0266E MORE THAN 8 PRIVILEGED PROGRAMS

Reason: A maximum of 8 privileged programs can be specified in a single TSS command; however, the command can be repeated an unlimited amount of times.

Action: Reenter the TSS command, specifying 8 or less privileged programs per command entry.

TSS0267E MORE THAN 5 PROFILES

Reason: A maximum of 5 profiles can be specified in a single TSS command; however, the TSS command can be repeated an unlimited number of times.

Action: Reenter the TSS command, specifying 5 or less profiles per command entry.

TSS0269E MORE THAN 30 VOLUMES

Reason: A maximum of 30 volumes can be specified in a single TSS command; however, the TSS command can be repeated an unlimited number of times.

Action: Reenter the TSS command, specifying 30 or less volumes per command entry.

TSS0271E MORE THAN 5 JOB SOURCES

Reason: A maximum of 5 job sources can be specified in a single TSS command; however, the TSS command can be repeated an unlimited number of times.

Action: Reenter the TSS command, specifying 5 or less job sources per command entry.

TSS0272E MORE THAN 5 USER DATA ELEMENTS

Reason: A maximum of 5 user data elements can be specified in a single TSS command; however, the TSS command can be repeated an unlimited number of times.

Action: Reenter the TSS command, specifying 5 or less user data elements per command entry.

TSS0273E MORE THAN 5 RESOURCE ELEMENTS

Reason: A maximum of 5 resource elements can be specified in a single TSS command; however, the TSS command can be repeated an unlimited number of times.

Action: Reenter the TSS command, specifying 5 or less resource elements per command entry.

TSS0274E MORE THAN 8 MISC1 AUTHORITIES

Reason: A maximum of 8 MISC1 AUTHORITIES can be specified in a single TSS command; however, the TSS command can be repeated an unlimited number of times.

Action: Reenter the TSS command, specifying 8 or less MISC1 AUTHORITIES per command entry.

TSS0275E MORE THAN 8 MISC9 AUTHORITIES

Reason: A maximum of 8 MISC9 AUTHORITIES can be specified in a single TSS command; however, the TSS command can be repeated an unlimited number of times.

Action: Reenter the TSS command, specifying 8 or less MISC9 AUTHORITIES per command entry.

TSS0276E MORE THAN 8 RESOURCE AUTHORITIES

Reason: A maximum of 8 resource authorities can be specified in a single TSS command; however, the TSS command can be repeated an unlimited number of times.

Action: Reenter the TSS command specifying 8 or less resource authorities per command entry.

TSS0277E MORE THAN 8 MINIDISKS

Reason: A maximum of 8 minidisks can be specified in a single TSS command; however, the TSS command can be repeated an unlimited number of times.

Action: Reenter the TSS command, specifying 8 or less minidisks per command entry.

TSS0278E MORE THAN 20 ACCESS LEVELS

Reason: You exceeded the 20-access-level limit for this resource.

Action: Reenter the TSS command, specifying 20 or fewer access levels.

TSS0279E RESCLASS MISSING, INVALID, OR RESERVED

Reason: A TSS RDT command was entered and the RESCLASS parameter was either missing, more than 8 characters, or already being used in the RDT record.

Note: When adding a new RESCLASS name, be sure that it does not match the first four characters of any existing resource class name.

Action: Reenter the TSS command, using a valid resource class.

TSS0280E RESCODE MISSING, INVALID, OR RESERVED

Reason: The TSS ADD(RDT) you just entered is missing the RESCODE. Other causes include a RESCODE with more than 2 characters, with invalid hex characters, or the RESCODE has already been used.

Action: Reenter the TSS command, using a valid RESCODE.

TSS0281E INVALID ACLST/DEFACC VALUE

Reason: A TSS RDT command was entered with the ACLST and/or DEFACC parameter. One of the following caused the error:

- The access level name was greater than 8.
- The access level name was entered without a hex value and that name did not match one of the system-supplied access level names.
- More than 4 characters were entered as a hex value.
- Non-hex characters were entered as an access level.

Action: Reenter the TSS command with a valid ACLST/DEFACC.

TSS0282E DEFACC ENTRY MUST MATCH ACLST ENTRY

Reason: The TSS RDT command you entered had an ACLST and/or DEFACC parameter. One of the following caused the error:

- If ACLST and DEFACC were entered, the name and hex value of DEFACC does not match an ACLST entry.
- If only ACLST was entered, none of the ACLST hex values match the DEFACC in the RDT.

- If only DEFACC was entered, its hex value does not match any of the ACLST values in the RDT.

Action: Reenter the TSS command with a valid ACLST/DEFACC.

TSS0283E RESOURCE OWNED WITHIN RESCLASS, CANNOT BE REMOVED

Reason: A TSS REM(RDT) command was entered but resources had been defined under the RESCLASS to be removed.

Action: Determine what resources are owned under this RESCLASS by issuing TSS WHOOWNS resclass(*), removing ownership, and reentering the TSS REMOVE(RDT) command.

TSS0284E ONLY "ATTR(EXIT,DEFPROT,MERGE)" VALID WHEN UPDATING A STATIC RDT ENTRY

Reason: A TSS REP(RDT) command was entered for a non-dynamic resource. EXIT, DEFPROT, and MERGE are the only valid attributes.

Action: Reenter the TSS command, using a valid attribute.

TSS0285E INVALID PRIVPGM NAME

Reason: A TSS command was entered with the PRIVPGM keyword but the PRIVPGM name had more than 8 characters or an '(' was entered but not followed by 'G)' for GENERIC. Example: PGM(G) is correct.

Action: Reenter the TSS command, using a valid PRIVPGM.

TSS0286E INVALID VMUSER NAME

Reason: A TSS command was entered with the VMUSER keyword, but the VMUSER name had more than 8 characters or an '(' that was not followed by a 'G)' for generic. Example: VMU(G) is correct.

Action: Reenter the TSS command, using a valid PRIVPGM.

TSS0287E ACTION DENY IS INVALID; RESOURCE HAS ACCESS LEVEL

Reason: You entered a TSS PERMIT ACTION(DENY) but the resource supports the ACCESS keyword.

Action: To prohibit the use of a resource which supports access levels, ACCESS(NONE) should be used.

TSS0288E MORE THAN 30 RESOURCE CLASSES

Reason: You entered a TSS LIST(RDT) RESCL() command, but the RESCLASS keyword had more than 30 classes in the list.

Action: Reenter the TSS command, specifying 30 or fewer RESCLASSes.

TSS0289E INVALID TERMINAL OR OPERATOR ID CARD

Reason: The OI DCARD keyword was specified, but either the terminal from which the command was entered does not have an operator id card reader, or either VTAM or TCAM encountered a permanent I/O error while reading the operator id card. Note that this keyword may not be specified if the TSS command is being used in batch.

Action: No action required.

TSS0290E FUNCTION INVALID IN RACF COMPATIBLE MODE

Reason: The LOCK, UNLOCK, and WHOAMI functions are not valid when CA-Top Secret is running in RACF compatible mode.

Action: No action required.

TSS0291E FUNCTION INVALID IN THIS ENVIRONMENT

Reason: The LOCK, UNLOCK, and WHOAMI functions are not valid from the console.

Action: No action required.

TSS0292E TSS COMMAND ABENDED PROCESSING THIS REQUEST

Reason: The TSS command subtask abended while processing your request.

Action: Notify your system support staff.

TSS0293E INVALID VALUE FOR KEYWORD ccccccc

Reason: The value of the keyword shown is incorrect.

Action: Refer to the *Command Reference* guide for acceptable value(s).

TSS0294E MORE THAN nn xxxxxxxxxxx

Reason: The keyword shown only accepts nn operands

Action: Reenter the command with no more than nn operands. You may enter the command more than once, if needed.

TSS0295E INVALID MAXLEN VALUE OR FIELD ENTERED IS TOO LONG

Reason: If ADD/REP to FDT: Either the value entered for MAXLEN exceeds 32767 bytes or the total value of all MAXLENS dynamically added to the FDT exceeds 32767.

If ADD/REP to ACID: The length of the field entered exceeds the MAXLEN given when the field was added to the FDT.

Action: If adding/changing to the FDT, you must reduce the size of the MAXLEN field.

If you are adding or changing an ACID, you must enter a smaller field or modify the size of the MAXLEN as designated in the FDT.

TSS0296E RESERVED SEGMENT NAME

Reason: When adding or changing the SEGMENT associated with an FDT entry the given segment name is reserved by the system.

Action: Chose another SEGMENT name and re-enter the command.

TSS0297A SPECIFY YOUR PASSWORD

Reason: Your signon password is required to perform the service you have requested, typically to unlock a terminal.

Action: Type your signon password. Press the ENTER key.

TSS0297E SCOPE ACID MUST BE TYPE LSCA OR ZONE

Reason: An attempt was made to assign a scope to an LSCA and one or more of the ACIDs identified in the SCOPE keyword was not a ZONE or an LSCA.

Action: Reenter the command using a valid ZONE or LSCA in the SCOPE keyword.

TSS0298A INSERT OPERATOR ID CARD

Reason: TSS must read the data from the OI DCARD for later verification when the ACID attempts to sign on to a facility.

Action: Insert the ACID's operator ID card into the reader.

TSS0299E keyword KEYWORD ILLEGAL FOR FUNCTION

Reason: The named keyword is invalid for the entered function.

Action: For a list of valid function keywords enter: TSS HELP

TSS0300I TSS function FUNCTION SUCCESSFUL

Reason: The listed CA-Top Secret function has successfully completed.

Action: No action required.

TSS0301I TSS function FUNCTION FAILED, RETURN CODE = XX

Reason: The listed CA-Top Secret function has failed. This message will always be preceded by a detailed message explaining the reason for the failure. The following code and messages apply:

- 4** Syntax error, such as invalid access
- 8** Functional error, such as data set not found
- 16** Unexpected error occurred, message TSS0390E will also display

Action: No action required.

TSS0302I *WARNING* THIS ACCESSOR-ID RECORD IS DAMAGED

Reason: The TSS command attempted to modify a security record and found that it contained invalid data.

Action: Contact CA technical support.

**TSS0303I AcidName(xxxxxxxx) Type(xxxx) Mode(xxxx) Facility(xxxxxxxx)
Terminal(xxxxxxxx) SystemID(xxxxxxxx) Log(xxx) INSTDATA(xxxxxxxx)
BYPASSING(xxxxx)**

Reason: This message displays information about an ACID in response to a TSS WHOAMI command.

Action: Informational message, no action necessary.

TSS0305E FDTNAME MISSING, INVALID, OR RESERVED

Reason: A TSS FDT command was entered and the FDTNAME parameter was either missing, more than 8 characters, or already being used in the FDT record.

Action: Reenter the TSS command, using a valid field name.

TSS0306E FDTCODE IS NOT DEFINED

Reason: The FDTCODE specified in the TSS command is not defined in the Field Descriptor Table (FDT).

Action: Reenter the TSS command, specifying a valid FDTCODE.

TSS0307E FDTCODE MISSING, INVALID, OR RESERVED

Reason: The TSS ADD(FDT) command that you just entered was invalid. Possible causes include: a missing FDTCODE, an FDTCODE with more than 2 characters, invalid hex characters, or the FDTCODE has already been used.

Action: Reenter the TSS command, using a valid FDTCODE.

TSS0310E DATASET/PREFIX SECURITY FILE SEGMENT IS FULL

Reason: No new data sets or data set prefixes can be created until the Security File is extended.

Action: To extend the Security File, use the CA-Top Secret utility, TSSXTEND, explained in the *Installation Guide*.

TSS0311E VOLUME SECURITY FILE SEGMENT IS FULL

Reason: No new volumes or volume prefixes can be added until the Security File is extended.

Action: To extend the Security File, use the CA-Top Secret utility, TSSXTEND, explained in the *Installation Guide*.

TSS0312E ACCESSOR-ID SECURITY FILE SEGMENT IS FULL

Reason: No new ACID's can be created until the Security File is enlarged.

Action: To extend the Security File, use the CA-Top Secret utility TSSXTEND explained in the *Installation Guide*.

TSS0313E PERMANENT I/O ERROR UPDATING THE SECURITY FILE

Reason: A permanent hardware I/O error was encountered by CA-Top Secret while updating the Security File. The system console operator will be informed of the problem.

Action: When the Security File becomes available, verify the results of the last entered command. If the problem is not hardware related, notify CA Technical Support.

TSS0314E ACID DOES NOT EXIST

Reason: The ACID specified on a function or in the ACID keyword has not been CREATED.

Action: Either create a new ACID or specify an existing one.

TSS0315E ACID ALREADY EXISTS

Reason: The ACID being CREATED already exists in the Security File.

Action: If you wish to create an ACID other than the existing one, you must specify a new acid name.

TSS0316E VOLUME NOT FOUND IN SECURITY FILE

Reason: The specified volume has not been ADDED to the Security File.

Action: Use the TSS ADD function if you wish to add the volume to the CA-Top Secret Security File. See the *Command Functions Guide* for the correct format of the ADD function.

TSS0317E DATASET/PREFIX NOT FOUND IN SECURITY FILE

Reason: The specified data set or data set prefix has not been ADDED to the Security File.

Action: The data set/prefix must be added to an existing ACID via the TSS ADD function.

TSS0318E RESOURCE NOT FOUND IN SECURITY FILE

Reason: The specified resource has not been ADDED to the Security File.

Action: The resource must be added to an existing ACID via the TSS ADD function.

TSS0320E SPECIFIED UID/GID ALREADY IN USE BY acid

Reason: This message indicates an error with the value supplied for either the UID, GID or HOMEUID keywords. The supplied value is already in-use by another ACID, or, the named-ACID already has a value set. Use the TSS LIST command function and list the ACID shown in the message to determine which one of these conditions has caused the error.

Action: Either give this user a different, unique, UID/GID number or remove this number from the listed ACID prior to adding to this ACID.

TSS0321E INVALID ACID TYPE FOR THIS UID/GID

Reason: The administrator has tried to either add a GID value to a non-TYPE(GROUP) acid or has tried to add a UID value to an ACID that is not a USER, DCA, VCA, ZCA, LSCA, or SCA.

Action: No action required.

TSS0322E INVALID KEYWORD WITH THIS ACID TYPE

Reason: The administrator has attempted to add a resource or field to an ACID that cannot have that information added to it.

Action: Ensure that the target ACID is the correct one and only add valid information to the ACID.

TSS0323E RESOURCE SECURITY FILE SEGMENT IS FULL

Reason: New resources cannot be added to the Security File until the file is enlarged.

Action: Enlarge the Security File using the TSSXTEND utility explained in the *Installation Guide*.

TSS0324E ADMINISTRATOR'S ACID DOES NOT EXIST ON TARGET NODE

Reason: A TSS command has been sent to another node using CPF, but the ACID for the administrator issuing the command does not exist on the remote system.

Action: You must get your ACID defined on the remote system prior to directing any administration commands to that node.

TSS0340E DATASET/PREFIX NOT OWNED WITHIN SCOPE

Reason: The data set or data set prefix specified in an ADD request is already owned by an ACID in another department or division.

Action: To grant an ACID access to the data set/prefix, use the TSS/PERMIT function.

TSS0342E DATASET/PREFIX NOT FOUND IN SECURITY RECORD

Reason: The data set or data set prefix specified in a REMOVE or REVOKE request was not found in the ACID's Security Record, so therefore, cannot be removed or revoked from that ACID.

Action: No action required.

TSS0343E VOLUME IS NOT OWNED WITHIN SCOPE

Reason: The volume specified in an ADD request is already owned by an ACID in another department or division.

Action: To grant access to the volume, use the TSS PERMIT function.

TSS0345E VOLUME NOT FOUND IN SECURITY RECORD

Reason: The volume specified in a REMOVE or REVOKE request was not found in the ACID's Security Record, so therefore, cannot be removed or revoked from that ACID.

Action: No action required.

TSS0346E PROFILE/GROUP NOT FOUND

Reason: The profile or group specified in an ADD, REMOVE or REVOKE request was not found.

Action: No action required.

TSS0347E NAMED ENTRY NOT FOUND IN RECORD

Reason: The linkid specified was not found or the entry specified with this linkid was not found.

Action: Ensure the linkid exists or that the entry is there.

TSS0350E RESOURCE IS NOT OWNED WITHIN SCOPE

Reason: The resource specified in an ADD request is already owned by an ACID in another department or division.

Action: To grant access to the resource, use the TSS PERMIT function.

TSS0351E SPECIFY 'UNDERCUT' TO TRANSFER OWNERSHIP

Reason: An attempt was made to ADD a resource to an ACID; however, the resource is already owned.

Action: If transfer of ownership is intended, you must specify the UNDERCUT keyword with the ADD function.

TSS0352E ACID NOT OWNED WITH SCOPE

Reason: The ACID whose Security Record you wish to modify is not within your scope of authority.

Action: Determine the department or division responsible for the ACID Security Record. Notify the responsible Security Administrator.

TSS0353E USER ALREADY ATTACHED TO PROFILE/GROUP

Reason: An attempt was made to ADD a PROFILE or GROUP to an ACID that already has a profile or group associated with it.

Action: No action required.

TSS0354E INVALID SPECIFICATION OF PROFILE

Reason: An attempt was made to ADD a profile to a department, division, another profile or to a valid ACID that already has that profile.

Action: Profiles can be added to the following Acid types only: USER, SCA, VCA, DCA. If you are attempting to define a profile, you must use the TSS CREATE function.

TSS0355E STARTED TASK PROCEDURE NOT FOUND

Reason: The PROCNAME specified in a REMOVE(STC) request was not found in the Started Task table.

Action: No action required.

TSS0356E SECURITY RECORD ENQ/DEQ FAILED

Reason: Before processing a security record, the TSS command attempts to ENQ on the security record. This ENQ attempt has failed.

Action: This message is usually an indication of a system-wide problem. Notify your system support staff.

TSS0357E PROFILE NOT OWNED WITHIN SCOPE

Reason: A PROFILE which is not within your scope of authority or that is not Globally Administrable (GAP keyword) was specified in an ADD request.

Action: No action required.

TSS0358E FUNCTION INVALID FOR "ALL" FACILITY

Reason: An invalid function was specified when administering the "ALL" record.

Action: No action required.

TSS0359E STORAGE GETMAIN FAILED

Reason: Insufficient storage was available for the entered TSS command. Either your region size is too small or there is a shortage of SVA storage.

Action: Notify CA Technical Support.

TSS0360E ACCESSOR-ID ALREADY OWNS THE RESOURCE

Reason: An attempt was made to PERMIT a resource to an ACID; however, the ACID already owns that resource. By definition, the owner ACID already possesses full access to the resource.

Action: No action required.

TSS0361E ATTEMPT TO ADD MORE THAN 254 PROFILES TO ACID

Reason: An ACID can be assigned a maximum of 254 Profiles.

Action: No action required.

TSS0362E ACCESSOR-ID IS THE OWNER OF THE RESOURCE

Reason: Resources that are owned by an ACID cannot be REVOKED from that ACID.

Action: To remove the ACID's access to the owned resource, use the REMOVE function.

TSS0363E DIVISION SPECIFICATION MISSING OR INVALID

Reason: There are two possible reasons:

1. The DIVISION keyword specified an invalid DIVISION name.
2. An attempt was made to CREATE a VCA and the DIVISION keyword was omitted.

Action: Specify the correct keyword.

TSS0364E DEPARTMENT SPECIFICATION MISSING OR INVALID

Reason: There are two possible reasons:

1. The DEPARTMENT keyword specified an invalid DEPARTMENT name.
2. An attempt was made to CREATE a DCA and the DEPARTMENT keyword was omitted.

Action: Specify the correct keyword.

TSS0365E FUNCTION INVALID FOR "STC" FACILITY

Reason: An invalid function was specified when administering the STARTED TASK(STC) record. Only ADD and REMOVE functions are valid.

Action: No action required.

TSS0367E RESOURCE HAS BEEN PERMITTED TO ANOTHER ACID

Reason: An attempt was made to REMOVE a resource; however, the resource has been permitted to another ACID.

Action: In order to successfully execute the REMOVE command, all permissions to the resource must be removed.

TSS0368E LSCA/ZONE/DIV/DEPT/PROFILE STILL HAS CONNECTED ACIDS

Reason: An attempt was made to DELETE a Department, Division, Zone or Profile. CA-Top Secret has failed the request because there are still ACIDs connected to it.

Action: Before DELETE can be executed on a Zone, Division Department or Profile record, all ACID assignments/connections must be removed. Use the TSS LIST command to display the ACIDs that are connected.

TSS0369E ADMIN INVALID FOR ZONE, DIV, DEPT, PROFILE, OR GROUP

Reason: Administration authority cannot be granted to any ACID other than a user, Administrator, or the "ALL" record.

Action: No action required.

TSS0370E OIDCARD DATA NOT FOUND IN SECURITY RECORD

Reason: The operator id card of an ACID was not found in the Security Record when a REMOVE request was specified.

Action: No action required.

TSS0371E LCF COMMAND NOT FOUND IN SECURITY RECORD

Reason: The command specified in a REMOVE request was not found in the ACID's LCF list.

Action: No action required.

TSS0372E FUNCTION INVALID FOR "AUDIT" FACILITY

Reason: An invalid function was specified for the "AUDIT" facility. The only valid functions are ADD and REMOVE.

Action: No action required.

TSS0374E ZONE SPECIFICATION MISSING OR INVALID

Reason: There are two possible reasons for this message:

- The ZONE keyword specified an invalid ZONE name.
- An attempt was made to CREATE a ZCA, and the ZONE keyword was omitted.

Action: Reenter the command using a valid ZONE ACID.

TSS0375E PERMITTED ACID NOT FOUND IN SECURITY RECORD

Reason: The acid specified in the ACID keyword of a REVOKE request was not found in the Security Record.

Action: No action required.

TSS0376E PASSWORD INVALID FOR ZONE, DIV, DEPT OR PROFILE

Reason: A password may only be given to a user or an administrator.

Action: Reenter the command excluding the PASSWORD parameter.

TSS0377E ADMIN AUTHORITY NOT FOUND IN SECURITY RECORD

Reason: The administration authority specified in a DEADMIN request did not exist.

Action: No action required.

TSS0378E FACILITY INVALID FOR DIVISION OR DEPARTMENT

Reason: Since Division and Department ACIDs cannot access a system facility, the FACILITY keyword is meaningless.

Action: No action required.

TSS0379E PERMIT AND REVOKE INVALID FOR ZONE, DIV, DEPT or GROUP

Reason: A resource cannot be PERMITTED or REVOKED from a DEPARTMENT, DIVISION, ZONE, or GROUP.

Action: No action required.

TSS0380E SOURCE NOT FOUND IN SECURITY RECORD

Reason: The source specified in a REMOVE request was not found in the ACID's Security Record.

Action: No action required.

TSS0381E INSTDATA NOT FOUND IN SECURITY RECORD

Reason: A request was made to REMOVE installation data from an ACID's Security Record; however, the ACID's Security Record did not contain installation data.

Action: No action required.

TSS0382E USER FIELD NOT FOUND IN SECURITY RECORD

Reason: The user resource specified in a REMOVE request was not found in the ACID's Security Record.

Action: No action required.

TSS0383E RESOURCE ELEMENT NOT FOUND

Reason: The general field specified in a REMOVE request was not found in the ACID's Security Record.

Action: No action required.

TSS0384E RESOURCE NOT FOUND IN SECURITY RECORD

Reason: A CICS resource--such as FCT or PPT--specified in a REMOVE or REVOKE request was not found in the ACID's Security Record.

Action: No action required.

TSS0385E DATASET/PREFIX ALREADY OWNED, USE PERMIT

Reason: An attempt was made to ADD a resource to an ACID. This message resulted because another ACID already owns the resource at a generically higher level (a shorter prefix).

Action: To grant access to the resource, use the "PERMIT" function. To transfer ownership, use the "ADDTO" function with the UNDERCUT parameter. The resource prefix must be at least as generically high as the prefix that is currently owned.

TSS0386E VOLUME ALREADY OWNED, USE PERMIT

Reason: See message TSS0385E

Action: No action required.

TSS0387E RESOURCE ALREADY OWNED, USE PERMIT

Reason: See message TSS0385E

Action: No action required.

TSS0389E FUNCTION INVALID WHEN USED WITH RDT

Reason: A TSS RDT command was entered but the function was not ADDTO, REMOVE FROM, REPLACE, DELETE, OR LIST.

Action: Reenter the TSS command, using the correct function.

TSS0390E UNEXPECTED ERROR, CODE = xxx

Reason: CA-Top Secret encountered a situation that logically should never occur.

Action: Collect dumps and/or trace logs produced by error. Contact CA Technical Support.

TSS0391E ADMIN ACID MUST BE TYPE LSCA

Reason: A TSS ADMIN(acid) SCOPE command was issued and the target of the command was not an LSCA.

Action: Reenter the command using a valid LSCA ACID.

TSS0391I MERGE DELETED RESOURCE XXXXXXXX

Reason: A TSS DELETE(RDT) was issued, and the indicated user defined resource class has been deleted from the RDT.

Action: Informational message only.

TSS0392E MERGE FAILED - COULD NOT DELETE RESCLASS XXXXXXXX

Reason: A TSS DELETE(RDT) was issued, and resources were found to be defined for the indicated user-defined resource class. The RDT may not be deleted until all user-defined resources have been removed.

Action: Remove all references to the user defined resources.

TSS0393E RESOWNER ACID DOES NOT EXIST

Reason: An attempt was made to ADD a RESOWNER to a data set for SMS, but the ACID indicated in the RESOWNER parameter was not a valid AICD.

Action: Re-enter the command using a valid ACID.

TSS0394E RESOWNER ACID TYPE IS INVALID

Reason: The ACID indicated by the RESOWNER parameter is not an SCA, VCA, DCA, or USER ACID.

Action: Reissue the command, specifying a valid ACID.

TSS0395E RESOWNER ACID IS NOT IN SCOPE

Reason: The ACID indicated by the RESOWNER parameter does not fall within your administrative scope.

Action: Either specify an ACID which falls within your scope, or have an administrator with the proper authority assign the RESOWNER.

TSS0396E USING ACID DOES NOT EXIST

Reason: In the USING parameter of CREATE, you specified an ACID which does not exist.

Action: Reissue the command, specifying a valid ACID.

TSS0397E TYPE SPECIFIED DOES NOT MATCH USING ACID

Reason: The type of ACID you specified in the using parameter of a TSS CREATE was incompatible with the acid type indicated by the TYPE keyword. For example, TSS CRE(USER01) TY(USER) USING(DEPT01) is incorrect because DEPT01 is a department-type ACID, not a USER ACID.

Action: Reissue the command, either specifying a valid ACID, or excluding the type parameter.

TSS0398E INVALID BEFORE/AFTER KEYWORD

Reason: Both the BEFORE keyword and AFTER keyword were specified on the ADD of a profile. The BEFORE and AFTER keywords cannot be specified together in one command.

Action: Reissue the command, specifying either the BEFORE or AFTER keyword, not both.

TSS0399E BEFORE/AFTER PROFILE DOES NOT EXIST

Reason: The profile specified by the BEFORE or AFTER keyword was not a valid PROFILE.

Action: Reissue the command, specifying a valid PROFILE acid.

TSS0400E BEFORE/AFTER PROFILE NOT ATTACHED TO ACID

Reason: The PROFILE acid specified by the BEFORE or AFTER keyword was not connected to the USER acid.

Action: Reissue the command, specifying a valid PROFILE acid.

TSS0401E INVALID TYPE

Reason: The TYPE parameter of a MOVE function is incompatible with the type of ACID being moved. Refer to the *Command Functions Guide* for a list of valid types which may be specified on a MOVE.

Action: Reissue the command, either omitting the TYPE keyword, or specifying a valid ACID type.

TSS0403E CPF INACTIVE; COMMAND WILL NOT BE EXECUTED OR LOGGED

Reason: An attempt was made to route a TSS command to a remote node through the TARGET keyword. However, the Command Propagation Facility (CPF) of CA-Top Secret is not active.

Action: Issue a TSS MODIFY(STATUS) to find the current status of CPF. Refer to the CPF chapter in the *Command Functions Guide* for further details.

TSS0404E MORE THAN 254 REMOTES TARGETED; REQUEST IGNORED

Reason: The TARGET keyword was specified on a TSS command and contained a list of more than 254 target nodes.

Action: In the unlikely event that you truly intended to route a TSS command to more than 254 nodes, the command will have to be issued more than once, with less than 254 TARGET nodes specified each time.

TSS0405E NO REMOTES TARGETED

Reason: The WAIT keyword was specified on a TSS command and either the TARGET keyword was omitted, or no default nodes were indicated by the CPFTGT control option.

Action: Either omit the WAIT keyword from the command, include the TARGET keyword with the WAIT command, or establish default TARGETs through the CPFTGT control option.

TSS0406E INVALID VALUE FOR WAIT KEYWORD

Reason: The WAIT keyword of the TSS command did not contain a value of Y (Yes) or N (No).

Action: Either re-specify the value for the WAIT keyword, or omit the keyword and allow the command to take the default indicated by the CPFMSGs control option.

TSS0407E CPF SUBTASK HAS ABENDED

Reason: An error occurred attempting to route a command to or from a remote node.

Action: Contact CA-Technical Support.

TSS0408E RESCLASS AND RESCODE ARE MUTUALLY EXCLUSIVE FOR LIST FUNCTION

Reason: Both the RESCLASS and RESCODE keywords were specified on a LIST(RDT) command. Only one keyword may be used.

Action: Reissue the command, specifying either the RESCLASS or RESCODE.

TSS0409E RESCODE IS NOT DEFINED

Reason: The RESCODE specified in the TSS command is not defined in the Resource Descriptor Table (RDT).

Action: Re-enter the command, specifying a valid RESCODE.

TSS0410E MORE THAN 8 MISC2 AUTHORITIES

Reason: A TSS ADMIN/DEADMIN command for MISC2 authorities was attempted, and the list of authorities contained more than 8 entries.

Action: Examine the syntax of the command entered, as there are only three unique values for MISC2.

TSS0412E DSNAMES IS REQUIRED WITH USE OF LIBRARY

Reason: Currently, only the DSN (data set) resource supports program pathing from libraries.

Action: If you're not permitting a data set, re-enter the command, omitting the library keyword.

TSS0413E RESOURCE ALREADY DEFINED TO PERMITTEE

Reason: A PERMIT with ACTION(ADMIN) was issued against the owner of the resource.

Action: The owner of a resource automatically has administrative authority over the resource, and a PERMIT with ACTION(ADMIN) is not allowed.

TSS0414E EXTENDED ADMINISTRATION DOES NOT SUPPORT MASKING

Reason: Extended administration (ACTION(ADMIN)) does not support the use of masking characters in the resource name.

Action: Re-enter the command, omitting the masking character in the resource name.

TSS0418I NO HELP AVAILABLE

Reason: You issued a TSS HELP command for an operand that is not supported in CA-Top Secret help.

Action: No action necessary.

TSS0419E INVALID REMOTE NODE IN TARGET LIST

Reason: The remote node identified in target list is not defined in the CPFNODES control option.

Action: Add desired target to CPFNODES in parmfile.

TSS0420E INCONSISTENT VALUES IN DATA KEYWORD

Reason: Keywords entered for the DATA parameter conflict with one another.

Action: Reenter the command with one or the other DATA keyword.

TSS0421E FUNCTION INVALID WHEN USED WITH APPCLU

Reason: An attempt was made to RENAME, PERMIT, REVOKE, ADMIN or DEADADMIN APPCLU ACID.

Action: Retry command using one of the valid TSS command functions (i.e., ADD, REMOVE, or REPLACE).

TSS0422E PASSWORD VERIFICATION FAILED AT REMOTE NODE

Reason: ACID updated his password and during the propagation of that new password, CPF discovered that the ACID's old password on the local node did not match his current password on the remote node. This could indicate that there are two different ACIDs with the same ACID name on two or more different nodes. Password change does not take effect on the remote node.

Action: No action required. This message is issued to the CPF SPOOL data set of the remote node.

TSS0423I FROM: cpfnode

Reason: This message is issued immediately before a display of messages received from a remote node in response to a synchronous (WAIT(y)) command previously sent to that node.

Action: No action required.

**TSS0424I ACID aaaaaaaa FOR PROCNAME bbbbbbbb REPLACED WITH
ACID cccccccc**

Reason: This is an informational message indicating that a TSS ADD was done to the STC record for a procname that already exists; however, the ACID parameter was different than the ACID associated with the procname. The current ACID is replaced with the new ACID.

aaaaaaa = the old ACID
bbbbbbbb = the procname
ccccccc = the new ACID

Action: No action required.

TSS0425E SCOPE ACID MUST BE TYPE LSCA OR ZONE

Reason: An attempt was made to assign a scope to an LSCA and one or more of the ACIDs identified in the SCOPE keyword was not a ZONE or an LSCA.

Action: Reenter the command using a valid ZONE or LSCA for the SCOPE.

TSS0426E ADMIN ACID MUST BE TYPE LSCA

Reason: A TSS ADMIN(ACID) SCOPE command was issued and the target of the command was not an LSCA.

Action: Reenter the command using a valid LSCA ACID.

TSS0427E INVALID KEYWORD FOR THIS RESOURCE: xxxxxxxx

Reason: The displayed keyword (xxxxxxx) cannot be used for the given resource.

Action: Correct the command and re-issue it.

TSS0428E INVALID RESOURCE TYPE FOR ATTRIBUTE: xxxxxxxx

Reason: The displayed attribute (xxxxxxx) cannot be used with the given resource type.

Action: Correct the command and re-issue it.

TSS0429E SCOPED PROFILES ARE FOR ZCA, VCA, OR DCA ONLY

Reason: An attempt was made to add profile scopes to an invalid ACID type.

Action: None.

TSS0430I CPF INITIALIZING; COMMAND WILL EXECUTE ON LOCAL NODE ONLY.

Reason: CPF(ON) has been specified, but CCI is either not available or not fully initialized. Until CCI completes initialization, commands entered on the local node will execute only on that node, and will not be propagated. The command also will not be logged to the CPF Recovery File.

Action: Check to determine that CCI has completed initialization (CPF status shows ON, and not INIT) before issuing any commands intended for remote nodes.

TSS0431I YOU MUST SPECIFY AN SDT RECORD TYPE WITH THIS COMMAND

Reason: Administrator has entered TSS LIST(SDT) only and it also requires a record type to identify which type to list.

Action: Re-issue the command giving a record type.

TSS0432E REQUIRED KEYWORD MISSING OR INVALID: xxxxxxxx

Reason: Administrator has entered an ADD or REPLACE command that requires the specified (xxxxxxx) field to be included with correct syntax.

Action: Re-issue the command either correcting or supplying the needed keyword.

TSS0499W UPDATE STC RECORD FOR PROC PROCNAME

Reason: The STC Record has been found to contain a proc called 'procname' which uses the ACID that has just been deleted.

Action: Remove the ACID from the STC Record.

TSS0515E INVALID USE OF (G)ENERIC OPTION

Reason: You have incorrectly used the "G" (Generic prefixing indicator) on a command.

Action: Refer to the *User Guide* for more information on using the (G)eneric indicator.

TSS0599E CA-Top Secret ENVIRONMENT ERROR

Reason: The CA-Top Secret address space was not available.

Action: Retry when CA-Top Secret is available.

TSS0600E USER NOT DEFINED TO CA-Top Secret

Reason: Data was requested on an ACID which does not exist.

Action: Define the ACID to CA-Top Secret or verify that the ACID has been specified correctly.

TSS0700E PCSDSDAYS MUST BE AN INTEGER 1 THROUGH 45

Reason: The subfield value was not between 1 and 45.

Action: Enter a subfield value between 1 and 45.

TSS0701E PCIDLE MUST BE AN INTEGER 0 THROUGH 60

Reason: The subfield value was not between 0 and 60.

Action: Enter a subfield value between 0 and 60.

TSS0702E PCLGTYPE MUST BE AN INTEGER 1 THROUGH 4

Reason: The subfield value was not between 1 and 4.

Action: Enter a subfield value between 1 and 4.

TSS0703E PCMINPWD MUST BE AN INTEGER 1 THROUGH 8

Reason: The subfield value was not between 1 and 8.

Action: Enter a subfield value between 1 and 8.

TSS0900E I/O error. Restore security file from backup.

Reason: I/O subsystem encountered a damaged Security file.

Action: Restore Security Database using procedures outlined in installation guide.

TSS0901E Security file unavailable

Reason: I/O subsystem attempted to access the Security File, but could not access it.

Action: Is the file available or formatted correctly? Collect any dump and/ or console information. Contact CA-Top Secret Technical support for further assistance.

TSS0902E Logical XE error

Reason: I/O subsystem encountered an internal chain error.

Action: Collect any print or console output. Contact CA-Top Secret Technical Support for further details.

TSS0903E Logical Read error

Reason: I/O subsystem encountered an internal read error.

Action: Collect any print or console output. Contact CA-Top Secret Technical Support for further details.

**TSS0905I Unable to enqueue on resource XXXXXXXX - held by system
XXXXXXXXX.**

Reason: CA-Top Secret attempted to enqueue the Security file for update of resource XXXXXXXX - But system XXXXXXXX holds the lock.

Action: None. The system will wait until the enqueue can be obtained.

TSS0905I Unable top obtain security file XXXXXXXX lock.

Reason: CA-Top Secret has been unable to obtain a lock on security file XXXXXXXX, because another system had it locked for XX minutes.

Action: Investigate why the system holding the lock has not released it. A possible reason could be that the system was shut down during an I/O update. Reply RESET if the locking system is unable to release the lock on its own. Reply WAIT if the locking system makes CA-Top Secret retry its lock request. A RESET reply might corrupt the database if another system did not complete its update.

TSS0906I System XXXXX has held XXXXXXX for XX minutes.

Reason: This message is part of a sequence of messages, which are explained under TSS0905I.

Action: Follow action described under TSS0905I.

TSS0907A Reply <RESET> or <WAIT>

Reason: This message is part of a sequence of messages, which are explained under TSS0905I.

Action: Follow action described under TSS0905I.

TSS0908I **WARNING Indiscriminately replying <RESET>**

Reason: This message is part of a sequence of messages, which are explained under TSS0905I.

Action: Follow action described under TSS0905I.

TSS0909I May corrupt the CA-Top Secret file

Reason: This message is part of a sequence of messages, which are explained under TSS0905I.

Action: Follow action described under TSS0905I.

TSS0910I Unable to locate parameter file

Reason: CA-Top Secret was unable to locate its parameter database.

Action: Default startup values will be used until a parameter database has been defined.

TSS0911E Parameter file record length invalid

Reason: The record length of the parameter file appears to be incorrect.

Action: Check if the accessed parameter file was defined correctly with TSSPARM program.

TSS0912E Parameter file read error

Reason: CA-Top Secret encountered a read error of the Parameter file.

Action: Parameter file might be incorrect. Please redefine it with the TSSPARM program.

TSS0913W Recovery File Unavailable

Reason: RECOVERY(ON) has been defined in the CA-Top Secret parameter file, but the file appears to be unavailable.

Action: Please ensure the Recovery file is defined correctly with provided TSSMAINT program and sample from Installation guide. Recovery will remain inactive until a valid recovery file has been detected.

TSS0914W Recovery File Unformatted

Reason: RECOVERY(ON) has been defined in the CA-Top Secret parameter file, but the file appears to be unformatted.

Action: Please ensure the Recovery file is formatted correctly with provided TSSMAINT program and sample from Installation guide. Recovery will remain inactive until a valid recovery file has been detected.

TSS0915W Recovery processing terminated

Reason: A previous error caused recovery to be terminated.

Action: Follow the instructions from the previous Recovery file error, and restart CA-Top Secret.

TSS0916W Recovery file should be reformatted

Reason: Some type of internal error has been detected on the recovery file.

Action: The Recovery file should be reformatted with provided TSSMAINT utility.

TSS0927E SFS invalid DASD device type CUU xxxx

Reason: I/O subsystem encountered an unknown DASD type on device CUU.

Action: Contact CA-Top Secret Technical Support about the type of DASD, to obtain new support.

TSS0933E SFS I/O error CSW=xxxxxxxxxxxxx xxxxxxxxxxxxxxxx CUU=xxxx

Reason: I/O subsystem encountered an I/O error on DASD xxxx.

Action: Contact CA-Top Secret Technical Support personnel about the error.

TSS0942E Security Record damaged or insufficient storage - Try Again

Reason: Either a bad Security record or insufficient storage in the CA-Top Secret address space.

Action: Check storage allocation, retry I/O function. If error persists contact CA-Top Secret Technical Support for further assistance.

TSS0944E Request queue manager failure

Reason: CA-Top Secret queue manager encountered internal error.

Action: Collect possible dump or console output. Contact CA-Top Secret Technical Support for further assistance.

TSS0945E Error Processing Backup file

Reason: CA-Top Secret encountered an error while the backup file was being processed.

Action: Ensure Backup file was Initialized with the same values and DASD type as the Security file, also ensure DASD allocation sizes are identical between the backup and security files.

TSS0946I Deactivating automatic backup

Reason: Either backup was terminated with a CA-Top Secret MODIFY command and the backup file was not available.

Action: Ensure backup file is available and BACKUP(YES) has been specified in the CA-Top Secret parameter dataset.

TSS0947I Security file backup commencing

Reason: Automatic backup of the Security file is commencing.

Action: None. This is an automatic process.

TSS0948I Security file backup completed

Reason: Automatic backup of security file has completed.

Action: None. This is a normal return code.

TSS0949I Fast logging buffer full. Event logging temporarily delayed.

Reason: The pre-allocated log buffer are full, future events will be delayed

Action: Ensure the Audit task is active. Increase buffer size or storage allocations in CA-Top Secret address space.

**TSS0951I CA-Top Secret initialization error -
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX**

Reason: I/O subsystem failed to initialize XXXXXXXXXXXXXXXXXXXX.

Action: Contact CA-Top Secret support for further assistance.

TSS0960E SHARED PROFILE TABLE IS FULL - jobname

Reason: During a signon, the profile sharing table used by this region was found to be full. The signon continues but profiles needed by this user will be privately obtained and not eligible for sharing by other users of the region. When users of a region do not share profiles, region storage is often adversely impacted.

Action: Report this message to security personnel. The size of the shared profile table used by this region may need adjustment. Refer to the PRFT facility option in the CA-Top Secret *Control Options Guide* for more information.

TSS0961W SIGNON FASTPATH UNAVAILABLE RC=xx

Reason: During signon to a region supporting profile sharing, it was detected that CA-Top Secret signon fastpath logic was temporarily unavailable due to system workloads. The current signon continues but without the benefit of signon fastpath performance.

Action: Intermittent issuance of the message, especially during peak periods, does not signify a problem. When available; CA-Top Secret employs ESA AR-mode service facilities to improve signon performance for regions using profile sharing. If these services are frequently unavailable, consider disabling profile sharing for the affected regions.

TSS0962E MAXUSER EXCEEDED - XREF TABLE FULL

Reason: The number of users signed on to a multiuser facility exceeds the value specified for the MAXUSER facility control option.

Action: The MAXUSER control option for the affected facility should be increased appropriately. The region must be recycled for the control option to take effect.

TSS1000E INSUFFICIENT MEMORY.

Reason: TSSCHART was unable to acquire a sufficient amount of memory for its work area.

Action: No action required.

TSS1001E UNABLE TO IDENTIFY MASTER SCA.

Reason: TSSCHART was unable to obtain information about the Master Security Administrator from the CA-Top Secret address space.

Action: No action required.

TSS1002E SECURITY FILE IS EMPTY.

Reason: TSSCHART found no departments, divisions or alternate SCA's in the Security File--that is, there is no information present on the Security File to chart.

Action: No action required.

TSS1003E CA-Top Secret IS UNAVAILABLE AT THIS TIME.

Reason: The CA-Top Secret address space was not currently active when TSSCHART was run. CA-Top Secret is required to obtain Security File information during the charting process.

Action: Rerun when CA-Top Secret is active.

TSS1004E TSS CROSS MEMORY COMMUNICATIONS FAILURE

Reason: This message is issued by TSSCHART when it is unable to service a request (i.e.,TSS is down, VSE system service failure...).

Action: Restart CA-Top Secret if it is down. If this does not work or if the error is not caused by CA-Top Secret, review other dumps occurring at the same time and contact the appropriate vendor.

TSS1005E INSUFFICIENT AUTHORITY FOR TSSCHART.

Reason: The following administration authorities were not found:
ACID(REPORT) and
RESOURCE(REPORT)

Action: Obtain proper administrative authorities and rerun.

TSS1008E KEYWORD keyword - INSUFFICIENT AUTHORITY.

Reason: One of the following was encountered:

- CHART(ACID) was specified without the administrator having ACID(REPORT) authority; or
- CHART(RESOURCE) was specified without the administrator having RESOURCE(REPORT) authority.

Action: No action required.

TSS1009E KEYWORD keyword - INVALID SUBFIELD VALUE.

Reason: An invalid subfield value was specified for the indicated keyword.

Action: Correct subfield value and resubmit.

TSS1010E KEYWORD keyword - ALREADY SPECIFIED.

Reason: Duplicate CHART or RESOURCE keywords were encountered.

Action: Delete duplicate keyword and resubmit.

TSS1011E KEYWORD keyword - CONFLICTING PARAMETER.

Reason: One of the following was encountered:

- DIV and XDIV were both specified
- DEPT and XDEPT were both specified
- PROF and XPROF were both specified
- USER and XUSER were both specified.

Action: Correct keywords and parameters and resubmit.

TSS1012E ACID acid IS NOT WITHIN YOUR SCOPE.

Reason: The specified acid is not within your scope of authority. Only those acids within your scope may be charted.

Action: No action required.

TSS1013E ACID acid IS UNKNOWN/UNDEFINED TO CA-Top Secret.

Reason: The specified acid has not been defined to CA-Top Secret. (The acid has not been created.)

Action: No action required.

TSS1014E ACID acid - PARAMETER/TYPE MISMATCH

Reason: The specified acid type did not match the type of acid expected for that keyword. (A department acid was specified in the DIV or XDIV keyword.)

Action: No action required.

TSS1015E MISSING/INVALID SECURITY ENVIRONMENT

Reason: TSSCHART has found that no security environment has been established for this administrator.

Action: No action required.

TSS1016E TSS/TSSCHART VERSION MISMATCH

Reason: Different versions of CA-Top Secret and TSSCHART are incompatible.

Action: No action required.

TSS1047E TSSCHART MUST EXECUTE APF-AUTHORIZED

Reason: TSSCHART must be executed from an APF authorized library.

Action: Ensure TSSCHART is in an APF authorized library and rerun.

TSS1301I CACHE HAS BEEN CLEARED

Reason: A CACHE(CLEAR) command was issued or the CACHE threshold value was exceeded and the CACHE was cleared.

Action: No action is required, you may wish to increase the CACHE threshold if CACHE is cleared too often.

TSS1302I CACHE COMMAND FAILED

Reason: An error has occurred during the processing of the CACHE command.

Action: Enter a TSS MODIFY CACHE(nnnn) command to start CACHE.

TSS1303I CACHE IS OFF

Reason: You issued the TSS MODIFY CACHE(STATUS) command when CACHE was not active.

Action: Enter a TSS MODIFY CACHE(nnnn) command to start CACHE.

TSS1304I ----- CACHE STATISTICS -----

Reason: These messages provide statistics on how much cache is used and how efficient CACHE is in avoiding extra I/O.

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

SIZE Current amount of storage used. If CACHE overflows, it is automatically cleared and starts to fill again.

CALLS Number of calls made to CACHE.

SATISFIED Number of calls satisfied in CACHE.

CLEARED How many times CACHE was cleared for the life of the CA-Top Secret address space. Clear is also automatically performed whenever a cache request is issued that would cause the CURRENT SIZE to exceed the MAXSIZE.

Action: No action necessary.

TSS1305I MAXSIZE (nnnnnnnnnK) SIZE (nnnnnnnnnK)

Reason: This message is part of a sequence of messages, which are explained under TSS1304I.

Action: Follow action described under TSS1304I.

TSS1306I CALLS (nnnnnnnnn) SATISFIED (nnnnnnnnn)

Reason: This message is part of a sequence of messages, which are explained under TSS1304I.

Action: Follow action described under TSS1304I.

TSS1307I CLEARED (nnnnnnnnn)

Reason: This message is part of a sequence of messages, which are explained under TSS1304I.

Action: Follow action described under TSS1304I.

TSS1308 INVALID REFRESH REQUEST

Reason: An invalid REFRESH option was entered.

Action: Enter a correct option and reissue the REFRESH command.

TSS1309 SAF MODULES REFRESH FAILED

Reason: There are CA-SAF modules missing from your CA-Top Secret library.

Action: Contact your Systems Programmer to have the missing modules loaded.

TSS2000I CA-TSS MSTR INITIALIZATION IN PROGRESS

Reason: This is an informational message indicating that Master Scheduler Initialization has begun.

Action: No action required.

TSS2001I CA-TSS MSTR INITIALIZATION COMPLETE

Reason: This is an informational message indicating that Master Scheduler Initialization has completed.

Action: No action required.

TSS2003I CA-TSS MSTR SAF REPLACEMENT SUCCESSFUL

Reason: The SAF interface has been properly installed.

Action: No action required.

TSS2004I CA-TSS MSTR SAF INSTALLATION SUCCESSFUL

Reason: The CA-Top Secret SAF interface has been properly installed.

Action: No action required.

TSS2020E CA-TSS MSTR INITIALIZATION FAILURE

Reason: One or more errors have occurred during Master Scheduler Initialization.

Action: Check other messages to determine the problem. An IPL and/or other actions may be necessary.

TSS2021E CA-TSS MSTR IPL IS REQUIRED TO CORRECT ERRORS

Reason: An error occurred that can only be corrected by a system IPL.

Action: Check other messages to determine cause of problem. An IPL is necessary.

TSS2022E CA-TSS MSTR TERMINATED WITH USER 2000-nn ABEND

Reason: An error occurred during Master Scheduler Initialization.

Action: Check other messages to determine cause of problem. The abend reason code 'nn' will match the last two characters of the matching error message. For example, if the user abend code reason is '34', then a TSS2034E message will also be issued with other problem related information. An IPL may be necessary.

TSS2023E CA-TSS MSTR TERMINATED BY SYSTEM xxx-nnnn ABEND

Reason: An error occurred during Master Scheduler Initialization.

Action: Check other messages to determine cause of problem. An IPL may be necessary.

TSS2024W CA-TSS MSTR INITIALIZATION COMPLETED WITH ERROR(S)

Reason: An error has occurred during Master Scheduler Initialization.

Action: Check other messages to determine the cause of problem. An IPL will not be required, however may still be advised.

TSS2031E CA-TSS MSTR module WORK AREA GETVIS FAILED

Reason: A work area GETVIS failed during Master Scheduler Initialization.

Action: Check other related messages, correct the error and IPL.

TSS2032E (NO MESSAGE)

Reason: An error occurred during WTO processing, during Master Scheduler Initialization.

Action: Check any other related messages, correct the error and IPL.

TSS2036E CA-TSS MSTR MODULE TSSFRVT CORRUPTED OR INVALID

Reason: Module TSSFRVT has been corrupted or failed other checking.

Action: Reinstall module TSSFRVT and IPL.

TSS2037E CA-TSS MSTR SAFV GETVIS FIELD - RC nn

Reason: Module TSSMSI00 was unable to obtain sufficient SVA for the SAF vector table.

Action: Check for other messages. An IPL will be necessary to correct the problem.

TSS2038E CA-TSS MSTR TSSFR00 INSTALLATION FAILED - RC 00000

Reason: TSSMSI00 was unable to properly install TSSFR00 - the VSE SAF router.

Action: Check for other messages. An IPL will be necessary to correct problem.

TSS2039W CA-TSS MSTR MASTER ADDRESS SPACE ACEE CREATE FAILED

Reason: An error occurred while processing the security environment for the Master Scheduler address space (ASID 1).

Action: Check for other messages. An IPL may be necessary to correct the problem.

TSS5587E AUDIT FILE SYNAD ERROR:

Reason: An unrecoverable I/O error has occurred while accessing the Audit/Tracking File. Execution terminates with a Return Code of 24. This message includes detailed information about the error in the "TEXT" field, as follows:

Column Number Contents

1-6	Type of operation attempted.
8-22	General description of error.
24-37	Actual track address and block number at which error occurred (BBCCHHR in hexadecimal form).
39-44	Access method used

Action: No action required.

Note: We suggest that you enter the 53E abend into the System Recovery Table (SRT) as a recoverable abend. This will avoid a CICS failure in the event any CA-Top Secret generated subtasks fail. Refer to the *Implementation: CICS Guide* for more details.

TSS5800E VXPROXY FORMAT IS (REM_NODE,REM_USER,LOCAL_USER)

Reason: This message was issued in response to a format error in using the VXPROXY keyword.

Action: Reissue the command using the indicated syntax.

TSS5858E EXTENT OVERFLOW IN NDT RECORD

Reason: A serious internal error occurred during command processing. The NDT record structure was inconsistent and resulted in an overflow.

Action: Contact CA technical support.

TSS6000I TSS/CICS INITIALIZATION PHASE 1 STARTED

Reason: CICS has determined that external security is required and issues a RACLIST which prompts TSS/CICS to begin its initialization.

Action: No action required.

Module: TSSCINIT

TSS6001I TSS/CICS INITIALIZATION PHASE 1 COMPLETED

Reason: Phase 1 of 3 has successfully completed.

Action: No action required.

Module: TSSCINIT

TSS6002I TSS/CICS INITIALIZATION PHASE 2 STARTED

Reason: TSS/CICS has entered Phase 2 of its initialization and is setting up its event points.

Action: No action required.

Module: TSSTCINT

TSS6003I TSS/CICS INITIALIZATION PHASE 2 COMPLETED

Reason: TSS/CICS event points set, Phase 2 of 3 completed.

Action: No action required.

Module: TSSTCINT

TSS6004I TSS/CICS INITIALIZATION PHASE 3 STARTED

Reason: TSS/CICS has entered Phase 3 of its initialization and is performing the TSS/CICS subsystem initialization.

Action: No action required.

Module: TSSTCINT

TSS6005I TSS/CICS INITIALIZATION PHASE 3 COMPLETED

Reason: TSS/CICS subsystem initialization complete, Phase 3 of 3 completed.

Action: No action required.

Module: TSSTCINT

TSS6006I TSS/CICS SECURITY INACTIVE

Reason: TSS/CICS security is inactive for this CICS region. There will be no external security checks performed.

Action: No action required.

Module: TSSTCINT/TSSCRT

TSS6007I TSS/CICS SECURITY ACTIVATED

Reason: TSS/CICS security has been activated for this CICS region.

Action: No action required.

Module: TSSTCINT/TSSCRT

TSS6008I TSS/CICS TERMINATION STARTED

Reason: TSS/CICS shutdown phase has started.

Action: No action required.

Module: TSSTCINT

TSS6009E TSS/CICS ERROR TERMINATION CALL PROCESSING

Reason: This message is generated during Phase 2 initialization. TSS/CICS has determined this is not a CICS region. Either no AFCB address was found, or CICS's AFCB header was not identified as "AFCX."

Action: No action required.

Module: TSSTCINT

TSS6010I TSS/CICS TERMINATION COMPLETED

Reason: TSS/CICS has completed its termination process.

Action: No action required.

Module: TSSTCINT

TSS6011E TSS/CICS PM ATTACH PROCESSING ERROR

Reason: TSS/CICS has attempted to attach subtask DFHTSPM0 but the attach request failed.

Action: Examine register 15 for attach return code. If STORAGE shortage, lower CICS region size by 500k.

Module: TSSCPI/TSSCRT

TSS6012E TSS/CICS CM ATTACH PROCESSING ERROR

Reason: TSS/CICS has attempted to attach subtask DFHTTSM0 but the attach request failed.

Action: Examine register 15 for attach return code. If STORAGE shortage, lower CICS region size by 500k.

Module: TSSCPI

TSS6013E TSS/CICS EXTSEC=NO PARAMETER INVALID

Reason: An attempt to set the EXTSEC parameter to NO was denied due to no SYSID entry for this CICS region in the Facilities SYSID Bypass List.

Action: Add the SYSID of the region to the Facilities Bypass List.

Module: TSSCPI/TSSCRT

TSS6014I TSS/CICS EXTSEC=YES PARAMETER IS FORCED

Reason: No SYSID entry in the Facilities Bypass List was found, so the attempt to alter this parameter was overridden. External security remains in force.

Action: No action required.

Module: TSSCPI/TSSCRT

TSS6015I TSS/CICS PTSCECB1 POSTED

Reason: The Facility Matrix External Security Initialization Parameters have overlaid the DFHSIT Security Initialization Parameters.

Action: No action required.

Module: TSSCPI/TSSCRT

TSS6016I TSS/CICS PTSCECB2 POSTED

Reason: TSS/CICS program manager subtask initialization complete.

Action: No action required.

Module: TSSCPI/TSSCRT

TSS6017I TSS/CICS PTSCECB3 POSTED

Reason: TSS/CICS storage manager subtask initialization complete.

Action: No action required.

Module: TSSCPI

TSS6018E TSS/CICS TSSCPI PROCESSING ERROR

Reason: TSS/CICS subtask attach failure.

Action: No action required.

Module: TSSCPI

TSS6019E TSS/CICS FREEVIS ERROR FOR THE PTCB SP=230

Reason: FREEVIS was successful for TSS/CICS Product Token Control Block.

Action: Contact CA-Top Secret Support Center.

Module: TSSCPI

TSS6020E TSS/CICS SUBTASK MANAGER ATTACH FAILURE

Reason: TSS/CICS signon subtask manager attach has failed. (DFHTRAC0)

Action: Examine register 15 for attach return code.

Module: TSSCSMGR

TSS6021E TSS/CICS GETMAIN ERROR TSSCPTCB SP=230

Reason: GETVIS unsuccessful for TSS/CICS Product Token Control Block.
(4000 bytes/SP230)

Action: Reduce CICS region size by 500k.

Module: TSSCPI

TSS6022E TSS/CICS GETMAIN ERROR TSSCCMGR SP=230

Reason: TSS/CICS control block getvis failure.

Action: Reduce CICS region size by 500k.

Module: TSSCPI/TSSCRT

TSS6023E TSS/CICS FREEMAIN ERROR TSSCCMGR SP=230

Reason: TSS/CICS control block FREEVIS failure

Action: Contact CA-Top Secret Support Center.

Module: TSSCPI

TSS6024E TSS/CICS INITIALIZATION SUBTASK GETMAIN ERROR

Reason: STCB getvis failure. (700 bytes/SP=230/24-bit)

Action: Reduce CICS region size by 500k.

Module: TSSCPI/TSSCRT

TSS6025E TSS/CICS INITIALIZATION SUBTASK LOGIC ERROR

Reason: TSSCPM program logic error. Invalid PTS\$ECB3 function request.

Action: Contact CA-Top Secret Support Center.

Module: TSSCPI/TSSCRT

TSS6029E TSS/CICS SECURITY INITIALIZATION FAILURE

Reason: TSS/CICS subtask initialization failure.

Action: This message will be part of other TSS/CICS messages displayed. Obtain console log and call CA-Top Secret Support.

Module: TSSCPI

TSS6030I TSS/CICS INSTALL CHECK ==> FACMATRX=

Reason: Displays the value of FACMATRX TSS/CICS is using for this execution of CICS.

Action: No action required.

Module: TSSCPI/TSSCRT

TSS6031I TSS/CICS INSTALL CHECK ==> EXTSEC=

Reason: Displays the value of EXTSEC TSS/CICS is using for this execution of CICS.

Action: No action required.

Module: TSSCPI/TSSCRT

TSS6032I TSS/CICS INSTALL CHECK ==> XCMD=

Reason: Displays the value of XCMD TSS/CICS is using for this execution of CICS.

Action: No action required.

Module: TSSCPI/TSSCRT

TSS6033I TSS/CICS INSTALL CHECK ==> XDCT=

Reason: Displays the value of XDCT TSS/CICS is using for this execution of CICS.

Action: No action required.

Module: TSSCPI/TSSCRT

TSS6034I TSS/CICS INSTALL CHECK ==> XFCT=

Reason: Displays the value of XFCT TSS/CICS is using for this execution of CICS.

Action: No action required.

Module: TSSCPI/TSSCRT

TSS6035I TSS/CICS INSTALL CHECK ==> XJCT=

Reason: Displays the value of XJCT TSS/CICS is using for this execution of CICS.

Action: No action required.

Module: TSSCPI/TSSCRT

TSS6036I TSS/CICS INSTALL CHECK ==> XPCT=

Reason: Displays the value of XPCT TSS/CICS is using for this execution of CICS.

Action: No action required.

Module: TSSCPI/TSSCRT

TSS6037I TSS/CICS INSTALL CHECK ==> XPPT=

Reason: Displays the value of XPPT TSS/CICS is using for this execution of CICS.

Action: No action required.

Module: TSSCPI/TSSCRT

TSS6038I TSS/CICS INSTALL CHECK ==> XPSB=

Reason: Displays the value of XPSB TSS/CICS is using for this execution of CICS.

Action: No action required.

Module: TSSCPI/TSSCRT

TSS6039I TSS/CICS INSTALL CHECK ==> XDBD=

Reason: Displays the value of XDBD TSS/CICS is using for this execution of CICS.

Action: No action required.

Module: TSSCPI/TSSCRT

TSS6040I TSS/CICS INSTALL CHECK ==> XTRAN=

Reason: Displays the value of XTRAN TSS/CICS is using for this execution of CICS.

Action: No action required.

Module: TSSCPI/TSSCRT

TSS6041I TSS/CICS INSTALL CHECK ==> XTST=

Reason: Displays the value of XTST TSS/CICS is using for this execution of CICS.

Action: No action required.

Module: TSSCPI/TSSCRT

TSS6042I TSS/CICS INSTALL CHECK ==> DSNCHECK=

Reason: Displays the value of DSNCHECK TSS/CICS is using for this execution of CICS.

Action: No action required.

Module: TSSCPI/TSSCRT

TSS6043I TSS/CICS INSTALL CHECK ==> PCTEXTSEC=

Reason: Displays the value of PCTEXTSEC TSS/CICS is using for this execution of CICS.

Action: No action required.

Module: TSSCPI/TSSCRT

TSS6044I TSS/CICS INSTALL CHECK ==> XAPPC=

Reason: Displays the value of XAPPC TSS/CICS is using for this execution of CICS.

Action: No action required.

Module: TSSCPI/TSSCRT

TSS6045I TSS/CICS INSTALL CHECK ==> LTLOGOFF=

Reason: Displays the value of the LTLOGOFF TSS/CICS is using for this execution of CICS.

Action: No action required.

TSS6046I TSS/CICS INSTALL CHECK ==> PCTCMDSEC=

Reason: Displays the value of PCTCMDSEC TSS/CICS is using for this execution of CICS.

Action: No action required.

Module: TSSCPI/TSSCRT

TSS6047I TSS/CICS G U S H C I PROCESSING

Reason: Successful GETVIS of TSS/CICS User Hash Chain Index.

Action: No action required.

Module: TSSCCMGR

TSS6049I TSS/CICS L C N-R D M PROCESSING

Reason: Successfully loaded TSS/CICS Non-Release Dependent Modules.

Action: No action required.

Module: TSSCPM

TSS6050I TSS/CICS L C R D M PROCESSING

Reason: Successfully loaded TSS/CICS Release Dependent Modules.

Action: No action required.

Module: TSSCPM

TSS6051I TSS/CICS L C R R T M PROCESSING

Reason: Successfully loaded TSS/CICS Resource Request Table Module.

Action: No action required.

Module: TSSCPM

TSS6052I TSS/CICS L C E M T M PROCESSING

Reason: Successfully loaded TSS/CICS Error Messages Table Modules.

Action: No action required.

Module: TSSCPM

TSS6053I TSS/CICS L C T M PROCESSING

Reason: Successfully loaded TSS/CICS Table Modules.

Action: No action required.

Module: TSSCPM

TSS6054I TSS/CICS L C P A M PROCESSING

Reason: Successfully loaded TSS/CICS Patch Area Modules.

Action: No action required.

Module: TSSCPM

TSS6055I TSS/CICS L C S M PROCESSING

Reason: Successfully loaded TSS/CICS Stub Modules.

Action: No action required.

Module: TSSCPM

TSS6056I TSS/CICS D C N-R D M PROCESSING

Reason: Successfully deleted TSS/CICS Non-Release Dependent Modules.

Action: No action required.

Module: TSSCPM

TSS6057I TSS/CICS D C R D M PROCESSING

Reason: Successfully deleted TSS/CICS Release Dependent Modules.

Action: No action required.

Module: TSSCPM

TSS6058I TSS/CICS D C R R T M PROCESSING

Reason: Successfully deleted TSS/CICS Resource Request Table Modules.

Action: No action required.

Module: TSSCPM

TSS6059I TSS/CICS D C E M T M PROCESSING

Reason: Successfully deleted TSS/CICS Error Message Table Module.

Action: No action required.

Module: TSSCPM

TSS6060I TSS/CICS D C T M PROCESSING

Reason: Successfully deleted TSS/CICS Table Modules.

Action: No action required.

Module: TSSCPM

TSS6061I TSS/CICS D C S M PROCESSING

Reason: Successfully deleted TSS/CICS Stub Module.

Action: No action required.

Module: TSSCPM

TSS6063I TSS/CICS SECURITY STATUS CHANGE PROCESSING STARTED

Reason: TSS/CICS security parameter modification starting.

Action: No action required.

Module: TSSCRT

**TSS6065I TSS/CICS SECURITY STATUS CHANGE PROCESSING COM-
PLETED**

Reason: TSS/CICS security parameter modification completed.

Action: No action required.

Module: TSSCRT

TSS6067E TSS/CICS SECURITY INITIALIZATION FAILURE

Reason: This message is generated during Phase 3 initialization. Either no AFCB address was found, CICS' AFCB header was not identified as "AFCX", cannot support this release of CICS, the PTCB address cannot be located, TSS/CICS subtask errors or TSSCPI errors.

Action: This message may be part of other TSS/CICS messages displayed. Obtain console log and call CA-Top Secret Support.

Module: TSSTCINT

TSS6068I TSS/CICS D C P A M PROCESSING

Reason: Successfully deleted TSS/CICS Patch Area Modules.

Action: No action required.

Module: TSSCPM

TSS6069I TSS/CICS C S T M A PROCESSING

Reason: The TSS/CICS SIGNON/SIGNOFF subtask manager is being attached.

Action: No action required.

Module: TSSCSMGR

TSS6071E TSS/CICS S S T M INVALID PARAMETER LIST PASSED

Reason: Invalid TXSECREQ request function.

Action: No action required.

Module: TSSCSMGR

TSS6072I TSS/CICS C S T M T PROCESSING

Reason: TSS/CICS SIGNON/SIGNOFF subtask manager terminating.

Action: No action required.

Module: TSSCSMGR

TSS6073I TSS/CICS C S T M WAITING FOR ACTIVE TCBS TO COMPLETE

Reason: TSS/CICS SIGNON/SIGNOFF subtask manager is waiting for all DFHTRAC0 subtasks to complete before terminating.

Action: No action required.

Module: TSSCSMGR

TSS6074E TSS/CICS S S T M G W A PROCESSING ERROR

Reason: TSSCSMGR STCB getvis failure. (700 bytes SP-230)

Action: No action required.

Module: TSSCSMGR

TSS6075I TSS/CICS G U S C B C PROCESSING

Reason: Successful GETVIS of TSS/CICS User Signon Control Block (USCB) Cell Storage.

Action: No action required.

Module: TSSCCMGR

TSS6076I TSS/CICS G U S C B B PROCESSING

Reason: Successful build of the TSS/CICS User Signon Control Block (USCB) Block Storage.

Action: No action required.

Module: TSSCCMGR

TSS6077I TSS/CICS G T T P T PROCESSING

Reason: Successful Getvis of TSS/CICS Task Token Pointer Table storage.

Action: No action required.

Module: TSSCCMGR

TSS6078I TSS/CICS G T T C B C PROCESSING

Reason: Successful Getvis of TSS/CICS Task Token Control Block Cell storage.

Action: No action required.

Module: TSSCCMGR

TSS6079I TSS/CICS G T T C B B PROCESSING

Reason: Successful initialization of the TTPT.

Action: No action required.

Module: TSSCCMGR

TSS6080I TSS/CICS G D U H C I PROCESSING

Reason: Successful GETVIS of TSS/CICS Duplicate User Hash Chain Index Storage.

Action: No action required.

Module: TSSCCMGR

TSS6081I TSS/CICS G D U S B C PROCESSING

Reason: Successful GETVIS of TSS/CICS Duplicate User Signon Block (DUSB) Cell Storage.

Action: No action required.

Module: TSSCCMGR

TSS6082I TSS/CICS G D U S B B PROCESSING

Reason: Successful build of the TSS/CICS Duplicate User Signon Block (DUSB) Block.

Action: No action required.

Module: TSSCCMGR

TSS6083I TSS/CICS MODULE REFRESH SUCCESSFUL FOR _____.

Reason: Transaction TSSC was invoked to reload (refresh) a TSS/CICS module. It was successfully reloaded.

Action: No action required.

Module: TSSCPM

TSS6084E TSS/CICS MODULE LOAD FAILURE FOR _____.

Reason: An attempt was made to refresh a TSS/CICS module via the TSSC transaction, but was unsuccessful.

Action: Retry TSS=NEWC command. If trouble persists, contact CA-Top Secret Support Center.

Module: TSSCPM

TSS6085E SIGNON/SIGNOFF SUBTASK ATTACH DELAYED

Reason: Due to lack of STORAGE.

Action: Reduce MAXSIGN parameter for the facility.

Module: TSSCSMGR

TSS6086E TSS/CICS SM ATTACH PROCESSING ERROR

Reason: Due to lack of STORAGE.

Action: Reduce MAXSIGN parameter for the facility.

Module: TSSCCMGR

TSS6087E TSS COMMAND FAILED, OPERATOR NOT SIGNED ON

Reason: You cannot invoke the TSS command without being signed on to CA-Top Secret.

Action: Signon to terminal using your CA-Top Secret user id and password.

Module: TSSCCTSS

TSS6088I TSS/CICS CORE MANAGER SUBTASK IS ACTIVE

Reason: The CA-Top Secret CICS core manager subtask is currently active.

Action: No action is necessary.

TSS6089I TSS/CICS PROGRAM MANAGER SUBTASK IS ACTIVE

Reason: The CA-Top Secret CICS program manager subtask is currently active.

Action: No action is necessary.

TSS6091E ACCESSOR NOT AUTHORIZED FOR JOB SUBMISSION

Reason: The submitting ACID does not have authority to submit the job with another ACID.

Action: Cross-authorize the submitting ACID to the execution ACID via

TSS PER(subacid) ACID(execacid) - or - TSS ADD(subacid) NOSUBCHK
--

TSS6092E TSS/CICS FACILITY TYPE NOT CICS

Reason: Indicates that the facility type was not CICS.

Action: Re-issue facility type with a valid CICS facility.

TSS6095I TSS/CICS SIGNON MANAGER SUBTASK IS ACTIVE

Reason: The CA-Top Secret CICS signon manager subtask is currently active.

Action: No action is necessary.

TSS6096I TSS/CICS ATTACHING nnnn SIGNON SERVER SUBTASK

Reason: The CA-Top Secret CICS signon server subtask is in the process of attaching nnnn servers.

Action: No action is necessary.

TSS6097I TSS/CICS DETACHING SIGNON SERVER SUBTASK

Reason: CA-Top Secret CICS is detaching the signon server subtask.

Action: No action is necessary.

TSS6098I TSS/CICS DETACHING SIGNON MANAGER SUBTASK

Reason: CA-Top Secret CICS is detaching the signon manager subtask.

Action: No action is necessary.

TSS6100E DSN SECURITY CHECK PROCESSING ERROR

Reason: DSNB/File access error.

Action: Open all CICS files or shutdown DSN security checking.

Module: TSSCXs/TSSCFM

TSS6101I TSS/CICS SIGNON PROCESSING DELAYED. MAXSIGN LIMIT HAS BEEN REACHED.

Reason: MAXSIGN limit set in the CICS facility has been reached. The MAXSIGN action is set to "RETRY", CA-Top Secret will re-attempt the signon after a four second wait.

Action: No action required if the signon retry is successful. If repeated failures, check the MAXSIGN facility control option. Modify the limit or the action control sub-option if appropriate.

Note: In CICS 4.1, the CICS region has to be recycled before the new values of MAXSIGN can take effect.

TSS6102I SIGNON FAILURE FOR 'variable text'

Reason: CA-Top Secret CICS has had a failure for the listed reason.

Action: No action is necessary.

TSS6103I TSS/CICS SIGNON SERVER ATTACH FAILED. UNABLE TO ATTACH SERVER SUBTASK

Reason: CA-Top Secret CICS has had a failure in attaching the signon server, the server subtask will not run until the server is attached.

Action: No action is necessary.

TSS6110E TSS/CICS MAXUSER LIMIT REACHED — SIGNON REJECTED

Reason: The maximum amount of signed-on users allowed in the region was reached, signon attempt rejected. Based on the MAXUSER facility option setting.

Action: Wait one minute and re-attempt the signon. If MAXUSER is frequently reached, consider raising the value of the MAXUSER option.

Module: TSSCRT

TSS6111E TSS/CICS MAXSIGN LIMIT REACHED — SIGNON REJECTED

Reason: The maximum number of concurrent CICS signons was reached. Based on the facility option MAXSIGN. Signon was rejected due to the KILL suboption specified on the MAXSIGN facility option.

Action: Wait one minute and re-attempt the signon. If MAXSIGN is frequently reached, consider raising the value of the MAXSIGN option or set the MAXSIGN suboption to RETRY.

Module: TSSCPOST

TSS6120E INVALID SECURITY PARAMETER LIST PASSED

Reason: The request code found in the Security Parameter List is invalid or not supported.

Action: Contact CA-Top Secret Support Center.

Module: TSSCXs/TSSCXE

TSS6121E SECURITY RESOURCE CHECK PROCESSING ERROR

Reason: No resource class name block found, request failed.

Action: Check if TSS/CICS is properly installed.

Module: TSSCXs

TSS6130E TSS/CICS SIGNON/SIGNOFF PROCESSING ERROR RC=8780

Reason: DFHTRAC0 ACEE/SECREC getvis failure.

Action: Reduce MAXSIGN parameter for the facility.

Module: TSSCPOST

TSS6131E TSS/CICS SIGNON/SIGNOFF PROCESSING ERROR RC=3220

Reason: DFHTRAC0 attach failure due to lack of STORAGE.

Action: Reduce MAXSIGN parameter for the facility.

Module: TSSCPOST

TSS6132E TSS/CICS SIGNON/SIGNOFF PROCESSING ERROR RC=3230

Reason: DFHTRAC0 attach failure.

Action: Contact CA-Top Secret Support Center.

Module: TSSCPOST

TSS6133E TSS/CICS SIGNON/SIGNOFF PROCESSING ERROR RC=0018

Reason: Invalid Parameter List passed to DFHTRAC.

Action: Contact CA-Top Secret Support Center.

Module: TSSCPOST

TSS6134E TSS/CICS SIGNON/SIGNOFF PROCESSING ERROR RC=0099

Reason: TSSCRINT STCB getvis error.

Action: Lower MAXSIGN parameter of the facility matrix.

Module: TSSCPOST

TSS6135E TSS/CICS SIGNON/SIGNOFF PROCESSING ERROR - RC=ERROR

Reason: DFHTSSM0 subtask attach error (DFHTRAC0).

Action: Contact CA-Top Secret Support Center.

Module: TSSCPOST

TSS6140E TSS/CICS SECURITY TAMPERING CAUSED BY < _____ >

Reason: Security violation detected.

Action: Message and additional information may be located in the security log.

Module: TSSCTSS

TSS6151E TSS/CICS GETVIS FAILURE RETURNED FROM RACINIT

Reason: A CICS signon (RACINIT) was attempted, but failed due to getvis failure in the base CA-Top Secret system.

Action: Lower CICS Region by 500k. If trouble persists, contact CA-Top Secret Support Center.

Module: TSSCPOST

TSS6152E TSS/CICS BAD PARAMETER LIST RETURNED FROM RACINIT

Reason: A CICS signon (RACINIT) was attempted, but failed due to invalid parameter passed to the base CA-Top Secret system.

Action: Contact CA-Top Secret Support Center.

Module: TSSCPOST

TSS6153E TSS/CICS BAD RETURN FROM RACINIT

Reason: A CICS signon (RACINIT) was attempted, but failed due to unknown reason.

Action: Contact CA-Top Secret Support Center.

Module: TSSCPOST

TSS6200E TSS Command OS Attach Failure <EP=TSS>

Reason: A subtask creation for the TSS command failed due to an attach failure.

Action: Contact CA-Top Secret Support Center.

Module: TSSCCTSS

TSS6201E CA-TSS is not Active

Reason: CA-Top Secret was found not to be active.

Action: Start the CA-Top Secret address space.

Module: TSSCCTSS

TSS6202E TSS Command Transaction Processing Error <ECB= -0>

Reason: The DETACH for the TSS command failed.

Action: Contact CA-Top Secret Support Center.

Module: TSSCCTSS

TSS6203I TSS Command Transaction Processing Error

Reason: No data was returned from the TSS command.

Action: Contact CA-Top Secret Support Center.

Module: TSSCCTSS

TSS6300I TSS/CICS UNLOCK FUNCTION SUCCESSFUL

Reason: Valid CA-Top Secret password was entered, terminal unlocked.

Action: No action required.

Module: TSSCTSS

TSS7000I acid LAST-USED date time SYSTEM=id FACILITY=facility

Reason: This message displays after successful initiation as controlled by FACILITY/LUMSG, where:

acid the accessor id associated with the job or session

date date when the ACID was last used (day,month,year)

time time when the ACID was last used (hour,minutes)

id SMF ID of the CPU on which the ACID was used

facility system facility last used

Action: No action required.

TSS7001I COUNT=nnnnn MODE=mode LOCKTIME=nnn NAME=name

Reason: The "status" message presented on successful initiation as controlled by FACILITY/STMSG control option, where:

COUNT number of times, to date, that the ACID has been used

MODE user's current MODE--i.e.,DORMANT,IMPL,WARN,FAIL

LOCKTIME
default terminal locking time

NAME name assigned to the user ACID

Action: No action required.

TSS7002I YOUR TIMEZONE ADJUSTMENT FACTOR IS #nn HOURS

Reason: The "status" message indicates the value set by the TZONE keyword. The TZONE keyword allows you to adjust for time zone differences between the user's actual workstation and the CPU.

Action: No action required.

TSS7003W PASSWORD WILL EXPIRE ON mm/dd/yy

Reason: The current password for the facility will expire on the date displayed.

Action: Change the password soon.

TSS7004W USE OF ACCESSORID EXPIRES ON mm/dd/yy

Reason: The user's ACID for the facility is about to become invalid.

Action: No action required.

TSS7011A PLEASE ENTER YOUR *NEW* PASSWORD OR 'RANDOM'

Reason: CA-Top Secret requires your new password(s).

Action: Enter your new CA-Top Secret password. The password must follow the rules outlined in the NEWPW control option. Enter "RANDOM" if you want the system to randomly generate a new password for you.

**TSS7013I INCLUDING NAMES,LOCATIONS, LICENSE/PHONE
NUMBERS,SSN/SIN**

Reason: This is an informational message only. Using personal information in a password makes it easier for someone to guess a user's password.

Action: No action required.

TSS7015I Format is Password/New Password/Reverify Password

Reason: Your password(s) were entered incorrectly. The correct format is displayed.

Action: No action required.

TSS7016A ENTER NEW PASSWORD AGAIN FOR REVERIFICATION

Reason: Either CA-Top Secret wants to make sure that the user entered (and/or remembers) the new password correctly, OR the user entered a "verification" password that did not match the new password.

Action: Re-enter the password, being careful to match the original password exactly. If, after **two** verification retries, the passwords still do not match, the user receives a TSS7111E and a DRC(015).

**TSS7020A RANDOM PASSWORD ABOUT TO BE DISPLAYED; HIT ENTER TO
CONTINUE**

Reason: A CA-Top Secret-generated "RANDOM" password will be displayed until you press ENTER.

Action: Read and memorize the password. Then erase the password by pressing ENTER.

TSS7021I YOUR NEW PASSWORD IS password

Reason: Either your password expired and CA-Top Secret assigned a new password to you OR you specified "RANDOM" as the new password.

Action: Memorize your new password. To maintain a high level of security, do not write the new password down. Press the ENTER key.

TSS7022A MEMORIZE PASSWORD & HIT ENTER KEY - DO *NOT* RECORD

Reason: Either your password expired and CA-Top Secret assigned a new password to you OR you specified "RANDOM" as the new password.

Action: Memorize your new password. To maintain a high level of security, do not write the new password down. Press the ENTER key.

TSS7030I PASSWORD CHANGED

Reason: You have successfully changed your password.

Action: No action required.

TSS7050I J=jobname A=acid -MRO ATTRIBUTE IGNORED

Reason: An ACID with the MRO attribute specified signed on to an already existing address space. The MRO attribute is only assigned to the control ACID with which a job or STC is initiated in the address space.

jobname the name of the job or started task to which the ACID was signing on.

acid accessor id assigned the MRO attribute.

Action: If an error has been made assigning the ACID the MRO attribute, issue the following TSS command to remove the attribute: **TSS REMOVE(acid) MRO**.

TSS7052W CURRENT PASSWORD EXPIRED-PREVIOUS BATCH PASSWORD USED

Reason: Your password has expired. The system is using the expired password to run the submitted batch job. The HPBPW option, which limits the number of days the expired password will be honored, is active.

Action: Change your password as soon as possible.

TSS7053I DEFAULT ACID <acid name> ASSIGNED

Reason: This is a reminder that you have been assigned the displayed default ACID.

Action: No action required.

TSS7054I SECURITY BYPASS ACTIVE FOR JOB=jobname ACID=acid

Reason: This is to notify you that the specified job/user is using an ACID that is bypassing security. This may also occur if jobs start while CA-Top Secret is being initialized and your DOWN control option specifies Bypass.

Action: No action required.

TSS7100E drc J=jobname A=acid T=terminal F=facility - reason

Reason: This summary violation message displays when a system logon is rejected by security. The message is routed to any active security console.

drc detailed reason code indicates the type of violation

jobname name of job or user that received the violation

acid accessor id for which the violation occurred
terminal the online terminal or batch reader related with the user or job
facility the facility that was being used
reason short explanation of the error may be present

Action: No action required.

TSS7101E PASSWORD IS INCORRECT

Reason: The password supplied for the ACID is invalid. Access to the facility will not be allowed unless the correct combination of ACID and password is supplied.

Action: Supply the correct password.

TSS7102E PASSWORD MISSING

Reason: The required password for the ACID was not supplied. Access to the facility will not be allowed unless the correct combination of ACID and password is supplied.

Action: Supply a password.

TSS7110E PASSWORD HAS EXPIRED. NEW PASSWORD MISSING

Reason: The current password is no longer valid. A new password must be entered to replace the current one.

Action: User must supply current and new passwords.

TSS7111E NEW PASSWORD CHANGE INVALID - reason

Reason: The new password supplied for the ACID is invalid. If the current password has expired, access to the facility will not be allowed until correct combination of ACID and passwords is supplied.

Action: Correct the new password as indicated by the "reason" in the message.

TSS7112E INVALID CHARACTER IN PASSWORD

Reason: Your password contains a character other than A through Z, 0 thru 9, \$, #, and @.

Action: Reenter your password.

TSS7115E REVERIFY PASSWORD NOT THE SAME AS NEW PASSWORD

Reason: Reverify password was entered incorrectly or is not the same as the new password entry.

Action: Re-enter the password being careful to match the new password exactly.

TSS7116E REVERIFY PASSWORD DOES NOT MATCH. TRY AGAIN.

Reason: The new password was entered twice for verification (see message TSS7010A). The entries do not match, which indicates that a typing error was made.

Action: Carefully reenter the request to change your password.

TSS7120E PASSWORD VIOLATION THRESHOLD EXCEEDED

Reason: The user has tried, but failed, to enter the correct password too many times. The number of acceptable unsuccessful attempts is determined by the PTHRESH setting. In any event, the ACID is suspended.

Action: The Security Administrator must remove the SUSPEND attribute from the ACID.

TSS7130E OPERATOR ID CARD REQUIRED FOR LOGON/SIGNON

Reason: The user did not supply an Operator ID Card for logon.

Action: The user must specify the OIDCARD keyword on the TSS LOGON command. CA-Top Secret will prompt the user to insert the OID card.

TSS7131E OPERATOR ID CARD INCORRECT

Reason: The user did not supply the correct OIDCARD for the ACID.

Action: No action required.

TSS7132E VOICE OR DIGITIZED IMAGE VERIFICATION FAILED

Reason: A logon/signon was rejected because the security device did not recognize the user.

Action: No action required.

TSS7140E ACCESSOR ID HAS EXPIRED; NO LONGER VALID

Reason: The FOR or UNTIL keyword of an ACID has expired. The ACID can no longer be used.

Action: Report to the Security Administrator to renew the ACID.

TSS7141E USE OF ACCESSOR ID SUSPENDED

Reason: Use of the ACID has been revoked.

Action: An administrator must remove the ACID's suspension by using the TSS REMOVE function.

TSS7142E ACCESSOR ID NOT YET AVAILABLE FOR USE - STILL INACTIVE

Reason: Use of the ACID has been temporarily revoked.

Action: An administrator must remove the ACID's suspension by using the TSS REMOVE function.

TSS7143E ACCESSOR ID HAS BEEN INACTIVE TOO LONG

Reason: From the day on which the password expired, ACID has been inactive longer than the interval set by the INACTIVE control option.

Action: The Security Administrator should replace the password, and specify the expiration interval or expire option.

TSS7144E ACCESSOR ID MISSING

Reason: An attempt to access the system failed; the ID card did not contain an ACID.

Action: Supply the ACID on the ID card.

TSS7145E ACCESSOR ID <acid> NOT DEFINED TO SECURITY

Reason: The ACID is not defined to the Security Record.

Action: The Security Administrator can CREATE the desired ACID.

TSS7160E FACILITY <facility> NOT AUTHORIZED FOR YOUR USE

Reason: The ACID is not authorized to access the named system facility.

Action: The ACID must obtain proper authorization from his CA-Top Secret administrator.

TSS7161E FACILITY <facility> NOT AVAILABLE THIS DAY

Reason: Access to the facility is controlled on a time-of-day basis.

Action: Log on to the facility at the authorized time.

TSS7162E FACILITY <facility> NOT AVAILABLE THIS DAY.

Reason: Access to the facility is controlled on a day-to-day basis.

Action: Log on to the facility on the authorized day.

TSS7170E ID ORIGINATED FROM PROTECTED READER reader

Reason: The origin of this job is a defined reader (local or RJE) for which the user ACID does not have access authority. The ACID is not authorized for the TERMINAL.

Action: No action required.

TSS7171E UNAUTHORIZED SOURCE OF SYSTEM ENTRY

Reason: The ACID (job or user id) cannot be used from this terminal or reader. The ACID source of origin is restricted by the SOURCE option to prevent its unauthorized use.

Action: No action required.

TSS7172E YOUR ACCESSOR ID IS ALREADY IN USE ON TERMINAL terminal

Reason: The ACID is already signed on to the online subsystem at the designated terminal and the facility does not allow multiple signons.

Action: Although it is not recommended, multiple signons are permitted by the FACILITY/SIGN(M) option.

**TSS7173E AUTOMATIC TERMINAL SIGN-ON NOT ALLOWED FOR
ACID=acidname. PLEASE SIGN ON**

Reason: CA-Top Secret attempted to perform automatic sign-on based upon the terminal ID, and found that the ACID for the terminal had the NOATS attribute.

Action: Sign on by specifying a valid ACID name and password.

TSS7174E ONLY A TYPE(USER) ACID CAN BE USED FOR SYSTEM ENTRY

Reason: An attempt was made to initiate a job or on-line session using an ACID defined as TYPE(DEPT or DIVISION or PROFILE).

Action: A "user" ACID or "control" ACID should be used.

TSS7175E INITIATION DENIED BY SITE SECURITY EXIT

Reason: LOGON or job initiation has been failed by your installation exit.

Action: No action required.

TSS7176E OPERATOR NOT SIGNED ON, PLEASE SIGN ON

Reason: A transaction was entered without first signing on.

Action: Log on to the facility, using your CA-Top Secret ACID and password.

TSS7180E SECURITY IS INACTIVE - DOWN OPTION IS "FAIL"

Reason: CA-Top Secret is not active. If the facility is operating in any mode other than DORMANT, all requests will fail.

Action: No action required.

TSS7181E END OF DAY - NO FURTHER SYSTEM ACCESS ALLOWED

Reason: Operations is in the process of shutting down the system. CA-Top Secret has already been deactivated. No new jobs or sessions can be initiated.

Action: To reset the system, enter an authorized RESETEOD control option.

TSS7182E FACILITY DEACTIVATED BY ADMINISTRATOR. TRY LATER

Reason: The facility being accessed is not available for job/session initiation. The SCA has defined the facility as unavailable.

Action: Retry request at a later time.

TSS7183I SIGNON SERVICES ARE BUSY. PLEASE TRY AGAIN LATER.

Reason: The signon servier is in use, CA-Top Secret CICS cannot attach it until it become available.

Action: No action required.

**TSS7185E PASSWORD VIOLATION FOR CENTRAL SECURITY ADMINIS-
TRATOR AT T=terminal**

Reason: While attempting to use the master security administrator's ACID, on the named terminal, the MSCA did not supply a correct password. Possible breach of security.

Action: No action required.

**TSS7186I SUSPENDED CENTRAL SECURITY ADMINISTRATOR
ATTEMPTING SIGNON**

Reason: The MSCA ACID has been suspended and has signed on and entered the correct password.

Action: No action required.

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

Reason: This message is part of a sequence of messages, which are explained under TSS7186L.

Action: Enter Y to allow access or enter N to deny access.

Note: Depending on your current release of VSE/ESA, you may need to respond to this message multiple times.

TSS7188I REFRESH TRACE DATA

Reason: Data is traced when the Security Record is being refreshed.

Action: This is an informatinal message. No action needed.

TSS7190E ID=jobname ACID=acid VIOLATION THRESHOLD EXCEEDED

Reason: The session identified by "jobname" for the acid has accumulated more violations than allowed by the VTHRESH control option. This message indicates a possible breach of security.

Action: No action required.

TSS7191E ID/SESSION CANCELLED - EXCESSIVE VIOLATIONS

Reason: A user exceeded the maximum number of allowable violations set by VTHRESH, and the site has specified the VTHRESH (nn,CANCEL) option. The session is automatically cancelled.

Action: No action required. If the VTHRESH option also specifies the SUSPEND parameter, the SUSPEND attribute must be removed from the ACID.

TSS7192E SESSION LOCKED - EXCESSIVE VIOLATIONS: SIGNOFF

Reason: The user has exceeded the allowable number of violations, as determined by the VTHRESH setting. The session is automatically cancelled.

Action: Sign off, and then sign on to unlock the session.

TSS7193E UNLOCK REJECTED - PASSWORD IS INCORRECT

Reason: The wrong UNLOCK password was entered. The terminal remains locked.

Action: To unlock the terminal, enter: TSS UNLOCK. When prompted, enter your signon password.

TSS7194E COMMAND REJECTED - TERMINAL IS LOCKED

Reason: The terminal being used is currently locked, making it unavailable to all commands except TSS UNLOCK.

Action: To unlock the terminal, enter: TSS UNLOCK. When prompted, enter your signon password.

TSS7195E Resource Violation Threshold Exceeded

Reason: ACID has exceeded the VTHRESH (violation threshold) during this session.

Action: User will have to log off to reset violation count.

TSS7196E CA-TOP SECRET SECURITY HAS LOCKED THIS TERMINAL

Reason: CA-Top Secret rejected the transaction because the terminal was locked either by a user or by the automatic terminal locking feature.

Action: A terminal can be unlocked by entering the TSS UNLOCK command and the correct signon password.

TSS7197A SPECIFY YOUR PASSWORD TO USE THIS TRANSACTION

Reason: Your password must be verified in order for the transaction to continue.

Action: Enter your password.

TSS7198A SPECIFY YOUR PASSWORD TO UNLOCK THIS TERMINAL

Reason: CA-Top Secret has locked the terminal. The transaction cannot continue.

Action: Enter your password.

**TSS7199A ENTER PASSWORD TO UNLOCK: CSSF OR CLEAR KEY TO
SIGNOFF**

Reason: CA-Top Secret has locked the terminal, the transaction cannot continue.

Action: Enter your password to unlock the terminal, enter "CSSF" or press the Clear key to sign the terminal off.

TSS7200E drc J=jobname A=acid VOL=volser ACC=rlevel/alevel

Reason: This is a summary volume violation message.

drc detailed error reason code for violation

jobname name of job or user session that caused the violation

acid accessor id associated with the job or user

volser name of volume being violated

alevel the attempted access level

rlevel the user's requested access level

Action: No action required.

TSS7201E VOLUME volser NOT AUTHORIZED FOR ACCESS

Reason: An unauthorized ACID attempted to access a volume which he or she was not properly authorized to use.

Action: No action required.

TSS7202E VOLUME volser NOT AVAILABLE THIS TIME PERIOD

Reason: The volume is accessible during a restricted time period only.

Action: No action required.

TSS7203E VOLUME volser NOT AVAILABLE THIS DAY

Reason: Volume access is permitted only on certain days.

Action: No action required.

TSS7204E VOLUME volser NOT AVAILABLE THROUGH THIS FACILITY

Reason: Users must access the volume through an authorized facility.

Action: No action required.

**TSS7205E VOLUME volser NOT ACCESSED THROUGH AUTHORIZED
PROGRAM**

Reason: The volume access is restricted via a PRIVPGM rule. The program in use is unauthorized.

Action: No action required.

TSS7206E VOLUME volser ACCESS DENIED BY SITE EXIT

Reason: The attempted access of a volume or data set on a volume failed during the installation exit's volume access validation.

Action: No action required.

TSS7207E VOLUME volser REQUESTED ACCESS LEVEL (level) NOT AUTHORIZED

Reason: An attempt to access a volume or a data set on a volume was not allowed. The user did not own the volume or was not PERMITTED to the volume at the requested access level.

Action: No action required.

TSS7208E VOLUME volser NOT AUTHORIZED FOR DATASET CREATION

Reason: A data set cannot be created on the volume because 1) the volume is undefined, or 2) the user is not permitted volume access on the "CREATE" level.

Action: No action required.

TSS7209E VOLUME volser ACCESSED BUT NO DATASET NAME PROVIDED

Reason: The user specified a volume but did not specify a data set name with ACCESS(CREATE).

Action: No action required.

TSS7210E VOLUME volser LABEL=BLP VIOLATION

Reason: An unauthorized attempt was made to use Bypass Label Processing (BLP) for a volume.

Action: No action required.

TSS7220E drc J=jobname A=acid VOL=volser ACC=level DSN=dsname

Reason: This is the summary violation message for unauthorized attempts to access a protected data set. The message is sent to the Security Console, routcde=9.

Action: No action required.

TSS7221E DATASET NOT ACCESSIBLE - dsname

Reason: User ACID does not own or is not authorized to access the named data set.

Action: The ACID must be authorized by an administrator via the TSS PERMIT function.

TSS7222E DATASET NOT AVAILABLE DURING THIS TIME PERIOD

Reason: Access to the dataset is protected on a time-of-day basis.

Action: No action required.

TSS7223E DATASET NOT AVAILABLE THIS DAY

Reason: The access to a data set is protected on a day-to-day basis. At present, access to the data set is not permitted.

Action: No action required.

TSS7224E DATASET NOT AVAILABLE THROUGH THIS FACILITY

Reason: The access to a data set is protected on a facility basis. The current facility is not authorized.

Action: No action required.

TSS7225E DATASET NOT ACCESSED THROUGH AUTHORIZED PROGRAM

Reason: An attempt was made to access a specially protected data set by using a program that was not authorized (via TSS PERMIT PRIVPGM), or the program was not loaded from the library indicated by the LIBRARY parameter on the permit. A PRIVPGM can be in a library that is linklisted as well as specified by the LIB parameter.

Action: No action required.

TSS7226E DATASET ACCESS DENIED BY SITE EXIT

Reason: The site exit failed access to a data set.

Action: Check with your site programmers to determine the purpose of the installation exit code.

TSS7227E access ACCESS NOT GRANTED TO DATASET- dsname

Reason: An ACID is permitted some access to a data set; however, he does NOT possess the required access level for a function he wishes to perform on that data set.

Action: An administrator must authorize the ACID to the data set at the correct access level via the TSS PERMIT function using the ACCESS parameters.

TSS7230E DSNAME: dsname

Reason: Indicates the data set for which access was denied.

Action: No action required.

TSS7231E UNAUTHORIZED ID/STEP/TASK LIBRARY FOR DATASET

Reason: An attempt was made to access a specially protected data set. The library containing the privileged program that is opening the data set is not one which was authorized by the owner.

Action: The library must be authorized by the owner via a TSS PERMIT LIBRARY operation.

TSS7232E access ACCESS DENIED TO FETCH-PROTECTED DATASET

Reason: An attempt was made to open a FETCH-only program library. (If <access> = READ, the open was attempted by a system program that does not perform FETCH access.)

Action: No action required.

TSS7234E FETCH VIOLATION

Reason: User attempted to perform a non-FETCH operation against a FETCH-protected data set.

Action: User needs appropriate access level.

TSS7235E DATASET GLOBALLY RESTRICTED - dsname

Reason: This situation has occurred:

1. A user is attempting to open a VSAM dataset by a component instead of by cluster, which is the standard VSAM access method.

Action: No action required.

TSS7250E drc J=jobname A=acid TYPE=type RESOURCE=resource

Reason: This is a summary security violation message which reports unauthorized resource access. Message is routed to Security Console.

Action: No action required.

TSS7251E ACCESS DENIED TO resclass<resname>

Reason: The user is not allowed to access the named resource.

Action: No action required.

TSS7252E ACCESS DENIED THIS DAY TO resclass<resname>

Reason: The resource is protected on a day-to-day basis. It is not available today.

Action: No action required.

**TSS7253E ACCESS DENIED DURING THIS TIME PERIOD TO
resclass<resname>**

Reason: The resource is available during restricted hours only. It is currently not available.

Action: No action required.

**TSS7254E ACCESS NOT AVAILABLE THROUGH THIS FACILITY TO
resclass<resname>**

Reason: The access to the named RESOURCE is illegal because an unauthorized facility is being used.

Action: No action required.

**TSS7255E ACCESS NOT PERFORMED THROUGH AUTHORIZED PROGRAM
TO resclass<resname>**

Reason: An attempt was made to access the named resource but the wrong program was in control.

Action: No action required.

TSS7256E ACCESS DENIED BY SITE EXIT to resclass<resname>

Reason: Your site exit refused the user access to the named resource.

Action: No action required.

TSS7257E UNAUTHORIZED ACCESS LEVEL FOR resclass<resname>

Reason: An attempt was made to access a resource at the wrong level.

Action: No action required.

TSS7258E PROGRAM cmd IS NOT AUTHORIZED FOR YOUR USE

Reason: ACID is not authorized to use the named command.

Action: No action required.

TSS7259E ACCESS DENIED TO A RECORD IN <resclass>

Reason: User has attempted to access a protected record to which he is not authorized.

Action: If access to the record is valid, then a CA-Top Secret administrator must grant security access to that record.

TSS7265E TRANSACTION REVERIFY PASSWORD INCORRECT

Reason: The password that was entered in an attempt to proceed with the transaction was incorrect.

Action: No action required.

TSS7266E TRANSACTION REVERIFY PASSWORD MISSING

Reason: The transaction requires that a password be entered before the user can proceed.

Action: Self-explanatory.

TSS7267E YOU ARE NOT AUTHORIZED TO USE TRANSACTION - transaction

Reason: The job submission request was failed by the site's security exit code.

Action: Check with your site programmers to determine the purpose of the installation exit code.

TSS7270E ID SUBMIT/ACID AUTHORIZATION FAILED BY SITE SECURITY EXIT

Reason: This message is a part of a sequence of messages, which are explained under TSS7267E.

Action: Follow action described for TSS7267E.

TSS7272E ID SUBMIT/ACID AUTHORIZATION DENIED. ACID <acidname> NOT AUTHORIZED THROUGH THIS FACILITY FACILITY

Reason: An attempt was made to submit a job with a hard coded USER= in the JCL, and the ACID specified in the USER= is not authorized through this facility.

Action: Either remove the USER= from the JCL, or submit the job from another facility.

TSS7273E ID SUBMIT/ACID AUTHORIZATION DENIED. ACID <acidname> NOT ACCESSED THROUGH AUTHORIZED PROGRAM PROGRAM

Reason: PRIVPGM on permit to ACID.

Action: Submit through authorized program.

TSS7279E RESTRICTED PROGRAM xxxxxxxx IS NOT AUTHORIZED FOR YOUR USE

Reason: You are trying to execute a program that you are not authorized to use.

Action: Delete or correct the program name.

TSS7299I J=jobacid A=acidname TYPE=resclass RES=resource

Reason: CA-Top Secret sends this message to the security console to log access to resources permitted with an ACTION(NOTIFY).

Action: No action required.

TSS7450I LMP VERIFICATION COMPLETE

Reason: LMP product key verification completed successfully. This message is issued in response to an F TSS,LMPCHECK operator console command.

Action: No action required.

TSS7453W CA-TOP SECRET OPERATING IN WARN MODE UNTIL THE ABOVE ERROR IS CORRECTED

Reason: CA-Top Secret has switched to WARN mode due to an error in LMP product key verification. The previous message indicates the cause of the problem. All accesses that normally would be prevented will be allowed and logged.

Action: Take the action as indicated by the previous message.

TSS7454I CA-TOP SECRET NORMAL PROCESSING RESTORED

Reason: CA-Top Secret has successfully verified the LMP product keys and is no longer running in WARN mode.

Action: No action is necessary.

TSS7455I CA-Top Secret failed to verify provided IBM CUST or IBMPASS parameter

Reason: Either an incorrect IBM customer number was provided in IBM CUST or an incorrect IBM license key was provided in IBMPASS.

Action: Ensure proper values were entered in the CA-Top Secret Parameter file. Contact IBM support for further assistance.

TSS7456I Reexecute TSSMNGR job when keys have been corrected.

Reason: CA-Top Secret needs to be restarted to correct key problem.

Action: Either correct LMP key problem and reload with CAIRIM or correct IBM key or customer number problem and restart CA-Top Secret.

TSS7457E CA-TOP SECRET REQUIRES A LMP KEY TO RUN

Reason: No LMP Key was provided for this CPU.

Action: Make sure the LMP key for this CPU is properly installed in the key file of CAIRIM in your SYS1.PARMLIB.

TSS7458I IBM key verification complete

Reason: CA-Top Secret completed verifying IBM license information

Action: None

TSS7800A TSS IS NOT ACTIVE, REPLY <Y> OR <N> TO CONTINUE WITHOUT TSS SECURITY.

Reason: During IDMS/DC initialization, CA-Top Secret is not active.

Action: A reply of <Y> allows IDMS/DC to continue without CA-Top Secret security. A reply of <N> causes IDMS/DC to abend with a S913 abend code.

TSS7802I CA-TOP SECRET IDMS/DC INTERFACE INITIALIZATION COMPLETE

Reason: The CA-Top Secret IDMS/DC Interface has been activated, and is fully initialized.

Action: No action required.

TSS8001E CA-TOP SECRET MUST BE ACTIVE

Reason: CA-Top Secret must be active to run TSSUTIL.

Action: Wait until CA-Top Secret is active, then rerun TSSUTIL.

TSS8002E USER NOT DEFINED TO CA-TOP SECRET

Reason: Data requested on an ACID which does not exist.

Action: Define the ACID to CA-Top Secret or verify that the ACID has been specified correctly.

TSS8003E NO AUTHORITY TO USE THIS FUNCTION

Reason: The ACID requesting this function must be defined to CA-Top Secret as an SCA.

Action: An SCA ACID must request this function.

TSS8004E NO AUTHORITY (NOT YOUR DEPT)

Reason: The user requested data on a department outside of his scope.

Action: Correct TSSUTIL parameters for access to the department.

TSS8005E NO AUTHORITY (NOT YOUR DIVISION)

Reason: The user requested data on a division outside of his scope.

Action: Correct TSSUTIL parameters for access to the division.

TSS8006E DEPARTMENT UNKNOWN

Reason: The department requested doesn't exist.

Action: Define the department to CA-Top Secret.

TSS8007E ACCESSOR ID UNKNOWN

Reason: Data requested on an ACID which does not exist.

Action: Define the ACID to CA-Top Secret or verify that the ACID has been specified correctly.

TSS8008E ACCESSOR ID DOES NOT BELONG TO YOUR DEPARTMENT

Reason: ACID requested is outside the department's scope.

Action: Correct the department's control statement to include the ACID in the department's scope.

TSS8009E ERROR IN CONTROL STATEMENT

Reason: One of the control statements is incorrect.

Action: Refer to the *Report and Tracking Guide* for correct syntax.

TSS8010E INVALID CONTROL STATEMENT <xxxxx>

Reason: Selected invalid criteria options for the types of incidents to be processed.

Action: Refer to the *Report and Tracking Guide* for the correct criteria options.

TSS8011E DCA CANNOT SUPPLY DEPT OPTION

Reason: The DCA ACID cannot specify department.

Action: Delete the department control statement from the DCA; the default is the DCA's department.

TSS8012E DEPARTMENT DOES NOT BELONG TO YOUR DIVISION

Reason: The VCA is requesting a department outside of his scope.

Action: Delete the department control statement from the VCA or request a department within the scope; the default is all of the VCA's department.

TSS8013E DIVISION UNKNOWN

Reason: The division requested is not defined to CA-Top Secret.

Action: Define the division to CA-Top Secret or correct the existing division.

TSS8014E DIVISION NOT WITHIN YOUR SCOPE

Reason: Self-explanatory.

Action: Delete or correct the division control statement.

TSS8015E DEPARTMENT NOT WITHIN YOUR SCOPE

Reason: Self-explanatory.

Action: Delete or correct the department control statement.

TSS8016E ACCESSOR ID NOT WITHIN YOUR SCOPE

Reason: The specified ACID is not within your scope of authority. ACID must be an SCA to run the report.

Action: Request SCA to run the report, or delete ACID(*) from the control statement.

TSS8017E INSUFFICIENT REPORT AUTHORITY

Reason: User does not have ACID(REPORT) administrative authority.

Action: Refer to the *Report and Tracking Guide* for the correct administrative authorities.

TSS8018E INVALID DATE OR TIME SPAN

Reason: Self-explanatory.

Action: Enter the correct date and time in the proper format.

TSS8019E STORAGE GETMAIN FAILED

Reason: Insufficient storage was available for internal buffers. Execution terminates with a Return Code of 16.

Action: No action required.

TSS8020E CROSS MEMORY QUEUE FAILURE RC=xxx

Reason: A cross-memory failure occurred when TSSUTIL attempted to obtain security information. Execution terminates with a Return Code of 12.

Action: No action required.

TSS8021E UNDEFINED RESOURCE CLASS NAME: xxxxxxxx

Reason: Classname given is not defined to the RDT.

TSS8022E SMFIN AUDIT FILE NOT PREFORMATTED.

Reason: Internal format of Audit File is invalid.

Action: Format the Audit File using TSSMAINT.

TSS8023E SMFOUT AUDIT FILE NOT PREFORMATTED

Reason: Internal format of Audit File is invalid.

Action: Format the audit file using TSSMAINT.

TSS8025E UNDEFINED ACCESS LEVEL: access level

Reason: The access level requested is not defined to CA-Top Secret.

Action: Attempt a different access level.

TSS8026E UNDEFINED ACCESS RESCLASS: resclass

Reason: The access resclass specified is not defined to CA-Top Secret.

Action: Attempt a different resclass.

TSS8027E FAILURE TO OPEN FILE: xxxxxxxx

Reason: An error was encountered when TSSUTIL attempted to use the indicated DLBL name.

Action: Insure the correct file and DLBL are being used and rerun the job.

TSS8028E NO AUTHORITY (NOT IN YOUR ZONE)

Reason: The user requested data on a zone outside of his scope.

Action: Correct the TSSUTIL parameters for access to the zone.

TSS8029E ZONE UNKNOWN

Reason: The zone requested doesn't exist.

Action: Define the zone to CA-Top Secret.

TSS8030E ZONE NOT WITHIN YOUR SCOPE

Reason: The zone requested is not within your scope of authority.

Action: Delete or correct the zone control statement.

TSS8032E DUPLICATE KEYWORD ENTERED

Reason: A control card keyword parameter has been entered twice on the same report request.

Action: Remove one of the parameters and resubmit the TSSUTIL job.

TSS8080E GETMAIN FAILED

Reason: TSS CPR was unable to acquire a sufficient amount of memory for it's work area.

Action: No action required.

TSS8081E MUST BE A MSCA or SCA

Reason: User is not a MSCA or SCA

Action: Sign-on with MSCA or SCA Control ACID.

TSS8082E I/O ERROR DLBL - xxxxxxxx

Reason: An I/O error was encountered for DLBL xxxxxxxx.

Action: No action required.

TSS8083E CA-Top Secret IS NOT ACTIVE

Reason: CA-Top Secret must be active to run TSS CPR.

Action: Attempt to rerun when CA-Top Secret is up.

TSS8084E INVALID CPF RECOVERY FILE

Reason: The CPF Recovery File is not valid.

Action: Insure that the DSN for the DLBL CPFFILE is a valid CPF Recovery File and rerun.

TSS8085E OPEN ERROR DLBL - xxxxxxxx

Reason: The DLBL-name of xxxxxxxx could not be opened.

Action: No action required.

TSS8110I AUTHORIZE RECOVERY PROCESSING

Reason: CA-Top Secret is not active to validate use of the TSSRECVR utility.

Action: See TSS8111A

TSS8111A REPLY: <Y> TO ALLOW; <N> TO ABORT

Reason: See message number TSS8110I

Action: To continue use of TSSRECVR, reply: Y, else, reply: N.

TSS8112E SYNAD ERROR - error text

Reason: An I/O error was encountered while processing the Recovery File.

Action: If error is not due to a HARDWARE problem, get the dumps or traces and contact CA Technical Support.

TSS8125E OPTION UNKNOWN OR INVALID

Reason: An option specified in the control statement is invalid.

Action: No action required.

TSS8126E MEMBER NOT FOUND

Reason: The member specified in the member operand of an APF control statement does not exist.

Action: No action required.

TSS8130E VOLUME XXXXXX IS NOT MOUNTED

Reason: TSSAUDIT attempted to dynamically allocate a data set that resides on a volume not currently mounted.

Action: No action required.

TSS8145E NO FUNCTION SPECIFIED

Reason: The first keyword specified as input to TSSAUDIT was not a valid TSSAUDIT function.

TSS8170E TSSTRACK ENVIRONMENT ERROR

Reason: The CA-Top Secret address space was not active when TSSTRACK was run.

Action: When CA-Top Secret is active, run TSSTRACK.

TSS8171E TRACKING TERMINATED WITH ERROR

Reason: TSSTRACK was terminated. Will result in User Abend 1801.

Action: Retry TSSTRACK. If problem persists, contact Technical Support.

TSS8172E INVALID NUMERIC VALUE - ????????

Reason: The value supplied (???????) for a TSSTRACK selection criteria/Control Option was invalid for the following reasons:

- It did not fall within the valid numeric range for the selection criterion; or,
- It was not numeric. The request to change the value is suppressed.

Action: Correct the syntax error indicated and re-specify the option.

TSS8173E SYNTAX ERROR IN OPTION - ????????

Reason: A valid TSSTRACK selection criteria/control option has been entered, but the value specified (???????) for it is invalid. The option is ignored.

Action: Correct the syntax error indicated and re-specify the option.

TSS8174E UNKNOWN PARAMETER ENCOUNTERED - ????????

Reason: '???????' from the input to TSSTRACK is not a valid selection criteria/control option.

Action: Remove the incorrect parameter and re-specify other options if coded on the TSSTRACK Options prompt.

TSS8175E UNLOCK LOCK FUNCTION FAILED

Reason: The indicated function, either locked or unlocked unsuccessfully due to receiving a non-zero return code from CA-Top Secret. Function is ignored.

Action: For the UNLOCK function, reissue the UNLOCK TSSTRACK control option and re-specify the correct password to message TSS8176A.

TSS8176A ENTER YOUR PASSWORD TO UNLOCK THIS TERMINAL

Reason: The TSSTRACK UNLOCK control option was specified.

Action: Enter the correct CA-Top Secret password to unlock the terminal.

TSS8178E UNABLE TO ALLOCATE xxxxxx

Reason: TSSTRACK was unable to dynamically allocate the file indicated (xxxxxx).

Action: See message TSS8180E. Function is terminated.

TSS8179E THE AUDIT/TRACKING FILE IS NOT AVAILABLE

Reason: TSSTRACK unable to access the Audit/Tracking File.

Action: Retry when the Audit/Tracking File is available.

TSS8181I ONLINE TRACKING TERMINATED

Reason: Issued in response to the "End" or "Stop" selection criterion. Execution terminates with a Return Code of 0.

Action: No action required.

TSS8182E IMPROPER INITIALIZATION

Reason: TSSTRACK not able to initialize.

Action: Reissue TSSTRACK later.

TSS8184I AUDIT AUDIT2 File WRAP DETECTED AT hh:mm:ss

Reason: CA-Top Secret reused a data block on the Audit/Tracking File indicated in the message while TSSTRACK was processing a request to display the oldest events on the file.

Action: This message is informational. The requested events are no longer available to TSSTRACK.

TSS8185E UNABLE TO GETMAIN ENOUGH BUFFER STORAGE

Reason: Insufficient storage was available for internal buffers. Execution terminates with a Return Code of 16.

Action: No action required.

TSS8186E AUDIT/TRACKING FILE IS NOT FORMATTED

Reason: The Audit/Tracking File has not been formatted by the TSSMAINT Utility. Execution terminates with a Return Code of 20.

Action: No action required.

TSS8187E CONFLICTING/INCORRECT OPTION SPECIFIED - xxxxxxxx

Reason: The control options passed to TSSTRACK contain a conflict or the function is not supported by the terminal device. The variable, 'xxxxxxx' located in the message, is the control option in conflict, or it is incorrectly specified.

Action: Review the control options and re-specify. Also, consult the *Report and Tracking Guide*.

TSS8188E AUDIT/TRACKING FILE IS EMPTY.

Reason: No records were found in the Audit/Tracking File. Execution terminates with a Return Code of 20.

Action: No action required.

TSS8189E UNABLE TO OPEN AUDIT/TRACKING FILE

Reason: The Audit/Tracking File could not be opened. Execution terminates with a Return Code of 16.

Action: No action required.

TSS8190I TSSTRACK FUNCTION COMPLETED

Reason: Self explanatory.

Action: No action required, informational message.

TSS8191E NO AUTHORITY TO USE TSSTRACK

Reason: You are not authorized to use the TSSTRACK Utility. Execution terminates with a Return Code of 8.

Action: Obtain proper administration authorities; refer to the *Report and Tracking Guide*.

TSS8192A ENTER TSSTRACK SELECTION CRITERIA/OPTIONS:

Reason: TSSTRACK detected that the PA1/Attention key was hit or no Selection criteria/control options were specified on the TSSTRACK command/transaction.

Action: Enter valid TSSTRACK selection criteria/control option parameters.

**TSS8193A ENTER LIST OF DETAIL REASON CODES, SEPARATED BY
COMMAS**

Reason: TSSTRACK found the DRC control option, but no detail violation error reason codes were specified.

Action: Enter Detail Error Reason Code in hexadecimal notation, separated by commas.

TSS8194I UNLOCK LOCK FUNCTION SUCCESSFUL

Reason: Self explanatory.

Action: No action required.

TSS8195W UNLOCK IGNORED, TERMINAL NOT LOCKED

Reason: The TSSTRACK UNLOCK function was specified, but the terminal was not in a locked condition.

Action: Issue the LOCK control option if terminal must be locked.

TSS8196I SELECTED EVENTS NOT FOUND

Reason: Using the selection criteria specified, TSSTRACK could not find any matching events on the Audit/Tracking file(s).

Action: No action required. Informational message.

TSS8197E DETAIL ERROR REASON CODE NOT FOUND - xx

Reason: The description of the DRC code specified is not available.

Action: No action required. Informational message.

TSS8199E TSSTRACK FUNCTION FAILED, REASON=xxxxxxx

Reason: TSSTRACK could not continue processing due to an error.

Action: 'xxxxxxx' can be one of the following reasons:

SYNTAX-ERROR

An invalid keyword or a keyword with an invalid or improper value was specified. Specify the proper keyword/parameter.

CMODE-LIMIT

The maximum number of terminals that TSSTRACK can support in Continuous Mode has been reached. No other TSSTRACK sessions in Continuous Mode are allowed. Execute TSSTRACK at a later time, if the problem persists contact CA-Technical Support.

NO-CMODE-TRM

The CICS Terminal ID specified in the TSS TRACK=OFF command does not identify a Terminal executing TSSTRACK in Continuous Mode. Specify the correct terminal id.

STRG-UNAVAIL

TSSTRACK under CICS could not obtain the amount of DSA storage needed to continue processing. Execute TSSTRACK at a later time.

TSS8324E USER IS NOT AUTHORIZED TO APPLY ENCRYPT KEY

Reason: User is attempting to set the Encryption Key for the Security File. Either the user is not authorized to do so; or CA-Top Secret is not active.

Action: Check that the user is an SCA and that CA-Top Secret is active.

TSS8330I ENTER <SIMULATOR COMMAND> OR <END>

Reason: TSSSIM is ready to process the next command.

Action: Enter a valid command or END to terminate the simulation.

TSS8331I TSS SIMULATION MONITOR ENDED

Reason: Terminal operator has ended simulation.

Action: No action is necessary.

TSS8332E CA-TSS IS NOT CURRENTLY ACTIVE.

Reason: The CA-Top Secret address space was not active when TSSSIM was run. CA-Top Secret is required to obtain Security File information during the simulation process.

Action: Rerun when CA-Top Secret is active.

TSS8333E RSSCSIM0 INSUFFICIENT MEMORY.

Reason: A GETMAIN has failed due to insufficient memory.

Action: Allocate more memory and rerun.

TSS8334E TSS/SIMULATOR VERSION MISMATCH.

Reason: The version of TSSRSIM0 you attempted to run is not the same as the currently running version of CA-Top Secret.

Action: Investigate what version of CA-Top Secret is running and use the correct version of TSSRSIM0 for that version.

TSS8335E INVALID/MISSING SECURITY ENVIRONMENT.

Reason: TSSSIM has found that no security environment has been established for this administrator.

Action: No action required.

TSS8336E SIMULATOR MODULE ENVIRONMENT ERROR.

Reason: TSSSIM was unsuccessful in locating a simulator load module or the user does not have access to TSSSIM.

Action: Check the install or give the user MISC1(TSSSIM) authority.

TSS8337E TSSSIM IS ALREADY ACTIVE AT YOUR TERMINAL

Reason: TSSSIM cannot be active under both screens of a split-screen session.

Action: No action required.

TSS8338E YOU ARE NOT AUTHORIZED TO USE TSSSIM.

Reason: You do not have sufficient authority to use TSSSIM.

Action: Obtain proper administrative authorities and retry.

TSS8339E INVALID MONITOR SUFFIX CHARACTER.

Reason: Unable to determine for interrupt.

Action: Terminate TSSSIM and reinitiate the process.

TSS8341E ENVIRONMENT COMMUNICATION ERROR -- MESSAGES LOST.

Reason: No text buffer was returned from the simulation module.

Action: Contact CA-Top Secret Support.

TSS8342E INTERNAL SYSTEM ERROR -- SIMULATION SUBTASK ABEND.

Reason: The simulator subtask has abended.

Action: Contact CA-Top Secret Support.

TSS8343E INTERNAL SYSTEM ERROR -- INITIALIZATION SUBTASK FAILURE.

Reason: The simulator subtask has abended.

Action: Contact CA-Top Secret Support.

TSS8344E INTERNAL SYSTEM ERROR -- SFS RC = (xxx)

Reason: An error has occurred while trying to retrieve security information from the Security File.

Action: Contact CA-Top Secret Support.

TSS8351E CA-TOP SECRET IS NOT CURRENTLY ACTIVE

Reason: The CA-Top Secret address space was not active when TSSIM was run. TSS is required to obtain Security File information during the simulation process.

Action: Return when CA-Top Secret is active.

TSS8352E UNABLE TO ALLOCATE DLBLNAME = dsname

Reason: TSSSIM could not successfully dynamically allocate (or open) the indicated data set name.

Action: No action required.

TSS8353E <module> - INSUFFICIENT MEMORY, GETMAIN FAILED

Reason: The module has been unable to acquire sufficient memory for its workarea.

Action: No action required.

TSS8354E TSS/TSSSIM VERSION MISMATCH

Reason: Different versions of CA-Top Secret and TSSSIM are incompatible--i.e., TSSSIM version 4 will not operate if version 3 is currently running.

Action: No action required.

TSS8355E MISSING/INVALID SECURITY ENVIRONMENT

Reason: TSSSIM has found that no security environment has been established for this administrator.

Action: No action required.

TSS8356E SIMULATOR MODULE ENVIRONMENT ERROR

Reason: TSSSIM was unsuccessful in locating a simulator load module or the user does not have access to TSSSIM.

Action: Check the install or give the user MISC1(TSSSIM) authority.

TSS8360E UNKNOWN COMMAND

Reason: The last simulator subcommand was unknown to TSSIM.

Action: No action required.

TSS8361E KEYWORD keyword IS MISSING OR INVALID

Reason: An expected/required keyword was omitted from the subcommand or the subfield for the specified keyword was invalid.

Action: No action required.

TSS8362E COMMAND REQUIRES AN ACTIVE SIMULATED SESSION

Reason: The last simulator subcommand entered is only valid when a simulated security environment has been established via the simulator LOGON or SIGNON command.

Action: No action required.

TSS8363E RESERVED COMMAND IS NOT AVAILABLE

Reason: The last simulator subcommand entered is reserved for future use but is currently unavailable.

Action: No action required.

TSS8364E INSUFFICIENT SESSION AUTHORITY FOR THIS COMMAND

Reason: You do not have sufficient authority to issue this simulator subcommand.

Action: Obtain proper administrative authorities and reissue command.

TSS8365E RESOURCE IS NOT OWNED WITHIN YOUR SCOPE

Reason: The resource you are checking is not owned within your scope of authority.

Action: No action required.

TSS8370I SIMULATED SESSION SUCCESSFULLY ESTABLISHED

Reason: This is an informational message indicating that no errors were encountered while processing the simulator LOGON or SIGNON commands. You may now issue resource-checking subcommands on behalf of the simulated acid session.

Action: No action required.

TSS8371E SIGNON ERROR(S) ENCOUNTERED - SESSION NOT ESTABLISHED

Reason: TSSSIM encountered an error while processing the simulator LOGON or SIGNON command. This message is usually preceded by message TSS8385I, which contains more detailed information regarding the error. Resource check subcommands cannot be entered at this time, since the simulated acid session was not established.

Action: No action required.

TSS8372W NOTE: ACID IS SUSPENDED.

Reason: This is a warning message indicating that the simulated ACID is currently suspended; however, LOGON/SIGNON processing continues.

Action: No action required.

TSS8373W NOTE: FACILITY IS NOT IN USE AT YOUR SITE

Reason: This is a warning message indicating that the "in-use" bit is not currently set in the facility matrix for the desired facility. LOGON/SIGNON processing continues.

Action: No action required.

TSS8374W NOTE: FACILITY IS CURRENTLY DEACTIVATED.

Reason: This is a warning message indicating that the requested facility is not currently accepting actual logons; however, the simulator LOGON/SIGNON processing continues.

Action: No action required.

TSS8375W NOTE: ACID IS NOT AUTHORIZED TO USE THIS FACILITY

Reason: This warning indicates that the simulated ACID is not authorized to use the requested facility. LOGON or SIGNON processing continues.

Action: No action required.

TSS8376W NOTE: ACID IS NOT AUTHORIZED TO USE THIS CPU

Reason: This is a warning message indicating that the simulated ACID is not authorized to use the current CPU. LOGON/SIGNON processing continues.

Action: No action required.

TSS8377W NOTE: ACID IS NOT AUTHORIZED TO USE THIS TERMINAL

Reason: This is a warning message indicating that the simulated ACID is not authorized to use the requested terminal. LOGON or SIGNON processing continues.

Action: No action required.

TSS8378W NOTE: ACID HAS BEEN INACTIVE TOO LONG

Reason: This is a warning message indicating that the simulated ACID has been inactive too long; however, LOGON/SIGNON processing continues.

Action: No action required.

TSS8379W NOTE: ACID IS NOT WITHIN YOUR SCOPE

Reason: This warning indicates that the simulated ACID is not within your scope of authority. LOGON or SIGNON processing continues; however, when the session is established, resource checks are limited to those resources which fall within the administrator's scope.

Action: No action required.

TSS8380I SIMULATED RESOURCE ACCESS GRANTED

Reason: The simulated ACID would receive access to the requested resource. (Note, this message is always generated for resource-checks when the simulated session is not in FAIL mode.)

Action: No action required.

TSS8381I SIMULATED RESOURCE ACCESS DENIED.

Reason: This is an informational message indicating that the simulated ACID would be denied access to the requested resource.

Action: No action required.

TSS8385I <SVCNAME> R15 = xx RC = xx DRC = xx

Reason: This informational message indicates the results of the last subcommand which invoked CA-Top Secret to perform a resource check. The following information is detailed: (a) the CA-Top Secret routine (RACINIT, RACHECK, RACDEF, FRACHECK), (b) register 15 as returned to the caller, (c) the security return code, and (d) the detailed security return code.

Action: No action required.

TSS8386I <NO FEEDBACK MESSAGES>

Reason: No security messages have been found in the feedback area for a resource-check subcommand.

Action: No action required.

TSS8390I RESOURCE = (c) xxxxxxxx

Reason: Lists the resource upon which access is being checked.

Action: Informational message, no action necessary.

TSS8391I SVC=ss RC=rr DRC=DLBL VDRC=vv XSW=xx ALG=aa

Reason: Lists the following information for the system being simulated:

SVC Security SVC called for the resource check:

RC Security return code

DRC CA-Top Secret Detailed Reason Code

VDRC CA-Top Secret DRC for volumes

XSW Algorithm results:

00 - auth
04 - not found
08 - unauthorized

ALG Algorithm selection:

00 - override
80 - merge
40 - allmerge

Action: Informational message, no action necessary.

**TSS8392I REQUESTED ACCESS = nnnnnnnn
ALLOWED ACCESS = nnnnnnnn
VOLUME ACCESS = nnnnnnnn**

Reason: Lists the access level requested and allowed for the simulated ACID, and the volume access.

Action: Informational message, no action necessary.

TSS8393I OVERRIDES = xxxxxxxx,xxxxxxx,...

Reason: Lists the overrides allowed for the simulated ACID, any or all of the following may be displayed:

DSN
LCF
RES
SUB
VOL
USR-BYP
EMG-BYP

Action: Informational message, no action necessary.

TSS8394I RES ORIGIN = rrrrrrrr - llllllll

Reason: Lists whether the resource is owned or permitted and its location:

rrrrrrrr is either OWNED or PERMITTED.

lllllll is *USER*, PROFILE=profilename, or *ALL*.

Action: Informational message, no action necessary.

TSS8395I RES RULE # = nnn

Reason: Lists the permission number of the record listed in message TSS8394I.

Action: Informational message, no action necessary.

TSS8397I SECURITY PERMISSION INFORMATION

Reason: The following information is displayed concerning the security permission that allowed or denied access to the resource:

RESOURCE

resource name

ACCESS permitted access

FACILITY facility restriction

PRIVPGM program restriction

Action: Informational message, no action necessary.

TSS8398I VOLUME FEEDBACK:f1 f2 f3 f4

Reason: This message displays bitmapped tape volume information that may be requested by CA-Top Secret Technical Support if you report a problem with TSSSIM.

Action: Informational message, no action necessary.

TSS8399I SUBRTN FLAGS: f1 f2 f3 f4 f5

Reason: This message displays bitmapped subroutine information that may be requested by CA-Top Secret Technical Support if you report a problem with TSSSIM.

Action: Informational message, no action necessary.

TSS8400I PARENT SVC = pp CALLING SVC = cc

Reason: This message displays the hexadecimal numbers of the security caller and the security routine being called.

Action: Informational message, no action necessary.

**TSS8401I CURRENT/PARENT/BOTTOM PRIVPGM(S) = ccccccc pppppppp
bbbbbbbb**

Reason: This message displays the names of the current PRIVPGM program, the calling program, and the called program.

Action: Informational message, no action necessary.

**TSS8410I SIMULATED ACID = aaaaaa QUALIFIER = bbbbbb MODE = cccc
SIMULATED FAC = dddd TERMINAL = eeeeeee CPU = ffff
DEFAULT SVC = ggg NUMBER = hh (HEX) ACCESS = ii
DEFAULT PRIVPGM = jjjjj DEFAULT LIBRARY = kk
SECURITY TRACE = ll**

Reason: This message displays information about an ACID in response to a TSSSIM STATUS command. The following information is displayed:

- name of simulated ACID
- data set qualifier
- simulation mode
- simulated facility
- terminal name
- CPU
- default SVC name, number, and associated access
- default privileged program PRIVPGM
- default library
- default TRACE setting

Action: Informational message, no action necessary.

TSS8407E INTERNAL SIMULATOR CONTROL BLOCK ERROR (xxxxxxx).

Reason: TSSSIM has encountered an unexpected error while identifying the indicated control block.

Action: Notify CA technical support if this error persists.

TSS8408E UNEXPECTED SECURITY FILE SERVICES ERROR (nnn).

Reason: TSSSIM has encountered an unexpected non-zero return code from TSS, while attempting to retrieve information from the Security File.

Action: Notify CA technical support if this error persists.

TSS8409E TSSSIM FATAL ERROR(S).

Reason: Due to an earlier-printed error message, TSSSIM was unable to continue.

Action: Notify your systems programmer.

TSS8411W DATASET PERMIT WITH LIBRARY UNSUPPORTED

Reason: The TSSSIM \$DSN command does not support checking of a dataset permission with the PRIVPRM and LIBRARY specifications.

Action: No action required.

**TSS8429E UNEXPECTED SECURITY FILE SERVICES COMMUNICATION
ERROR (nnn)**

Reason: TSSCHART encountered an unexpected non-zero return code from the CA-Top Secret address space when trying to obtain Security File information.

Action: No action required.

TSS8600I SECURITY INACTIVE FOR PROTECTION FACILITY

Reason: Data access request cannot be validated.

Action: No action required.

TSS8601A REPLY <Y> TO CONTINUE; <N> TO ABORT

Reason: To proceed to secure data sets without access validation, reply "Y". To cancel TSSPROT, reply "N".

Action: No action required.

TSS8700E COMMAND IS AMBIGUOUS OR UNKNOWN

Reason: Keyword entered from TSSCHART or TSSSIM is ambiguous or unknown.

Action: Enter correct keyword.

TSS8701E KEYWORD < > IS MISSING OR INVALID

Reason: Keyword is either incorrect or needs to be supplied.

Action: Provide or correct the specified keyword.

TSS8702E KEYWORD < > IS AMBIGUOUS OR UNKNOWN

Reason: Keyword supplied is either unknown or requires additional information (i.e., additional operands)

Action: Clarify or correct the specified keyword.

TSS8703E COMMAND CONTAINS UNBALANCED PARENTHESES

Reason: Command either contains an odd number of parentheses indicating that one parenthesis either needs to be added or subtracted.

Action: Reissue the command with the correct number of parentheses.

TSS8730 TABLE FULL - USER TABLE

Reason: The table generated to hold the users is full.

Action: Program terminates. Increase the value for V1 with the TABLES control statement.

TSS8731 USER DOES NOT EXIST ON RACF. NO ACTION TAKEN

Reason: An ACID or user in a control statement is specified that does not exist on the RACF data base.

Action: The statement is ignored. No action required.

TSS8732 TABLE FULL - USER DEFINED PROFILE TABLE

Reason: The user-defined profile table is full.

Action: Program terminates. Increase the value for V2 with the TABLES control statement.

TSS8733 TABLE FULL - USERS TABLE FOR USER DEFINED PROFILES

Reason: The user table for user-defined profiles is full.

Action: Program terminates. Increase the value for V3 with the TABLES control statement.

TSS8734 TABLE FULL - GROUP TABLE

Reason: The group table is full.

Action: Program terminates. Increase the value for V4 with the TABLES control statement.

TSS8735 TABLE FULL - USERS TABLE FOR ALL GROUPS

Reason: The user table for all groups is full.

Action: Program terminates. Increase the value for V5 with the TABLES control statement.

TSS8736 TABLE FULL - DEPARTMENT TABLE

Reason: The department table is full.

Action: Program terminates. Increase the value for V6 with the TABLES control statement.

TSS8737 TABLE FULL - DSN LEVEL

Reason: The data set level table is full.

Action: Program terminates. Increase the value for V7 with the TABLES control statement.

TSS8742 TABLE FULL - GROUP OF DSNS ALL IN ONE DEPT

Reason: The table defining the data sets owned by one department is full.

Action: Program terminates. Increase the value for V9 with the TABLES control statement.

TSS8743 TABLE FULL - ALL USERS ACCESSING CONTIG GROUP OF DSNS ALL IN ONE DEPT

Reason: The table defining the users accessing a contiguous group of data sets in one department is full.

Action: Program terminates. Increase the value for V10 with the TABLES control statement.

TSS8744 TABLE FULL - USERS TABLE FOR PROFILES TO DESCRIBE ALL ACC LISTS WITH PROFILES

Reason: The table defining all access lists with profiles is full.

Action: Program terminates. Increase the value for V11 with the TABLES control statement.

TSS8745 TABLE FULL - USERS TABLE FOR DSN ACC LIST

Reason: The table defining the data set access lists is full.

Action: Program terminates. Increase the value for V12 with the TABLES control statement.

TSS8746 INVALID SYNTAX WORD

Reason: An invalid control statement is encountered.

Action: The statement is ignored. No action required.

TSS8747 VALUE TOO LONG

Reason: A value specified in a control statement is too long.

Action: The statement is ignored. No action required.

TSS8748 END OF VALID CONTROL CARDS

Reason: Control card processing is finished.

Action: An advisory message. No action required.

TSS8750 TOO MANY IN LIST OF VALUES

Reason: A control statement contains too many values in a list.

Action: The statement is ignored. No action required.

TSS8751 DSN LEVEL NUMBER ERROR, IGNORED

Reason: A level of ownership less than 1 or greater than 7 is specified in an OWN control statement.

Action: The statement is ignored. No action required.

TSS8752 DSN LENGTH ZERO, IGNORED

Reason: A "DSN ()" is specified in an OWN control statement, which results in a data set length of zero.

Action: The statement is ignored. No action required.

TSS8753 CONTROL CARD OUT OF SEQUENCE - SKIPPED

Reason: Control statements are specified out of sequence. OWN control statements must come last.

Action: Statements after the last OWN control statement are ignored. No action required.

TSS8754 DEPARTMENT NOT FOUND - SKIPPED

Reason: A department in an ASSIGN control statement is specified that has not been created by the conversion process.

Action: The statement is ignored. No action required.

TSS8755 GENERIC DEPARTMENT NOT ALLOWED FOR PROFILE NAME SELECTION - SKIPPED

Reason: A generic department name is specified in an ASSIGN control statement.

Action: The statement is ignored. No action required.

TSS9000I CA-TOP SECRET SECURITY 30yymmAKDnn ACTIVE

Reason: The specified version of CA-Top Secret is initialized and ready to control security. Where: 30 is the release, yymm is the genlevel, AKD is the product code and nn is the version number.

Action: No action required.

TSS9001I REINIT COMPLETE

Reason: CA-Top Secret successfully invoked the REINIT Control Option.

Action: No action required.

TSS9003I AUDIT/TRACKING FEATURE NOT ACTIVE

Reason: The Audit/Tracking File is NOT being used to record security-related information.

Action: To create an Audit/Tracking File, refer to the TSSMAINT utility or the *Installation Guide*. To direct security-related information to the Audit/Tracking File, see the LOG control option in the *Control Options Guide*.

TSS9004I AUTOMATIC BACKUP FEATURE NOT ACTIVE

Reason: A reminder that the CA-Top Secret automatic backup feature is not installed.

Action: To install automatic backup, see the BACKUP Control Option.

TSS9006E CA-SAF NOT UP. RE-IPL NECESSARY

Reason: CA-SAF was not started prior to your attempt to start CA-Top Secret. The installation of CA-Top Secret was done incorrectly or a required library is missing from the linklist or lpalist.

Action: Ensure library containing CA-Top Secret is available when CASAUTIL activates, and that a CA-SAF Initialization message appeared during that startup of CA products with CASAUTIL.

TSS9007E *MAJOR VERSION CHANGE RE-IPL NECESSARY*****

Reason: You are running with a previous release of CA-Top Secret; internal control blocks not compatible.

Action: No action required.

TSS9008E CA-TOP SECRET ALREADY ACTIVE

Reason: An attempt to start CA-Top Secret has failed because it is already executing. User abend 0002 results.

Action: No action required.

TSS9010E CANNOT OBTAIN FIXED CSA PAGE

Reason: CA-Top Secret requires a page of Common Storage for cross-memory communication. Insufficient SVA is available for the period, or real storage is insufficient. CA-Top Secret can NOT start.

Action: No action required.

TSS9011E CANNOT OBTAIN A JOB ID

Reason: Issued for TSSMNGR if SSOBRQST SSI call failed.

TSS9011W RECOVERY FILE HAS WRAPPED AROUND

Reason: The CA-Top Secret Recovery File is full. Changes to the Security File will be recorded at the beginning of the File; overwriting current data.

Action: Back up the Recovery File.

TSS9012W RECOVERY FILE IS AT LEAST 90% FULL

Reason: The CA-Top Secret Recovery File is nearly full. Once full, the File's data is overwritten. This message is issued once the file reaches 90% capacity and subsequently, each time CA-Top Secret is restarted as long as the condition persists.

Action: Display the BACKUP control option to determine if a backup of the CA-Top Secret Security File will occur before the Recovery File reaches 100% full and then wraps. If a backup will not occur, then MODIFY the BACKUP control option to request an immediate backup.

TSS9013I GLOBAL STORAGE NOT FREED

Reason: CA-Top Secret was unable to free SVA unused storage.

Action: See the *User Guide*.

TSS9014E SECURITY FILE BLOCKSIZE ILLEGAL

Reason: The physical blocksize of the Security File is different from the BLOCKSIZE specified during file creation.

Action: If the file was just copied, restore the backup copy. Otherwise, use utility TSSMAINT to rebuild the Security File.

TSS9015E ERROR drc DURING SECURITY FILE INITIALIZATION

Reason: During the CA-Top Secret activation process, an error prevented the processing of the Security File.

Note: DRC (xx) = 39 and 4B may indicate incorrect customer key

Action:

1. Restart CA-Top Secret. If problem persists, see 2.
2. Re-IPL. If problem persists, the Security File may be damaged, and requiring reconstruction. Contact CA Technical Support if problem is not hardware-related.

TSS9016E I/O ERROR. RESTORE SECURITY FILE FROM BACKUP PROCESS RECOVERY FILE

Reason: During the CA-Top Secret activation process, an I/O error prevented Security File processing.

Action:

1. Restore Security File using the latest backup copy.

2. Use the Recovery Procedures to recover changes that were made to the file. If problem persists, use the backup Security File without recovery. Contact CA Technical Support.

TSS9017I SFS ABEND RECOVERY COMPLETE

Reason: The CA-Top Secret subtask, SFS, has been successfully reactivated after an abend.

Action: If the abend was NOT a result of hardware damage to the Security or Recovery Files, send the dump produced by the abend to CA Technical Support.

TSS9018I SECURITY FILE SERVICES REINSTATED

Reason: CA-Top Secret is able to process requests. See message TSS9017I.

Action: No action required.

TSS9019E INVALID START REQUEST

Reason: You tried to start CA-Top Secret from a facility other than as a Started Task.

Action: Use the START TSS command from a console.

TSS9020W INVALID PARAMETER FILE OPTION

Reason: A data set option reference by the PARMFILE DD-statement is in error. CA-Top Secret continues processing.

Action: Examine your options. To obtain the TSS log, enter the following O/S Console Control Option: F TSS,SYSOUT. The statement preceding the message is the option in error.

TSS9021W INVALID EXECUTE OPTION

Reason: A PARM option of the TSS EXEC statement is incorrect.

Action: Check the PARM of the CA-Top Secret Started Task Procedure.

TSS9022I AUTOMATIC COMMANDS BEING ISSUED

Reason: The commands in AUTOCMDS File are executing.

Action: No action required.

TSS9023E UNABLE TO OPEN AUTOCMDS FILE

Reason: The AUTOCMDS File cannot be opened. Automatic commands contained in AUTOCMDS are not started.

Action: Check to ensure that the CAIACMD DLBL statement in the TSS PROC points to a valid dataset.

TSS9024E UNABLE TO OPEN BACKUP FILE

Reason: The automatic DASD backup file (referenced by the BACKUP DLBL-statement) is not usable. Automatic backup is ignored. Processing continues.

Action: No action required.

TSS9025E UNABLE TO OPEN PARAMETER FILE

Reason: An attempt to read control options from the Parameter File was unsuccessful due to an open error. Processing continues.

Action:

1. Check processing options via console control option TSS,STATUS.
2. Examine attributes of Parameter File.

TSS9026E SECURITY FILE UNDEFINED

Reason: The CAISECF DLBL-statement is missing from the TSS.PROC procedure.

Action: Correct the CAISECF DLBL-statement in the TSS.PROC procedure.

TSS9027E SECURITY FILE UNAVAILABLE

Reason: CA-Top Secret was not able to open and access the Security File.

Action: Check the TSS.PROC procedure to ensure that the CAISECF DLBL-statement properly references the Security File.

TSS9028E RECOVERY FILE UNDEFINED

Reason: The CAIRCVR DLBL-statement is missing from the TSS.PROC procedure.

Action: Correct the CAIRCVR DLBL-statement in the TSS.PROC procedure.

TSS9029E RECOVERY FILE UNAVAILABLE

Reason: CA-Top Secret was not able to open or access the Recovery File.

Action: Check the TSS.PROC procedure to ensure that the CAIRCVR DLBL-statement properly references the Recovery File. If recovery processing is not required, use the RECOVER(OFF) option on the START TSS Command.

TSS9030E PRIMARY AND BACKUP SECURITY FILES IDENTICAL

Reason: Both the CAISECF and CAIBKUP.DLBL-statements in the TSS.PROC procedure reference the same data set name. CA-Top Secret has deactivated the automatic backup feature.

Action: If you are running from the Backup File, ignore this message. Otherwise, ensure that the TSS.PROC procedure references the correct data set names.

TSS9036E RECOVERY FILE UNFORMATTED

Reason: TSSMAINT was not used to format the Recovery File. Changes made to files cannot be recovered if system abend occurs.

Action: Use TSSMAINT to format the Recovery File.

TSS9038E RECOVERY PROCESSING TERMINATED

Reason: A previously reported recovery error has caused the RECOVERY feature to deactivate.

Action: Investigate the reported error and check the Recovery File accordingly. Here are some possible causes:

- Damage to the volume (hardware).
- Recovery File was not initialized.
- CAIRCVR DLBL-statement is missing or invalid, etc.

TSS9039E UNEXPECTED RECOVERY END-OF-FILE

Reason: CA-Top Secret was not able to wrap around the Recovery File. Change recovery is deactivated.

Action: Call CA Technical Support.

TSS9040W SECURITY FILE ENCRYPTION UNAVAILABLE

Reason: CA-Top Secret cannot encrypt the information in the Security File because the customer encryption key has not been supplied.

Action: Use TSSKEY00 (explained in the *Installation Guide*) to set your encryption key into CA-Top Secret.

TSS9041E CUSTOMER ENCRYPTION KEY REQUIRED TO UNLOCK FILE

Reason: See message TSS9040W

Action: See message TSS9040W

TSS9042A SPECIFY <ABORT>; ELSE 16 HEX DIGIT KEY

Reason: CA-Top Secret will terminate unless you enter the Customer Encryption Key.

Action: Enter the key as 16 hexadecimal digits or abort CA-Top Secret by entering the command **ABORT**.

TSS9043W KEY IS TEMPORARY - ZAP REQUIRED

Reason: The encryption key being used is temporary. You must eventually place a permanent key into CA-Top Secret, via TSSKEY.Z

Action: See message TSS9040W

TSS9044E INVALID HEX DIGIT IN KEY

Reason: The Security File Customer Encryption Key contains a character other than 0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F

Action: Reply to the TSS9042A message again, specifying a valid encryption key value.

TSS9045I RDT SYNCHRONIZATION COMPLETE

Reason: During startup, TOP SECRET recognized that maintenance had been applied to the Base Resource definition table. These changes have been merged into the existing RDT.

Action: Informational message only.

TSS9046I RDT SYNCHRONIZATION FAILED - reason

Reason: During startup, CA-Top Secret attempted to merge an updated base RDT with the Security File RDT. The merge failed for the indicated reason.

Action: If you are unable to determine the cause of the error from the reason, contact CA Technical Support.

TSS9048I RDT SYNCHRONIZATION RENAMED oooooooo TO \$nnnnnnnn.

Reason: A conflict has occurred between a new predefined RDT resource and a user-defined resource. The user-defined resource has been renamed to \$nnnnnnnn.

Action: Issue the TSS WHOHAS and TSS WHOOWNS commands to determine what administration is needed for the system-defined resource.

TSS9049I CA-TOP SECRET ABEND DURING INITIALIZATION

Reason: Abend conditions occurred during initialization.

Action: Restart TSS.

TSS9051E OID SUPPORT UNAVAILABLE

Reason: A required module is missing from the CA-Top Secret library.

Action: See message TSS9050E.

TSS9052E TSSRDT MODULE MISSING

Reason: A required module is missing from the CA-Top Secret library. CA-Top Secret abends with code 99.

Action: See message TSS9050E.

TSS9056E COMMAND LIMITING & PROGRAM RESTRICTIONS UNAVAILABLE

Reason: A required module is missing from the CA-Top Secret library.

Action: See message TSS9050E.

TSS9057E FETCH PROTECTION UNAVAILABLE

Reason: A required module is missing from the CA-Top Secret library.

Action: See message TSS9050E.

TSS9059E SAF NOT INITIALIZED - SVA SHORTAGE

Reason: CA-Top Secret was unable to install the SAF interface. Processing continues; however, unpredictable results will occur in a non-SU32 (i.e., SAF) environment.

Action: Shut down CA-Top Secret with BYPASS DOWN options and restart when SVA shortage is relieved. SAF interface uses less than 1K of SVA.

TSS9060E SECURITY FILE SYNAD

Reason: See TSS9063E

Action: No action required.

TSS9061E CAIRCVR SYNAD

Reason: An I/O error was returned on the Recovery File.

Action: Stop TSS, take a backup of the Recovery File and format the new file, restart TSS.

TSS9062E BACKUP FILE SYNAD

Reason: See TSS9063E

Action: No action required.

TSS9063E AUDIT FILE SYNAD

Reason: An I/O error occurred while processing the specified TOP SECRET File.

Action: If error is not due to a HARDWARE problem:

1. Get the dumps or traces
2. Contact CA Technical Support

TSS9064W SYSOUT CURRENTLY IN USE - RETRY REQUEST

Reason: An attempt to spin off the Trace Log failed.

Action: Retry request.

TSS9065A RESTART TSS WITH REINIT OPTION

Reason: The REINIT option is only valid when starting up TSS.

Action: Stop CA-Top Secret and specify the REINIT option using the start command.

TSS9066E LOGICAL XE ERROR

Reason: An invalid security record is present in CA-Top Secret common storage.

Action: A diagnostic dump will be taken. Call CA Technical Support.

TSS9068I TRACE/LOG SPUNOFF

Reason: This message displays in response to the SYSOUT option.

Action: No action required.

TSS9070W SYSOUT UNAVAILABLE, CPF JOURNAL FILE IGNORED IN LOG/RECVCMDS

Reason: This message is issued from TSSCPF if RECVCMDS or any node log files are allocated as SYSOUT in the startup procedure and CA-Top Secret starts before it is available.

Action: No action required.

TSS9070I OKAY

Reason: Positive acknowledgement to a successful execution of a TSS control option.

Action: No action required.

TSS9071E OPTION IGNORED - END OF DAY

Reason: Control Options defined as invalid after an end-of-day shutdown will be ignored by the system. This includes the LOG, MODE, and FACILITY options.

Action: To allow the options:

1. Enter the console control option: TSS MODIFY, RESETEOD
2. Reply with the correct password.
3. Re-enter the ignored options.

**TSS9073A ** SELECT TYPE OF SHUTDOWN ** <I> TO IGNORE
<Z> END OF DAY; RE-IPL WILL BE REQUIRED
<T> TEMPORARY; MAY IMPACT THROUGHPUT**

Reason: Displayed in response to the STOP TSS command. Lists the shutdown options.

Action: To ignore the shutdown reply: **I**.

To routinely shut down security at the end of the day reply: **Z**.

Note: New job submissions and new logons will abend. All other tasks should be brought down BEFORE stopping CA-Top Secret. End-of-day shutdowns can only be reset with an authorized RESETEOD option.

To shut down security mid-day reply: **T**.

To prevent an unauthorized mid-day shut down, the MSCA's **previous** password OR an operator id and password combination is required.

The system is forced to use DOWN options if security is shut down in any other mode than DORMANT. DOWN options, associated with facilities, affect only job/session initiation and tape processing.

TSS9074E OPTION NOT VALID AT STARTUP

Reason: The selected option cannot be specified on the EXEC PARM or in the PARMFILE. Options such as TSS and BYPASS must be entered through a MODIFY command.

Action: No action required.

TSS9075E INVALID OPTION

Reason: The entered MODIFY option is not known to TSS.

Action: Check spelling. Reenter option.

TSS9076I CURRENT OPTION IS option

Reason: The indicated control option is in error.

Note: Multiple occurrences of this message indicates that there are multiple errors found in the PARMFILE card.

Action: Re-enter the control option using the correct syntax.

TSS9077I OPTION IS OBSOLETE

Reason: The control option specified is not valid for the current version of TSS.

TSS9078I MODIFY OPTION IGNORED

Reason: An erroneous or unauthorized option was ignored.

Action: Retry the command if spelling/format is in error.

TSS9079E INVALID DATA

Reason: Incorrect parameter value entered.

Note: Multiple occurrences of this message indicates that there are multiple errors found in the PARMFILE card.

Action: Enter the correct data.

**TSS9080A ENTER OPERATOR ID/PASSWORD FOR MODIFY ACCOUNT-
ABILITY**

Reason: The entered CA-Top Secret control option requires operator accountability. The operator ACID must have the CONSOLE attribute.

Action: Enter an authorized ACID and password to continue.

TSS9081E OPERATOR AUTHENTICATION FAILED

Reason: The operator is not accountable due to one of the following conditions:

- the ACID is not defined
- the password is not correct
- the ACID has expired
- the ACID is suspended
- the ACID not type C/A or USER
- the ACID does not have CONSOLE attribute.

Action: If the ACID should be accountable, his administrator must assign the correct properties to the ACID.

TSS9082E YOU ARE NOT AUTHORIZED TO MODIFY SECURITY

Reason: An attempt to change security control options was halted because the Operator/Administrator does not have the CONSOLE attribute.

Action: No action required.

TSS9083E Q-FAILURE

Reason: CA-Top Secret internal communication error.

Action: Retry command. If problem persists, contact CA Technical Support.

TSS9084E OPERATOR ACID/PASSWORD INVALID OR ILLEGAL

Reason: See message TSS9081E

Action: No action required.

TSS9086I OPERATOR COMMUNICATIONS REINSTATED

Reason: The CA-Top Secret operator communications subtask has regained control after an abend.

Action: No action required.

TSS9087I OPCOM RECOVERY SUCCESSFUL

Reason: See message TSS9086I

Action: No action required.

TSS9088E INCORRECT PASSWORD

Reason: Password entered in response to message TSS9089A is incorrect or missing.

Action: No action required.

TSS9089A ENTER PASSWORD FOR FUNCTION

Reason: Restricted control options require authorization of the Central Security Administrator.

Action: Verify request and, if valid, enter the previous MSCA password, not the current password.

TSS9090A SECURITY EXIT FAILURE - EXIT DISABLED

Reason: System abend while executing the installation code. The exit is automatically turned off.

Action: A system dump was taken. Correct problem and reload the exit via the EXIT control option.

TSS9091E SECURITY BREACH (x) - POSSIBLE TAMPERING DETECTED

Reason: During a periodic internal check, CA-Top Secret discovered modification to critical logic or an address. Modification may be intentional or accidental.

Action: Notify your Security Administrator and Auditors. Notify CA Technical Support for a detailed description of what was modified. CA-Top Secret should eventually be reinitialized using the command: EXIT PROL.TSS

TSS9092W SECURITY IN EMERGENCY BYPASS STATE

Reason: Reminder that BYPASS(EVERYJOB) is in effect. All jobs will bypass security. CA-Top Secret commands will not work.

Action: No action required.

TSS9093W INVALID START OVERRIDE OPTION

Reason: An option in the PARM field of the CA-Top Secret procedure EXEC statement is incorrect.

Action: TSS starts but you must correct the statement prior to the next STARTup of TSS commands.

TSS9094I BACKUP COMPLETE

Reason: Displays in response to the TSS MODIFY, BACKUP control option or automatic backup. DASD backup of the Security File is complete.

Action: No action required.

TSS9095E SECURITY FILE BACKUP FAILED

Reason: Backup of the Security File failed due to a processing error, an I/O error, or incorrect file allocation.

Action: If CA-Top Secret abended or produced a dump, contact CA Technical Support.

TSS9096I SECURITY FILE BACKUP COMMENCING

Reason: Backup of the Security File has begun. The Security File is unavailable during backup processing. Job/session initiations, and use of CA-Top Secret commands must wait for backup to complete.

Note: Automatic backups should occur when the system(s) are relatively inactive (production work complete)--e.g, at night.

Action: No action required.

TSS9099I CA-Top Secret SECURITY FILE SERVICES NOW INACTIVE

Reason: Displays in response to a valid STOP TSS command. The DOWN options for the facilities take effect unless CA-Top Secret was running in DORMANT mode.

Note: CA-Top Secret is active. Only I/O services to the Security File are inactive. Bottleneck problems for throughput may occur.

Action: No action required.

TSS9101W *WARNING*** IPL WILL BE REQUIRED TO REINSTATE PROCESSING**

Reason: Response to valid Z shutdown.

Action: No action required.

TSS9102W REPLY <Y> TO CONFIRM SYSTEM SHUTDOWN

Reason: Response to a valid Z shutdown.

Action: Enter Y to shutdown, N to discontinue, the Z end-of-day shutdown, which requires an IPL to restart CA-Top Secret.

TSS9104E OPTION NOT ACCEPTED AFTER STARTUP

Reason: The option specified cannot be changed through a TSS MODIFY command. It may only be specified as a startup option in the Parameter File.

Action: Add the option to the Parameter File and restart CA-Top Secret.

TSS9105I GETMAIN FAILED; CPF NOW INACTIVE

Reason: The CPF component of CA-Top Secret was unable to obtain enough SVA to initialize. The TSS command will still execute normally. However, no commands will be routed to, or received from, remote nodes.

Action: Contact the systems programmer as to the cause of the SVA shortage.

TSS9106E SVA SHORTAGE-UNABLE TO INITIALIZE LOG INTERFACE

Reason: CA-Top Secret could not acquire sufficient common storage area. CA-Top Secret needs a minimum of 100K SVA to start.

Action: No action required.

TSS9120I ENQ/DEQ DONE for acid

Reason: The DEBUG control option was set ON. CA-Top Secret is reporting when an ENQ or DEQ was done on an 'acid'.

Action: No action required.

TSS9121I CA-TOP SECRET ENQ TABLE FULL, ENQ WAITING

Reason: The TSS command cannot obtain an enqueue on a specific ACID. The table used to keep track of enqueues is full. The TSS command will wait for an enqueue table entry to be freed and then continue normally.

Action: If this message occurs frequently, the blocksize of the Security File should be increased.

TSS9122I CA-TOP SECRET UNABLE TO ENQ ON ACID acid (ENQ HELD ON SYSTEM system)

Reason: The TSS command has not been able to enqueue on the named acid due to an enqueue being held from the system ('system' is the CA-CIS CPUID, prefixed with 'VSE'). CA-Top Secret will continue waiting for the enqueue to free. If the enqueue does not free, message TSS9123A prompts for permission to reset the enqueue.

Action: See message number TSS9123A.

**TSS9123A UNABLE TO OBTAIN SECURITY/AUDIT FILE LOCK. SYSTEM
system HAS HELD LOCK FOR nn MINUTES. IF system IS NOT
OPERATIONAL, REPLY 'RESET', OTHERWISE REPLY 'WAIT'.**

**WARNING: INDISCRIMINATELY REPLYING 'RESET' MAY
CAUSE CORRUPTION OF THE CA-TOP SECRET SECURITY FILE
REPLY 'RESET' or 'WAIT' <sysid>**

Reason: CA-Top Secret has not been able to obtain either the Security File lock or an enqueue. The resource has been held on the system for nn minutes. If BLP appears after the "system", the initial system is in the process of backing up the security file.

If the system holding the resource has gone down, replying RESET recovers the Security File lock.

Replying WAIT retries the request a set number of times. If none of the retries are successful, TSS9123A is reissued.

Action: Reply with desired option: RESET or WAIT. The correct response to the message is WAIT unless all live systems sharing the Security File have been issued the TSS9123A message as well. When all systems have the message, respond RESET on the first system and WAIT on the remaining systems.

Note: If no response is received after one minute has elapsed, CA-Top Secret will automatically reply to this message with WAIT.

**TSS9124I UNEXPECTED I/O ERROR DURING SECURITY FILE SERIALI-
ZATION. SENSE = 'ssss'**

Reason: An I/O error occurred during CA-Top Secret Security File serialization; ssss is the first two bytes of sense information from the VSE CCW.

Action: If the problem persists, call CA Technical Support.

**TSS9125I TSSLOCK PROCESSING DELAYED, WAITING FOR BACKUP TO
COMPLETE ON SYSTEM**

Action: While attempting to serialize the Security File, CA-Top Secret recognized that the lock is being held by another system that is currently performing an automatic backup of the file. Since this is a relatively long duration event, Top Secret will wait an additional amount of time to retry the lock before issuing the TSS9123A message.

Action: Informational message only.

**TSS9126A TSSSENQ: ENQ TABLE SIZE CHANGED FROM xxxxx TO yyyy.
REPLY 'CONT' OR 'TERM'**

Reason: The CA-Top Secret I/O routines determined that the ENQSIZE for this system is different than the size store on the Security File.

Action: Reply 'CONT' if you want the change the current value to yyyy. Reply 'TERM' to retain the current value (xxxxx). This message should normally only occur at CA-Top Secret startup. If it occurs after startup, then the value for ENQSIZE may be different on another system. CA-Top Secret should be stopped and restarted on the system(s) with the incorrect ENQSIZE.

TSS9127I INITIAL ENQ TABLE SIZE IS xxxxx

Reason: Indicates the initial size of the ACID enqueue table.

Action: No action required. Message is informational.

TSS9151D TSSMNGR is not active. Reply <W>ait or <C>ancel

Reason: The CA-Top Secret initialization at IPL has not yet successfully completed.

Action: Check the operator console for initialization messages, including TSS9000I which indicates CA-Top Secret has successfully initialized. Reply 'W' if the initialization process is slow and just needs more time to complete. Reply 'C' if you receive any other indication that the initialization has failed.

**TSS9190A CA-TSS COMMAND PROCESSOR ABEND cccc IN PROGRAM
program**

Reason: The TSS command subtask has abended while processing a TSS command. The request being processed will be failed and an SVC dump will be produced.

In most cases an SVCDUMP will accompany this message. To obtain more information about the error including abend PSW and Registers, The message should be followed by message TSS9191I.

Action:

Examine the SVCDUMP and, unless it indicates a hardware/software problem, contact CA Technical Support for assistance.

TSS9191I TSS COMMAND SUBTASK RECOVERY COMPLETE

Reason: The TSS command subtask has successfully recovered from an abend. It will resume processing the TSS command.

Action: No action required.

TSS9203I SWITCHED TO AUDIT/TRACKING OUTPUT FILE dddddddd

Reason: CA-Top Secret has begun writing to the alternate Audit/Tracking File identified by dddddddd.

Action: No action required.

TSS9204E AUDIT FILE UNAVAILABLE

Reason: CA-Top Secret was not able to open or access the Audit/Tracking File.

Action: Check the TSS.PROC or STDLABEL area to ensure that the CAIAUD1 DLBL statement properly references the Audit/Tracking File.

TSS9205E AUDIT FILE SYNCHRONIZATION ERROR

Reason: An error occurred when CA-Top Secret attempted to locate the logical point within the Audit/Tracking File(s).

Action: Contact CA technical support.

TSS9206E CURRENT FILE, xxxxxxxx, UNAVAILABLE

Reason: CA-Top Secret encountered an error when it attempted to use the indicated Audit/Tracking File.

Action: Ensure that the file has been properly formatted, and the dataset name is properly spelled within the CA-Top Secret Startup JCL.

**TSS9207I The (CURRENT|INITIAL) AUDIT/TRACKING OUTPUT FILE IS
ddddddd**

Reason: Identifies the Audit/Tracking File CA-Top Secret is writing to at startup (INITIAL) or after another system has switched files (CURRENT).

Action: None. Informational message only.

TSS9208I AUDIT/TRACKING FILE, filename, AT LEAST 90% FULL

Reason: The specified Audit/Tracking File is nearly full. When full, the file will wrap and data will be overlaid and lost.

This message is issued when the file is 90% full and subsequently, each time CA-Top Secret is restarted until the situation is corrected.

Action: Back up the Audit/Tracking File, or ignore the message if the File is large enough.

TSS9209I AUDIT FILE HAS WRAPPED

Reason: The Audit/Tracking File has filled up and wrapped.

Action: No action required.

TSS9210E AUDIT FILE ERROR - NOT PREFORMATTED

Reason: The Audit/Tracking File header is not properly formatted.

Action: Make sure the File was created with the current version of the TSSMAINT utility, and the CAIAUD1 DLBL statement in the CA-Top Secret startup procedure is pointing to the correct data set.

TSS9211E AUDIT FILE ERROR - ENQ FAILURE

Reason: CA-Top Secret was unable to ENQ on the Audit/Tracking File.

Action: Contact CA Technical Support.

TSS9212E AUDIT FILE ERROR - INVALID FORMAT

Reason: The Audit/Tracking File header is not properly formatted.

Action: Make sure the File was created with the current version of the TSSMAINT utility, and the CAIAUD1 DLBL statement in the CA-Top Secret startup procedure is pointing to the correct data set.

TSS9213E AUDIT FILE ERROR - UNEXPECTED EOF

Reason: The Audit/Tracking File header is not properly formatted.

Action: Make sure the File was created with the current version of the TSSMAINT utility, and the CAIAUD1 DLBL statement in the CA-Top Secret startup procedure is pointing to the correct data set.

TSS9214E AUDIT FILE ERROR - HEADER ERROR

Reason: The Audit/Tracking File contains invalid data within the first block.

Action: Make sure the File was created with the current version of the TSSMAINT utility, and the CAIAUD1 DLBL statement in the CA-Top Secret startup procedure is pointing to the correct data set.

TSS9215I INPUT BUFFER LENGTH IN ERROR

Reason: The Audit/Tracking File header is not properly formatted.

Action: Make sure the File was created with the current version of the TSSMAINT utility, and the CAIAUD1 DLBL statement in the CA-Top Secret startup procedure is pointing to the correct data set. In addition, ensure that if the Audit/Tracking File was moved, it was not reblocked.

TSS9216I BLOCKSIZE ERROR IN AUDIT FILE

Reason: The blocksize in the Audit/Tracking File header does not match the actual blocksize of the file.

Action: Make sure the TSSMAINT job that created the Audit/Tracking File used the same number in the BLKSIZE parameter on the Proc statement as in the BLKSIZE parameter used as input.

TSS9217I QGET ERROR, CALL CA-SUPPORT CENTER

Reason: CA-Top Secret experienced an error in the Audit/Tracking task queue.

Action: Gather any traces or dumps and contact CA Technical Support.

TSS9218I I/O ERROR ON AUDIT FILE

Reason: An I/O error was encountered with the Audit/Tracking File.

Action: Check the device the file is on, and if the error continues, try to create a new file on a different device.

TSS9219E AUDIT/TRACKING TASK ABENDING

Reason: An error occurred during logging to the Audit/Tracking File.

Action: Gather any traces or dumps and contact CA Technical Support.

TSS9220E AUDIT/TRACKING FILE DLBL NAMES DO NOT MATCH FILE IDS

Reason: This message is issued at startup of CA-Top Secret. The dataset name indicated by the CAIAUDI DLBL DSN= or CAIAUD1 DLBL = statements are incorrect or mismatched. They should state CAIAUD1 DLBL respectively.

Action: Correct the DLBL statements. Refer to your *Installation Guide* for more information.

TSS9269E LOGICAL READ ERROR

Reason: A logical error occurred during a read to the Security File.

Action: Gather any traces or dumps and contact CA Technical Support.

TSS9270E PASSWORD IS INCORRECT

Reason: An attempt was made to utilize the TSS command from an O/S console, and the password supplied in response to the TSS9089A message was not the MSCA's current password.

Action: Gather any traces or dumps and contact CA Technical Support.

TSS9271E UNABLE TO EXECUTE THIS COMMAND

Reason: An attempt was made to utilize the TSS command from an O/S console, and the TSS command was unable to execute.

Action: Gather any traces or dumps and contact CA Technical Support.

TSS9272A ENTER <TSS COMMAND> OR <END>

Reason: You are requested to enter either a TSS command or the characters END to terminate CA-Top Secret command processing via the console.

Action: When entering TSS commands, always enter the characters TSS as in TSS WHOOWNS TERM(R10). The response generated is limited to 50 lines of output, so as not to flood the console.

TSS9273A PASSWORD ERROR

Reason: Incorrect password entered.

Action: Enter the MSCA's previous password.

TSS9274E UNABLE TO LOAD TSS COMMAND

Reason: The system was unable to load module TSSAUTH on behalf of TSS. Possible storage shortage.

Action: No action required.

TSS9301I CA-TOP SECRET TONE INTERFACE INITIALIZATION COMPLETE

Reason: The CA-Top Secret TONE Interface has been activated, and is fully initialized.

Action: No action required.

TSS9400E DUF/Extract Failed - User Has No INSTDATA

Reason: A RACROUTE REQUEST=AUTH, CLASS=DUFXTR has been issued against an ACID that does not have any installation data associated with it.

Action: Add installation data to the ACID.

**TSS9402E ERROR OBTAINING SECURITY RECORD(S) FOR < >
-RETRYING REQUEST**

Reason: CA-Top Secret was unable to obtain an ACID's Security Record in response to a logon or other request. See other error messages issued in conjunction with TSS9402.

Action: No action required.

TSS9403E Insufficient SVA or Local Storage

Reason: CA-Top Secret was unable to satisfy a cross-memory request due to either insufficient EST or insufficient local storage.

Action: If the problem is insufficient SVA, enlarge the SVA/SVA31 site and IPL. (In this case, the message will be issued by multiple address spaces at the same time.)

If the problem is insufficient local storage, decrease the region size and restart the address space.

TSS9404E Security Record Damaged or Insufficient SVA. Try Again

Reason: CA-Top Secret was unable to process a logon request due to insufficient available SVA, or because a record was damaged.

Action: If the problem is a SVA shortage, decrease SVA usage by other users or enlarge the system's SVA size.

TSS9405E NO AUTHORITY FOR INTERNAL SECURITY FUNCTION ()

Reason: A RACROUTE request requiring APF authorization was issued in a non-APR state. Another reason may be that a DUFXTR/DUFUPD call was issued and the ACID making the call does not have the appropriate attribute added to its security record.

Action: Correct the module or library attributes and restart the job or started task or add the DUFXTR/DUFUPD attributes to the ACID making the call. If accompanied by a TSS7100E message, refer to Page DRC-1 for an explanation of the Detailed Reason Codes.

TSS9406E PROBABLE SITE INTERFACING ERROR (drc)

Reason: CA-Top Secret was unable to satisfy a RACROUTE request due to errors in parameters passed on those RACROUTE or improper installation setup.

Action: Check the DRC in the message text. If the DRC is:

030 it is a parameter list error.

035 you need to correct/update the Facility Matrix entry for this facility.

036 the issuer of the RACROUTE request has passed an invalid ACEE to CA-Top Secret.

TSS9407E INTERNAL SYSTEM ERROR ()

Reason: A logic error has occurred during RACROUTE request processing.

Action: If problem persists, contact CA-Top Secret Support Center.

TSS9408E INTERNAL INTEGRITY CHECK FAILED

Reason: A RACROUTE request detected an invalid or overlaid ACEE.

Action: Restart the address space (batch job).

TSS9409I xxx-yy ABEND IN rrrrrrrr PROCESSING reason

Reason: During RACROUTE request processing, CA-Top Secret terminated the request with a system abend code.

Action: Correct errors in module(s) using RACROUTE request.

TSS9410E UNKNOWN CLASSNAME (classname) for SVC (svcname)

Reason: A RACROUTE REQUEST=AUTH or REQUEST=DEFINE has been issued for an undefined class name.

Action: This is usually an implementation error. Add the Resource class to the RDT or correct the module issuing the request.

TSS9420E RLP LOGIC ERROR. SEE CAS3xxxE MESSAGE FOR DETAILS.

J=jobname, A=userid, T=term netname, R=resource name

Reason: The component that performs RLP analysis encountered a logic error within RLP administration definitions. The RECORD, SELECT, or MASKREC definitions are incorrect.

If the user is in FAIL mode, access to the record will be denied.

Action: Refer to the CAS3 message for details of the error.

TSS9485E A SECURITY ABEND HAS OCCURRED DURING SIGNON/SIGNOFF PROCESSING

Reason: An abend occurred while CA-Top Secret was processing a signon or signoff request. Signon/signoff failed.

Action: Notify CA Technical Support.

TSS9498A ALLOW TRAP DUMP FOR JOB=xxxxxxx ACID=xxxxxxx DRC=nnn YES OR NO?

Reason: Issued in response to a matching condition for the DIAGTRAP control option.

Action: Reply YES to take an SVC dump or No to suppress the SVC dump.

TSS9499I TRAP DUMP FOR JOB=xxxxxxx ACID=xxxxxxx

Reason: This message lists the title of a DIAGTRAP SVC dump taken to a SYS1.DUMPnn data set.

Action: No action required.

TSS9500I FACILITY=facility ID=id MODE=mode

Reason: Response to F TSS,FAC(ALL) command. Displays basic information for each facility defined as in-use.

FACILITY = facility name.

ID = the ID used for logging in TSSUTIL/TSSTRACK reports.

MODE = the current mode of the facility.

Action: No action required.

**TSS9501I SECURITY FILE (nnn%) ID = ccccccc SHRFILE(YES|NO|SECURITY)
ENQSIZE(xxxxx)**

Reason: Displays in response to the TSS MODIFY(STATUS) command.

SECURITY FILE (nnn%) = how full the security file is.

ID = ccccccc acronym of Security File in use.

SHRFILE(YES|NO|SECURITY) = whether or not files will be shared among other operating systems and/or CPUs.

Action: No action required.

**TSS9502I LAST CHANGED ON mm/dd/yy AT hh:mm
BACKUP(OFF|ACTIVE-hh:mm)**

Reason: Displays in response to the TSS MODIFY(STATUS) command. LAST CHANGED ON shows a file's archives

mm/dd/yy = date of last change made to the Security File as recorded in the Recovery File.

hh:mm = time of last change

BACKUP(OFF|ACTIVE-hh:mm) = whether or not automatic backup is on or off, or set up to go on during a specific time of day

Action: No action required.

TSS9503I AUDIT FILE (nnn%|N/A) RECOVERY FILE(nnn%|N/A)

Reason: Displays in response to the TSS MODIFY(STATUS) command.

nnn% = the percentage of the file that is full

if the AUDIT file is not available, 'N|A' will appear instead

Action: No action required.

TSS9504I TIMER(nnn) SYSOUT(C,CCCCCCCC) CANCEL(YES|NO)

Reason: Displays in response to the TSS MODIFY(STATUS) command.

TIMER(nnn) = the time interval at which data is written from CA-Top Secret buffers to the AUDIT/TRACKING file

SYSOUT(C,CCCCCCCC) = the class and destination of the diagnostic log output

CANCEL = whether or not the address space is eligible for cancellation

Action: No action required.

TSS9505I AUTH(opt,opt) MODE(mode) DOWN(Bx)

Reason: Displays in response to the TSS MODIFY(STATUS) command.

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

MODE signifies the security mode in which CA-Top Secret is operating.

DOWN determines how jobs are initiated and passwords are changed when address space is inactive. Bx = Batch, Ox = online. Valid values for 'x' are: W = Wait, B = Bypass, N = Normal, F = Fail.

Action: No action required.

TSS9505I FACMODE(nnx,nnx,nnx,...)

Reason: nn=ID of the facility and x=security mode the facility is operating under.

Valid values for "x" are: F=fail, W=warn, I=implement, D=dormant.

Action: Determine the ID by issuing a TSS MODIFY FAC(ALL).

TSS9506I LOG(opt,opt,...) LOGBUF(nnnn) CURRBUF(nnnn)

Reason: Displays in response to the TSS MODIFY(STATUS) command.

LOG = the GLOBAL logging options in effect

LOGBUFF = the maximum number of buffers CA-Top Secret will obtain

CURRBUF = the number of buffers currently in use

Action: No action required.

TSS9507I JOBACID(c,n,n) SUBACID(c,n) VMJESLNK(cccc)

Reason: Displays in response to the TSS MODIFY(STATUS) command.

JOBACID = how ACIDs for batch jobs are derived

SUBACID = how ACIDs for online batch jobs are derived

VMJESLINK = identifies the nodes from which CA-Top Secret will assign an ACID of the VM submitting user

Action: No action required.

TSS9510I TEMPDS(YES|NO) TAPE(OFF|DEF|DSN)

Reason: Displays in response to the TSS MODIFY(STATUS) command.

TEMPDS = whether or not temporary data sets are protected
TAPE= the type of tape protection (if any) in effect at the installation
OFF = CA-Top Secret is not invoked to validate a tape access request
DEF = CA-Top Secret validates access requests for defined volumes only
DSN = CA-Top Secret performs data set name checking using the full data set name on the DSN keyword of the JCL

Action: No action required.

TSS9511I PWEXP(nnn) PWHIST(nn) HPBPW(nnn) PWVIEW(YES|NO)

Reason: Displays in response to the TSS MODIFY(STATUS) command.

PWEXP = the password expiration interval
PWHIST = number of previous passwords to be maintained for an ACID file
HPBPW = the maximum number of days CA-Top Secret will honor an expired or previous password for batch jobs
PWVIEW = whether or not passwords may be viewed by authorized administrators

Action: No action required.

TSS9512I NEWPW(MIN=n,WARN=n,MINDAYS=nn,MASK=???????,opt,opt,..)

Reason: Displays in response to the TSS MODIFY(STATUS) command.

MIN = the minimum length of a password
WARN = number of days before expiration warning appears
MINDAYS = minimum number of days before the password can be changed by user
MASK = mask used to generate random passwords

Action: No action required.

TSS9513I PTHRESH(nnn) VTHRESH(nnn,cccc) INACTIVE(nnn)

Reason: Displays in response to the TSS MODIFY(STATUS) command.
PTHRESH defines the number of unsuccessful attempts a user is allowed when entering his or her password. Once PTHRESH is exceeded, the user is automatically suspended.
nnn = number of allowed guesses.

VTHRESH indicates the violation threshold and action, where:

nnn = number of allowed violations per session
ccc = the action(s) CA-Top Secret is to take when VTHRESH has been exceeded

INACTIVE selects the number of days before TSS will deny an unused ACID access to the system after the ACID's password has expired.

Action: No action required.

TSS9514I NPWRTHRESH(n) MSUSPEND(YES|NO)

Reason: Displays in response to the TSS MODIFY(STATUS) command.

NPWRTHRESH = the number of retry attempts allowed when attempting new password reverification before complete logon sequence needs restarting.

MSUSPEND = whether or not MSCA will be suspended if password violation occurs.

Action: No action required.

TSS9515I EXIT(ON|OFF) DATE(mm/dd/yy)

Reason: Displays in response to the TSS MODIFY(STATUS) command.

EXIT = the installation exits is activated (ON) or deactivated (OFF)

DATE = the format for dates displayed in listings

Action: No action required.

TSS9516I CPF(ccc) CPFWAIT(ccc) CPFTARGET(ccccccc)

Reason: Displays in response to the TSS MODIFY(STATUS) or the TSS MODIFY(CPFSTAT) command.

CPF(ON|OFF|INACTIVE) specifies whether or not the Command Propagation Facility (CPF) will be activated at startup.

CPFWAIT controls the default for the TSS command WAIT keyboard.

YES = a default value for TSS command WAIT keyword.

NO = no waiting will occur for messages.

CPFTARGET sets a default value for the TSS command TARGET keyword.

LOCAL = command execution is restricted to the local node only.

AUTO = target information from each command will be saved and used for the default routing of subsequent commands.

* = command execution is transmitted to all nodes defined in the CPFNODES control option.

Action: No action required.

TSS9517I CPFNODE(ccccc) STATUS(ccccc)

Reason: Displays in response to the TSS MODIFY(STATUS) or the TSS MODIFY(CPFSTAT) command.

CPFNODE indicates the current nodes to which CA-Top Secret commands may be transmitted.

STATUS provides the current settings of various control options and information concerning cross memory and Security File Service requests.

ACTIVE|INACTIVE = whether or not the VTAM node is currently active

SPOOL|NOSPOOL = whether or not commands sent to that node will be recorded to a spool file

ABEND = the connection to the node is in the process of abending

RETRY = an error occurred when transmitting to a remote node and CA-Top Secret is currently trying to resubmit the request.

PRE30 = the default is for a pre-release 3.0 connection. Once a command is sent to the receiving node, CA-Top Secret will determine whether the connection is to a 3.0 and set the status appropriately.

Action: No action required.

TSS9518I PRODUCTS(ccccc,cccc,....)

Reason: Displays in response to the TSS MODIFY(STATUS) command the list of products defined on your system.

Action: No action required.

TSS9520I DUFPGM(cccccc,cccc,cccc)

Reason: Displays the program names which will be allowed to retrieve and update installation data via DUFUPD and DUFXTR.

Action: No action required.

TSS9522I TEXTTSS(cccccccccccccccccc) DISPLAY(cccc)

Reason: Displays the text string that will display on reports and messages. The default is CA-Top Secret Security.

Action: No action required.

TSS9530I BYPASS(EVERYJOB|cccc,cccc,cccc)

Reason: Displays in response to the TSS MODIFY(STATUS) command.

BYPASS specifies jobs that bypass security in an emergency. EVERYJOB means that ALL jobs and online sessions bypass security.

Action: No action required.

**TSS9531I SECTRACE(ON|ACT,WTO|WTL) DIAGTRAP(www,cccccc,nn)
DEBUG(ON|OFF)**

Reason: Displays in response to the TSS MODIFY(STATUS) command. SECTRACE indicates the diagnostic security trace on users.

ON = global trace.

ACT = trace for users that have the TRACE attribute attached to their ACIDs.

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).

DIAGTRAP produces a diagnostic dump for CA Technical Support.

www = the trap is activated in a particular location.
ccccccc = the ACID or jobname which will trigger the dump.
nn = the DRC which will trigger the dump.

DEBUG controls debugging dumps that determine the cause of abnormal error conditions.

ON = a diagnostic dump, as requested by CA Technical Support.
OFF = DEBUG feature is deactivated.

Action: No action required.

TSS9532I IOTRACE(ccc) SFSDIAG(n) GTRACE(nnn)

Reason: Displays the setting (either ON or OFF) for the IOTRACE control option. The IOTRACE control option and diagnostic trace is used by CA technical support. Therefore, it should not be ON unless required by CA technical support.

Action: No action required.

TSS9533I CPFRCVUND(YES|NO)

Reason: YES indicates that CPF will communicate with nodes that are not defined in the local system node list.

NO indicates that CPF will not communicate with nodes that are not defined in the local system node list.

Action: Modify your CA-Top Secret parameter list to indicate the appropriate status.

TSS9541I DRC=nnn,MSG=TSSnnnn,SEC9=TSSnnnn,settings

Reason: Displays the DRC control option setting for the specified DRC.

DRC = the DRC#.
MSG = the message issued to the end user when the violation occurs.
SEC9 = the message issued to the security console when the violation occurs.
settings = the current options associated with the DRC, refer to the Control Options Guide for a description of their meanings.

Action: No action required.

TSS9542I rpw ppw rpw ppw

Reason: Displays the passwords restricted through the RPW control option.

TSS9543I msg# Settings

Reason: Displays MSG control option settings for the specified message number (msg#).

Action: No action required.

TSS9550I FACILITY DISPLAY FOR facility

Reason: Response to TSS,FAC(facility) command. Messages TSS9551I through TSS9555I (through TSS9570I for CICS) will also be displayed.

Action: No action required.

TSS9551I INITPGM=pgmname ID=f

Reason: INITPGM provides the name of the internal module program that is used to identify the facility that a user is signing on to.

ID 'f' indicates the unique code that identifies the facility for TSSUTIL/REPORT.

Action: No action required.

TSS9552I ATTRIBUTES=attributes list

Reason: Lists the attributes that are in effect for the facility.

Action: Refer to the *Control Options Guide* for the meaning of the listed options.

TSS9553I MODE=mode DOWN=options LOGGING=logging

Reason: Specifies the MODE for the facility.

Action: No action required.

TSS9554I UIDACID=s LOCKTIME=nnn DEFACID=xxxx KEY=xxx

Reason: Lists the logging options in use for the facility.

Action: No action required.

TSS9560I FACMATRX=YES|NO EXTSEC=YES|NO SAFMODE=YES|NO

Reason: Lists the options in the facility for FACMATRX, EXTSEC and SAFMODE.

FACMATRX

Indicates whether CA-Top Secret will use the settings from the Facility Matrix or the DFHSIT parameter settings (for XTRAN, XPCT, XFCT, etc.).

EXTSEC Indicates whether or not external security is requested.

SAFMODE Indicates whether or not SAF is requested.

Action: No action required.

**TSS9561I XJCT=YES|NO XFCT=YES|NO XCMD=YES|NO XDCT=YES|NO
XTRAN=YES|NO**

Reason: Identifies SIT parameters for a CICS facility.

XJCT Indicates whether or not JCT security protection is active.

XFCT Indicates whether or not FCT security protection is active.

XCMD Indicates whether or not command security protection is active.
XDCT Indicates whether or not DCT security protection is active.
XTRAN Indicates whether or not transaction security protection is active.
Action: No action required.

**TSS9561I XTST=YES|NO XPSB=YES|NO XPCT=YES|NO XPPT=YES|NO
XAPPC=NO|YES XUSER=YES|NO**

Reason: Identifies SIT parameters for a CICS facility.

XTST Indicates whether or not TCT security protection is active.
XPSB Indicates whether or not PSB security protection is active.
XPCT Indicates whether or not PCT security protection is active.
XPPT Indicates whether or not PPT security protection is active.
XAPPC Indicates whether or not session security protection is active.
XUSER Indicates whether or not USER security protection is active.
Action: No action required.

**TSS9564I PCTEXTSEC=HONOR|OVERRIDE
PCTCMDSEC=HONOR|OVERRIDE PCTRESSEC=OVERRIDE|HOLD**

Reason: Indicates whether to honor or override the CICS DFHPCT parameter settings.

PCTEXTSEC

Indicates whether or not CA-Top Secret will force transaction security or will honor what has been specified for the PCT EXTSEC= parameter.

PCTCMDSEC

Indicates whether or not CA-Top Secret will force EXEC CICS command protection or will honor what has been specified for PCT CMDSEC= parameter.

PCTRESSEC

Indicates whether or not CA-Top Secret will force resident security protection or will honor what has been specified for PCT RESSEC= parameter.

Action: No action required.

**TSS9565I DSNCHECK=YES|NO LTLOGOFF=YES|NO|SIGNOFF RLP=NO|YES
SLP=NO|YES**

Reason: Lists the dataset name and LOCKTIME logoff options for the facility. It also lists whether or not Record Level Protection and/or Screen Level Protection is active.

DSNCHECK

Indicates whether or not dataset name security is active.

LTLOGOFF

Indicates whether or not the users terminal will be logged off from CICS after their locktime has expired a second interval.

RLP Indicates whether or not Record Level Protection is active.

SLP Indicates whether or not Screen Level Protection is active.

Action: No action required.

TSS9566I MAXUSER=nnnn PRFT=nnn MAXSIGN=nnn,cccc

Reason: User entered a TSS MODIFY(FAC(TSS PROD)) which generated a string of messages and options showing all settings on that facility.

Action: No action required.

TSS9567I MAXSIGN VALUE EXCEEDS LIMIT, MAXIMUM VALUE ASSIGNED

Reason: The MAXSIGN facility sub option value entered is greater than the maximum allowed. The maximum acceptable value has been assigned.

Action: No action required.

TSS9570I BYPASS TABLE DISPLAY FOR FACILITY facility

Reason: Identifies the CICS facility for which a bypass list is displayed.

Action: No action required.

TSS9571I RESOURCE=resource BYPASS NAMES=name

Reason: Identifies CICS resources and names which will bypass CICS security checking within a CICS facility.

RESOURCE Identifies the type of resource

BYPASS NAMES Identifies the name(s) of the resource(s).

Action: No action required.

TSS9571I PROTECT NAMES: name

Reason: Identifies CICS resources that will **not** bypass CICS security checking within a CICS facility.

PROTECT NAMES Identifies the name(s) of the resource(s) being protected.

Action: No action required.

TSS9584I A SECURITY ABEND HAS OCCURRED PROCESSING TSS TRANSACTION

Reason: An ABEND occurred in CA-Top Secret while processing the TSS transaction. The transaction was not processed.

Action: Notify CA Technical Support.

TSS9590I INIT(n) XREQ(n) VSE(n)

Reason: Displays in response to the STATUS option.

INIT = number of job initiations validated
XREQ = number of cross-memory requests processed
VSE = number of VSE security calls processed

Action: No action required.

TSS9591I VIOL(n) EXEC(n) SMF(n)

Reason: Displays in response to the STATUS option.

VIOL = number of violations detected
AUDIT = number of AUDIT security records logged
SMF = number of SMF security records logged

Action: No action required.

TSS9592I CHNG(n) RECV(n) AUD(mnn)

Reason: Displays in response to the STATUS option.

CHNG = number of changes made to the Security File
RECV = number of changes saved in the Recovery File
AUD= number of records logged to Audit File

The CHANGE value will only be incremented if any of the following commands are issued:

ADD an ACID or a volume
DELETE an ACID or a volume
RENAME an ACID
REMOVE a volume

Action: No action required.

TSS9593I READ(n) WRIT(n)

Reason: Displays in response to the STATUS option.

READ = number of Security File Input requests
WRIT = number of Security File Output operations

Action: No action required.

TSS9594I #REQ(nnnnnn) LOCK(nnnnnn) LWAIT(nnnnnn)

Reason: Displays in response to the TSS MODIFY(STATUS) option.

#REQ = number of cross-memory security checks awaiting processing

LOCK = number of Security File lock I/Os issued

LWAIT = the number of failed Security File lock I/Os causing a wait

Action: No action required.

TSS9598A ALLOW TRAP DUMP FOR JOB=xxxxxxx ACID=xxxxxxx DRC=000

Reason: A trap event has occurred which requires operator prompting.

Action: Reply YES to cause a dump for the specified job and ACID or NO to indicate that a dump should not be taken.

TSS9599E TRAP DUMP FOR JOB=xxxxxxx ACID=xxxxxxx

Reason: Diagtrap has been taken.

Action: None required.

TSS9601E INVALID PLIST WAS SPECIFIED TO THE CACHE MODULE

Reason: The caller to the CACHE function did not prepare a valid Plist.

Action: Contact CA-Top Secret Technical Support.

TSS9602E INVALID ANCHOR WAS SPECIFIED TO THE CACHE MODULE

Reason: The caller to the CACHE function did not provide a valid anchor in the Plist.

Action: Contact CA-Top Secret Technical Support.

TSS9603E INVALID OPCODE WAS SPECIFIED TO THE CACHE MODULE

Reason: The caller to the CACHE function did not provide a valid OPCODE in the Plist.

Action: Contact CA-Top Secret Technical Support.

TSS9604E CACHE FAILED TO FREEVIS

Reason: The CACHE module tried to FREEVIS a portion of the CACHE but the FREEVIS SVC failed with a RC of 4. This means that some storage will stay allocated and may be a symptom of another problem.

Action: Watch for other messages and if the problem recurs contact CA-Top Secret Technical Support.

TSS9605W CACHE FAILED TO GETVIS. WILL CAUSE LESS EFFICIENT PERFORMANCE IMPROVEMENTS

Reason: The CACHE module tried to GETVIS a storage area for CACHE but the GETVIS SVC failed, probably due to a lack of storage. This means that the CACHE mechanism will not work at full capacity and may indicate some other problems in the system.

Action: Watch for other messages and if the problem recurs contact CA-Top Secret Technical Support.

TSS9610I ----- COMMAND PROCESSOR WORKLOAD BALANCE -----

Reason: Informational, in response to a MODIFY STATS command.

Action: No action required.

TSS9611I Total Commands Issued = nnnnnnnnnn

Reason: The total number of TSS commands issued in response to a MODIFY STATS command since TSSMNGR was started.

Action: No action required.

TSS9612I Cmd xx = nnn.nn% Cmd xx = nnn.nn%

Reason: For each active command processor (xx), the percent of that processor used based on the total number of commands issued. By default, two command processors are started at TSSMNGR initialization. The number of command processors can be increased by the CMDNUM control option. See the *Control Options Guide* for more information on CMDNUM.

Action: No action required.

TSS9613I Cmd xx = nnn.nn%

Reason: See message TSS9612I for a full description. This message is only displayed if there are an odd number of command processors active.

Action: No action required.

TSS9660I VERSION= n.n

Reason: Response to TSS, VERSION command. Displays the CA-Top Secret version number you are running.

Action: No action required.

TSS9680A CA-TSS VISTASK MANAGER ABEND cccc IN PROGRAM program

Reason: The CA-Top Secret address space has failed. Existing jobs and users will continue to function with full security in effect. New initiations are subject to DOWN options.

In most cases an SVCDUMP will accompany this message. To obtain more information about the error including abend PSW and Registers.

Action: Restart the CA-Top Secret address space, obtain dumps (if produced) and report the error to CA Technical Support.

TSS9681A CA-TSS SECURITY FILE SERVICES ABEND cccc IN PROGRAM program

Reason: The Security File services subtask has failed. Existing jobs will continue to function with full security in effect. New initiations are subject to DOWN options.

In most cases an SVCDUMP will accompany this message. To obtain more information about the error including abend PSW and Registers.

Action: Restart the CA-Top Secret address space, obtain dumps and report the error to CA Technical Support.

TSS9682A CA-TSS OPERATOR COMMUNICATIONS ABEND cccc IN PROGRAM program

Reason: The operator communication subtask has failed.

Action: See message TSS9681A

TSS9683A CA-TSS TIMER CONTROLS ABEND cccc IN PROGRAM program

Reason: The asynchronous logging subtask has failed

Action: See message TSS9681A

TSS9684A CA-TSS AUDIT FILE SERVICES ABEND cccc IN PROGRAM program

Reason: The asynchronous logging subtask has failed.

Action: See message TSS9681A

TSS9692E PASSWORD IS INCORRECT

Reason: The supplied password is incorrect.

Action: No action required.

TSS9700E DUF/EXTRACT FAILED - USER HAS NO (INST) DATA

Reason: A DUFUPD, DUFXTR or EXTRACT request (RACHECK) failed because the specified ACID did not have INSTALLATION data.

Action: No action required.

TSS9702E ERROR OBTAINING SECURITY RECORD(S) FOR acid. RETRYING REQUEST

Reason: While initiating a job or session, CA-Top Secret was unable to obtain the Security Record for the user due to an error in the TSS address space.

Action: CA-Top Secret retries once. If error persists, the Security Record may have been damaged or the Security File itself is damaged. Attempt recovery. If problem was not caused by system or hardware failure, contact CA Technical Support.

TSS9703E INSUFFICIENT SVA OR LOCAL STORAGE

Reason: During a job/session initiation, CA-Top Secret was unable to transfer the user's security record(s) from the CA-Top Secret address space to that of the user.

Action: Probable cause is lack of common storage (SVA). This is a system-wide problem.

TSS9704E SECURITY RECORD DAMAGED OR INSUFFICIENT SVA. TRY AGAIN.

Reason: An error that cannot be corrected was detected in the Security Record.

Action: Attempt to recover the Security Record. If the problem was not attributable to system software or hardware failure while updating the record, contact CA Technical Support.

TSS9705E NO AUTHORITY FOR INTERNAL SECURITY FUNCTION function

Reason: A RACINIT macro was issued by an unauthorized task or, the task has insufficient authority to DUFXTR or DUFUPD.

Action: See the FACILITY/AUTHINIT control option, or add DUFXTR and/or DUFUPD to the ACID.

TSS9706E PROBABLE SITE INTERFACING ERROR drc

Reason: Refer to the **Detailed Reason Code section** for cause of problem.

Action: If not a user error, contact CA Technical Support.

TSS9707E INTERNAL SYSTEM ERROR (drc)

Reason: Refer to the **Detailed Reason Code section** for cause of problem.

Action: If not a user error, contact CA Technical Support.

TSS9708E INTERNAL INTEGRITY CHECK FAIL

Reason: CA-Top Secret checks for user's environment every time an access takes place. The environment has been altered; possible subversion or system error.

Action: Take a dump of the user's address space. Contact CA Technical Support.

TSS9709I aaa-bb ABEND IN svcname PROCESSING- reason

Reason: A system abend has been issued in response to an invalid condition being detected by the CA-Top Secret SVC handler.

aaa Abend code in hexadecimal.

bb Reason code in hexadecimal.

svcname Name of security svc issued.

reason Short explanation of error encountered.

Summary of 282 abend and reason codes and their meanings:

-10 ABEND IN RACHECK PROCESSING- NOT APF AUTHORIZED

The form of RACHECK issued requires APF authorization but was issued by a non-APF caller.

-1C ABEND IN RACHECK PROCESSING- PROFILE/ENTITY CONFLICT

The RACHECK parameter list has conflicting bit settings. The parameter list indicates that both the PROFILE= and ENTITY= parameters have been coded.

Action: Correct the error(s) in the issuing code and rerun the job.

TSS9715E STORAGE OBTAIN FAILED <module/subroutine>

Reason: An internal error occurred.

Action: Contact CA Technical support.

TSS9716E STORAGE RELEASE FAILED <module/subroutine>

Reason: An internal error occurred.

Action: Contact CA Technical support.

**TSS9719E AN UNAUTHORIZED MODIFY COMMAND WAS ISSUED FROM
SYSTEM system BY USER acid**

Reason: A TSS MODIFY command was received from another system but the acid issuing the command is not defined to this system or does not have CONSOLE authority.

Action: Contact CA Technical support.

TSS9723E INCORRECT BUFFER SIZE FOR CF

Reason: A buffer size of 0 or larger than 32K was requested.

Action: Specify a buffer size between 1 and 32K.

Module: TSSSFSC1

Module: TSSMNGR

TSS9734E CA-TOP SECRET ALREADY CONNECTED

Reason: The system was already connected when a second connect was issued.

Action: If you wish to change connect information, you must first disconnect then reissue the connect.

Action:

TSS9737I DUPLICATE NAME GIVEN FOR CONNECT/GROUP/STRUCTURE

Reason: This is an informational message indicating that name specified on a SYSPLEX control option has already been used.

Action: Reenter the command specifying a different name for the connection, group or structure.

TSS9740E BAD PARM FOR TNGMON

Reason: A user error was encountered.

Action: You must correct parameters that caused error.

TSS9741E TNGMON TABLE MISSING

Reason: An internal CA-Top Secret problem occurred.

Action: Contact CA Technical Support.

TSS9742E STORAGE OBTAIN FAILED

Reason: Storage could not be obtained.

Action: Contact CA Technical Support.

TSS9743I ENTRY NOT FOUND

Reason: Requested entry could not be found.

Action: This is an informational message.

**TSS9800I CPF RECOVERY FILE FAILED TO OPEN: CONTINUING
WITHOUT FILE**

Reason: CA-Top Secret attempted to open the CPF recovery file (CAICPFR DLBL in the CA-TSS startup PROC) but failed. CPF processing will continue.

Action: If you desire to use the automatic queueing mechanism of CPF, ensure the CAICPFR DLBL is present in the startup proc for CA-Top Secret or in standard labels.

**TSS9801I CPF RECOVERY FILE HDR INCORRECT: FILE WILL NOT BE
PROCESSED**

Reason: CA-Top Secret opened the CPF recovery file but found it was not properly formatted. CPF processing will continue.

Action: Ensure the data set pointed to by the CAICPFR DLBL in the startup proc for CA-Top Secret has been properly formatted by TSSVIST.

TSS9802I FREEVIS FAILURE IN CPF TASK

Reason: Internal CPF error.

Action: Contact CA Technical support.

TSS9803W NO FREE RECORDS ON CPF RECOVERY FILE

Reason: CA-Top Secret attempted to write a record to the CPF recovery file, but the file was full.

Action: Since CA-Top Secret only writes to the recovery file when the receiving node is down, determine why that receiving has not restarted. If necessary, enlarge the CPF recovery file.

TSS9804A CA-TSS CPF COMMUNICATIONS LINK ABEND cccc IN PROGRAM program

Reason: The CPF Communications services subtask has failed. TSS commands and password changes will continue to function but will not be sent to remote nodes. CPF(OFF) will be in effect once this abend occurs.

Action: CPF can be restarted using the TSS MODIFY CPF(ON) command. Obtain dumps and report event to CA Technical Support.

In most cases an SVCDUMP will accompany this message.

TSS9805A CA-CCI NOT AVAILABLE, AUTO RETRY IN PROGRESS. REPLY <N> TO STOP CPF

Reason: The CPF subtask within CA-Top Secret has started, attempted to contact the CCI component of CA-ENF and found it was not available.

Action: This message informs you that CA-Top Secret is still attempting to connect with CCI. This message will be deleted when the connection is made Reply <N> if you do not wish to use CPF.

TSS9806I COMMAND QUEUED FOR DESTINATION cpfnode

Reason: Indicates (on the CPF journal file) to which node a command has been routed.

Action: None - Information only.

TSS9807I COMMUNICATIONS FAILURE (nnnn), COMMAND NOT SENT TO DESTINATION cpfnode

Reason: The command was not sent to the specified destination or node. This probably occurred because the link to the remote destination is down.

Action: Contact systems programmer to activate the link.

TSS9808E MSG FAILED VALIDITY CHECK ON REMOTE MACHINE

Reason: Internal CPF error.

Action: Contact CA Technical support.

**TSS9809E MSG FAILED DUE TO TOP SECRET SYSTEM ERROR ON
REMOTE MACHINE**

Reason: Internal CPF error.

Action: Contact CA Technical support.

TSS9810I *** COMMUNICATIONS ESTABLISHED WITH NODE xxxxxxxx**

Reason: CA-Top Secret has established remote communications.

Action: None - Information only.

TSS9811I *** CPF SUBTASK INITIALIZED FOR NODE *******

Reason: A new target node has been added to the current list of CPF nodes (VIA the NODES control option) and communications have been established.

Action: None - Information only.

TSS9812I REMOTE MACHINE NOT RECEIVING: CPF(OFF) SET

Reason: A TSS command was routed though CPF to a remote node. The CA-Top Secret running on the remote node had the CPF control option set to OFF. The command was rejected by the remote node.

Action: Determine why CPF is inactive on the remote node.

TSS9813I NODE BUSY; COMMAND NOT SENT TO NODE cpfnode

Reason: Someone else is also in the process of sending a synchronous command (via WAIT(Y)) to the remote node. The command was not sent to that node.

Action: This should not happen often. If so, contact CA Technical support.

**TSS9814E COMMAND RESULTS ON TARGET NODE node UNKNOWN; COM-
MUNICATIONS LOST**

Reason: The CA-Top Secret command was successfully sent to the specified node but communications with the node were lost before a response to the command was received.

Action: After communications are re-established with the node, either issue additional TSS commands or check the CPF Journal File for the completion status of the command.

TSS9815I CAICCI REASON TEXT: text

Reason: This message is issued immediately after message TSS9807I to explain the reason for the communication failure. The reason text in this message was provided by CAICCI.

Action: Refer to the CA-CIS documentation for more information.

TSS9816I REMOTE MACHINE NOT ACCEPTING COMMANDS FROM THIS NODE

Reason: A targeted node cannot accept commands from the originating node because either the originating node is defined to the target node as send-only (i.e. 'CPFNODES(ORIGNODE(S))') or the target node is running with CPFRCVUND(NO) set.

Action: Either do not target any TSS commands to the remote node or have the control options changed at the remote node to accept TSS commands from this node.

TSS9817I COMMANDS CANNOT BE SENT TO DESTINATION xxxxxxxx

Reason: TSS commands cannot be sent to a targetted node because that node is defined as receive-only (i.e. 'CPFNODES(TGTNODE(S))').

Action: Either do not target any TSS commands to the remote node or have the control options changed to allow commands to be sent to that node.

TSS9818I CPF RECOVERY FILE CONTAINS BAD RECORDS. REFORMAT REQUIRED.

Reason: During CPF recovery file initialization, records were discovered that do not match the CA-Top Secret Release 3.0 structure.

Action: Initialization will continue but CPF recovery will be turned off. Use the TSSVIST to reformat the CPF recovery file to eliminate any bad records.

TSS9993E STORAGE NOT FREED <c>

Reason: CA-Top Secret was unable to FREEVIS storage which it had allocated.

Action: Contact CA Technical support.

TSS9994E THE FDT IS MISSING. RESTART CA-TOP SECRET. INFORM SUPPORT.

Reason: During startup, CA-Top Secret attempted to merge the FDT with an updated base RDT that has been corrupted.

Action: Stop and restart CA-Top Secret, note whether you receive a TSS9045I RDT SYNCHRONIZATION COMPLETE message, contact CA-Top Secret Support.

TSS9999E CA-TSS SECURITY SVC ABEND cccc IN PROGRAM program

Reason: An error that **cannot** be corrected occurred when CA-Top Secret tried to validate a user's request for access to a resource. The error occurred within the user's address space. Also used for DIAGTRAP dump.

In most cases an SVCDUMP will accompany this message.

Action: If a system dump was taken, contact CA Technical Support.

Chapter 2. CAS Messages

2.1 CAS20 System Authorization Facility (SAF) Messages

CAS2000E UNDEFINED MESSAGE NUMBER *nnn*

Reason: Indicates that an attempt was made to print a message with the specified message number but the message number does not exist. *nnn* is the specified message number that could not be identified.

Action: Verify that CA-Top Secret has been installed correctly. If so, contact CA-Top Secret technical support and provide the message number and diagnostic information.

Module: SAFMSGFM

CAS2001E UNABLE TO ISSUE MESSAGE NUMBER *ooo* FOR UNDEFINED MESSAGE NUMBER *nnn*

Reason: The CA SAF message formatter tried to issue a message (*nnn*) that is not defined in the message table. When it tried to issue the message (*ooo*) to report the error, that message was also unavailable. This could occur if your site has modified the message table and damaged it.

Action: CA-Technical Support and provide any messages issued just before or after you received this message.

Module: SAFMSGFM

CAS2002E UNABLE TO ISSUE *sss* MESSAGE NUMBER *nnn*; THE MESSAGE TABLE IS NOT AVAILABLE

Reason: The CA SAF formatter tried to issue a message but it could not find the message table.

sss The name of the subsystem whose message table could not be found.

nnn The message number of the message that could not be issued.

Action: Verify that CA-Top Secret has been installed correctly. If so, contact CA-Top Secret technical support and provide the message number and any messages issued just before or after this message.

Module: SAFMSGFM

2.1.1 Security Initialization Routine

CAS2030E CA SAF INTERFACE INITIALIZATION - LOAD FAILED FOR MODULE lmod

Reason: The specified module could not be loaded. *lmod* is the specified load module name.

Action: Verify that CA-Top Secret has been installed correctly. If so, contact CA-Top Secret technical support and provide this message number and diagnostic information.

Module: SAFRTSEC

CAS2031I CA SAF INTERFACE INITIALIZATION COMPLETE

Reason: The CA SAF interface has been successfully initialized.

Action: This message is for information only. No action is required.

Module: SAFRTSEC

CAS2032E CA SAF INTERFACE INITIALIZATION FAILED

Reason: The CA SAF interface initialization failed.

Action: Contact CA-Top Secret technical support and provide this message number and diagnostic information.

Module: SAFRTSEC

2.2 CAS22 SAF Common Service Routines

CAS2220E * PBLOCK DEFINITION IN ERROR *****

Reason: This message indicates an internal error in parsing a RACROUTE call.

Action: CA-Technical Support and provide any messages that occurred just before or after this one.

Module: SAFAATST

CAS2221E * PBLOCK OPERANDS IN ERROR *****

Reason: This message indicates an internal error in parsing a RACROUTE call.

Action: CA-Technical Support and provide any messages that occurred just before or after this one.

Module: SAFAATST

CAS2225E RET: rrr RSN: sss PLF-ID: ppp OPDEF-ID: ooo

Reason: This message indicates an internal error in parsing a RACROUTE call.

Action: CA-Technical Support and provide this message and any messages that occurred just before or after this one.

Module: SAFAATST

CAS2226E ASMNAME: aaa OPERAND: ooo POS: ppp

Reason: This message indicates an internal error in parsing a RACROUTE call.

Action: CA-Technical Support and provide this message and any messages that occurred just before or after this one.

Module: SAFAATST

CAS2227E DATAPTR: ppp DATALEN: lll VALFLAGS: fff

Reason: This message indicates an internal error in parsing a RACROUTE call.

Action: CA-Technical Support and provide this message and any messages that occurred just before or after this one.

Module: SAFAATST

CAS2228E text

Reason: This message indicates an internal error in parsing a RACROUTE call.

Action: CA-Technical Support and provide this message and any other messages that occurred just before or after this one.

Module: SAFAATST

CAS2230W * UNDEFINED DATA IN SOURCE PLIST *****

Reason: This message indicates an internal error in parsing a RACROUTE call.

Action: CA-Technical Support and provide any messages received just before or after this one.

Module: SAFAATST

CAS2235W OFFSET: ooo LENGTH: lll NAME: nnn

Reason: This message indicates an internal error in parsing a RACROUTE call.

Action: CA-Technical Support and provide this message and any other messages that occurred just before or after this one.

Module: SAFAATST

CAS2236W DATA: ddd

Reason: This message indicates an internal error in parsing a RACROUTE call.

Action: CA-Technical Support and provide any messages received just before or after this one.

Module: SAFAATST

CAS2241E SAF PLIST SCAN FAILED FOR BLOCK bbb, RC=rc RSN=rsn

Reason: An error occurred while trying to parse the RACROUTE parameter list created by the RACROUTE specifications in the SAFDEF record.

Action: Contact CA-Top Secret technical support and provide this message number and diagnostic information.

Module: SAFAASDB

CAS2242E INVALID RACROUTE REQUEST TYPE SPECIFIED, TYPE=tt

Reason: The RACROUTE REQUEST= parameter specifies a value unknown to the CA-Top Secret RACROUTE parameter list data structure.

Action: Contact CA-Top Secret technical support and provide this message number and diagnostic information.

Module: SAFAASDB

CAS2243E PLIST BUILD ERROR, REQUEST: rr FIELD: ff RC: rc RSN: rsn

Reason: A severe error occurred while processing the SAFDEF RACROUTE parameters in the SAFDEF record.

rr Specifies the parameter list build request.

00 Initialization request

04 Process operand request

08 Termination request.

ff The keyword field in error. N/A indicates that the parameter is not applicable for the specified call.

rc Specifies the return code from the RACROUTE parameter list build service.

rsn Specifies the reason code from the RACROUTE parameter list build service.

Action: Contact CA-Top Secret technical support and provide the message number and diagnostic information.

Module: SAFAASDB

CAS2244E PLIST BUILD ERROR, FIELD: kwd RSN: rsn

Reason: An error occurred while processing the SAFDEF RACROUTE parameter specifications. *kwd* specifies the keyword field in error. *rsn* describes the reason that the SAFDEF RACROUTE operand is in error. It appears as one of the following reasons:

RELATIONAL OPERATOR MISSING OR INVALID

The relational operator is missing or is not a valid operator constant.

SYNTAX - POINTER USED WITH VALUE

A keyword with a pointer relational operator cannot specify a value.

OPERATOR CONFLICTS WITH DATATYPE

The relational operator is not valid for the data type associated with the specified keyword.

KEYWORD MISSING OR INVALID

The keyword associated with the RACROUTE parameter is missing or invalid.

WORD USED OUT OF CONTEXT

The keyword is not used properly for RACROUTE specification.

UNKNOWN OPTION

The operand value is not valid for the specified keyword with fixed values.

DUPLICATE OPERAND

The keyword was specified more than once for RACROUTE specification.

CONFLICTS WITH OTHER OPERANDS

The keyword may not be specified because it conflicts with an operand previously specified.

VALUE DOES NOT AGREE WITH DATA TYPE

The value is not valid for the specified data type.

CANNOT ACCEPT STRUCTURED DATA

The data type for the specified keyword is a data structure that cannot be specified by the RACROUTE specifications.

VALUE TOO LARGE FOR DATA TYPE

The specified value is greater than allowed for the keyword data type.

INVALID VALUE LENGTH

The specified value is out of the range allowed for the keyword.

INVALID VALUE MASK

The mask specified on the value is invalid for the keyword.

SYNTAX - VALUE OMITTED

A syntax error check occurred because of a missing value.

RELEASE NOT COMPATIBLE WITH REQUEST

The RACROUTE parameter is not valid for the release of the RACROUTE specification being generated. The release level may have been specified or automatically committed due to release-dependent parameters.

INVALID RELEASE ID SPECIFIED

The specified release number is invalid for the RACROUTE specification.

Action: Correct the SAFDEF RACROUTE parameter in error.

Module: SAFAASDB

CAS2260E ppp aaa AT addr LMOD llll CSECT cccc +oooo jjjj ssss pppp

Reason: Diagnostic information display for an abend. If any of these variable fields are unavailable at the time of the abend, N/A appears as the value.

ppp The component that requested the dump.

aaa The abend completion code.

addr

The address from the PSW at time of abend.

llll The name of the load module that abended.

cccc The CSECT name in the abended load module.

oooo The offset into the load module or the CSECT where the abend occurred. If the CSECT name is N/A, then the offset is in the load module.

jjjj The job name of the abending program.

ssss The job step name of the abending program.

pppp

The procedure step name of the abending program.

Action: Contact CA-Top Secret technical support and provide the message number and diagnostic information.

Module: SAFFETTL

CAS2261I NSI: psw

Reason: This message displays the program status word, in hexadecimal format, of the next sequential instruction after an abend has occurred. *psw* is the current program status word, in hexadecimal format, at the time of the abend.

Module: SAFFEIDF

CAS2262I ILC: ilc INTERRUPT CODE: itc REASON CODE: rsn

Reason: This message displays the instruction length count, interrupt code, and reason code associated with an abend.

ilc The instruction length code from the error PSW

itc The interrupt code associated with the error PSW

rsn The value of register 15 at the time of the abend.

Module: SAFFEIDF

CAS2263I TRANSLATION EXCEPTION ADDRESS: addr

Reason: This message displays the virtual address causing the translation exception displayed in hexadecimal format. *addr* is the virtual address causing the translation

Module: SAFFEIDF

CAS2264I DATA AT FAILING PSW ADDRESS: data

Reason: This message displays the data at the failing PSW address. *data* is the twelve bytes of hexadecimal data at the PSW address.

Module: SAFFEIDF

CAS2265I range rrrrrrrr rrrrrrrr rrrrrrrr rrrrrrrr

Reason: This message displays the contents of the general registers at the time of the abend.

range The register range being displayed

rrrrrrrr The register value at the time of the abend.

Module: SAFFEIDF

CAS2266I ppp DUMP IN PROGRESS

Reason: An SVC dump is in progress for the indicated processor id. *ppp* is the component that requested the dump.

Module: SAFFEDMP

CAS2267I ppp DUMP COMPLETED

Reason: The requested SVC dump successfully completed. *ppp* is the component that requested the dump.

Module: SAFFEDMP

CAS2268I ppp DUMP UNSUCCESSFULLY COMPLETED. R15 = rc

Reason: An error occurred during an SVC dump.

ppp The component that requested the dump

rc The return code from the SDUMP macro:

4 The dump data set was too small to contain the whole dump.

8 The dump data sets are full.

Module: SAFFEDMP

2.3 CAS3 Common Record-Level Protection Routines

CAS3001E SUPPLIED DATA BUFFER EXCEEDS MAXIMUM SIZE

Reason: The input data buffer provided to the RECORD definition processor routine was too large.

Action: Contact CA Technical Support.

CAS3002E DATA IS REQUIRED FOR KEYWORD

Reason: You specified a RECORD definition record keyword that requires data. No data was found.

Action: The RECORD definition record input process terminates. Determine the cause of the error and retry the data entry process.

Module: CRLPRECP

CAS3003E REQUIRED KEYWORD NOT FOUND

Reason: The RECORD definition record input processor was unable to locate the RECNAME keyword. Input processing is terminated.

Action: Check your input statements for correctness and retry the input process.

Module: CRLPRECP

CAS3004E INVALID KEYWORD FOUND

Reason: The RECORD definition record input processor encountered an unknown keyword in the input data. Input processing is terminated.

Action: Check your input data for correctness and retry the input process.

Module: CRLPRECP

CAS3005E CRLPRECP INVOKED FOR ILLEGAL FUNCTION

Reason: The RECORD definition record input processor was invoked to perform an unknown function. Input processing is terminated.

Action: Contact CA Technical Support.

Module: CRLPRECP

CAS3006E CRLPRECP INVOKED FOR INCORRECT RECORD TYPE

Reason: The RECORD definition record input processor was improperly invoked to handle a different type of record. Input processing is terminated.

Action: Contact CA Technical Support.

Module: CRLPRECP

CAS3007E CRLPRECP FUNCTION=INIT, NO SOURCE BUFFER SUPPLIED

Reason: An internal error occurred. Input processing is terminated.

Action: Contact CA Technical Support.

Module: CRLPRECP

CAS3008E CRLPRECP FUNCTION=INIT, NO SOURCE BUFFER LENGTH SUPPLIED

Reason: An internal error occurred. Input processing is terminated.

Action: Contact CA Technical Support.

Module: CRLPRECP

CAS3009E CRLPRECP FUNCTION=PROCESS, NO INPUT BUFFER SUPPLIED

Reason: An internal error occurred. Input processing is terminated.

Action: Contact CA Technical Support.

Module: CRLPRECP

CAS3010E CRLPRECP FUNCTION=PROCESS, NO INPUT BUFFER LENGTH SUPPLIED

Reason: An internal error occurred. Input processing is terminated.

Module: CRLPRECP

Action: Contact CA Technical Support.

CAS3011E CLOSING PARENTHESIS NOT FOUND FOR DATA FIELD

Reason: The RECORD definition record input processor encountered a keyword and data field that did not have a closing parenthesis. Input processing is terminated.

Action: Correct the input data and retry the input process.

Module: CRLPRECP

CAS3012E INVALID CHARACTER IN DATA FIELD

Reason: The RECORD definition record input processor encountered invalid data in a data field. Input processing is terminated.

Action: Correct the input data and retry the input process.

Module: CRLPRECP

CAS3013E CRLPRECP FUNCTION=PROCESS, INIT PROCESSING NOT PERFORMED

Reason: An internal error occurred. Input processing is terminated.

Action: Contact CA Technical Support.

Module: CRLPRECP

CAS3014E DUPLICATE FLDNAME SPECIFICATION

Reason: The RECORD definition record input processor found two or more FLDNAME definitions in the definition of record field. Input processing terminates.

Action: Remove the redundant FLDNAME specification and retry the input process.

Module: CRLPRECP

CAS3015E OPERAND TOO BIG FOR KEYWORD=VALUE

Reason: The RECORD definition record input processor found a data element for a VALUE keyword larger than 44 characters. Input processing terminates.

Action: Retry the input process specifying a VALUE keyword whose length is less than or equal to 44 characters.

Module: CRLPRECP

CAS3016E INVALID VALUE FOR TYPE KEYWORD

Reason: The RECORD definition record input processor encountered an invalid value for the TYPE keyword. Input processing is terminated.

Action: Correct the input data and retry the input process.

Module: CRLPRECP

CAS3017E DUPLICATE TYPE SPECIFICATION

Reason: The RECORD definition record input processor encountered a duplicate TYPE keyword for a definition of a field. Input processing is terminated.

Action: Remove duplicate TYPE specification; retry.

Module: CRLPRECP

CAS3018E DUPLICATE OFFSET SPECIFICATION

Reason: The RECORD definition record input processor found a duplicate OFFSET keyword for a definition of a field. Input processing terminates.

Action: Remove duplicate OFFSET specification; retry.

CAS3019E KEYWORD=OFFSET, INVALID NUMERIC DATA

Reason: The RECORD definition record input processor found too large of a number for the OFFSET keyword in the definition of a field. Input processing terminates.

Action: Ensure that the OFFSET keyword data is in the proper range; retry.

Module: CRLPRECP

CAS3020E KEYWORD=OFFSET, NUMBER OUT OF RANGE

Reason: The RECORD definition record input processor found an invalid number for the OFFSET keyword in the definition of a field. Input processing terminates.

Action: Ensure that the OFFSET keyword data is in the proper range; retry.

Module: CRLPRECP

CAS3021E KEYWORD=OFFSET, NO VALUE FOUND

Reason: The RECORD definition record input processor found an OFFSET keyword without data in the definition of a field. Input processing terminates.

Action: Supply valid data for the OFFSET keyword; retry.

Module: CRLPRECP

CAS3022E DUPLICATE LENGTH SPECIFICATION

Reason: The RECORD definition record input processor found a duplicate LENGTH keyword for a definition of a field.

Action: Remove the duplicate LENGTH specification; retry.

Module: CRLPRECP

CAS3023E KEYWORD=LENGTH, INVALID NUMERIC DATA

Reason: The RECORD definition record input processor found too large of a number for the LENGTH keyword in the definition of a field. Input processing terminates.

Action: Ensure that the LENGTH keyword data is in the proper range; retry.

Module: CRLPRECP

CAS3024E KEYWORD=LENGTH, NUMBER OUT OF RANGE

Reason: The RECORD definition record input processor found an invalid number for the LENGTH keyword in the definition of a field. Input processing terminates.

Action: Ensure that the LENGTH keyword data is in the proper range; retry.

Module: CRLPRECP

CAS3025E KEYWORD=LENGTH, NO VALUE FOUND

Reason: The RECORD definition record input processor found a LENGTH keyword without data in the definition of a field. Input processing terminates.

Action: Supply valid data for the LENGTH keyword; retry.

Module: CRLPRECP

CAS3026E DUPLICATE ROW SPECIFICATION

Reason: The RECORD definition record input processor encountered a duplicate ROW keyword for a definition of a field. Input processing is terminated.

Action: Remove the duplicate ROW specification; retry.

Module: CRLPRECP

CAS3027E KEYWORD=ROW, INVALID NUMERIC DATA

Reason: The RECORD definition record input processor encountered too large of a number for the ROW keyword in the definition of a field. Input processing is terminated.

Action: Ensure that the ROW keyword data is in the proper range; retry.

Module: CRLPRECP

CAS3028E KEYWORD=ROW, NUMBER OUT OF RANGE

Reason: The RECORD definition record input processor encountered an invalid number for the ROW keyword in the definition of a field. Input processing is terminated.

Action: Ensure that the ROW keyword data is in the proper range; retry.

Module: CRLPRECP

CAS3029E KEYWORD=ROW, NO VALUE FOUND

Reason: The RECORD definition record input processor encountered an ROW keyword without data in the definition of a field. Input processing is terminated.

Action: Supply valid data for the ROW keyword and retry the input process.

Module: CRLPRECP

CAS3030E DUPLICATE COL SPECIFICATION

Reason: The RECORD definition record input processor encountered a duplicate COL keyword for a definition of a field. Input processing is terminated.

Action: Remove the duplicate COL specification from the input data and retry.

Module: CRLPRECP

CAS3031E KEYWORD=COL, INVALID NUMERIC DATA

Reason: The RECORD definition record input processor encountered too large of a number for the COL keyword in the definition of a field. Input processing is terminated.

Action: Ensure that the data for the COL keyword is in the proper range and retry the input process.

Module: CRLPRECP

CAS3032E KEYWORD=COL, NUMBER OUT OF RANGE

Reason: The RECORD definition record input processor encountered an invalid number for the COL keyword in the definition of a field. Input processing is terminated.

Action: Ensure that the data for the COL keyword is in the proper range and retry the input process.

Module: CRLPRECP

CAS3033E KEYWORD=COL, NO VALUE FOUND

Reason: The RECORD definition record input processor encountered a COL keyword without data in the definition of a field. Input processing is terminated.

Action: Supply valid data for the COL keyword and retry the input process.

Module: CRLPRECP

CAS3034E FLDNAME SPECIFICATION REQUIRED

Reason: The RECORD definition record input processor did not find a FLDNAME specification for an input line of a field definition. Input processing is terminated.

Action: Each input statement describing a record field must have an associated FLDNAME definition. Supply a valid FLDNAME definition and retry the input process.

Module: CRLPRECP

CAS3035E LENGTH MUTUALLY EXCLUSIVE WITH VALUE

Reason: The RECORD definition record input processor encountered both a LENGTH definition and VALUE DEFINITION in the input for a field definition. Input processing is terminated.

Action: LENGTH and VALUE are mutually exclusive. Remove the redundant keyword and retry the input process.

Module: CRLPRECP

CAS3036E ROW MUTUALLY EXCLUSIVE WITH VALUE

Reason: The RECORD definition record input processor encountered both a ROW and VALUE definition in the input for a field definition. Input processing is terminated.

Action: ROW and VALUE are mutually exclusive. Remove the redundant keyword and retry the input process.

Module: CRLPRECP

CAS3037E COL MUTUALLY EXCLUSIVE WITH VALUE

Reason: The RECORD definition record input processor encountered both a COL and VALUE definition in the input for a field definition. Input processing is terminated.

Action: COL and VALUE are mutually exclusive. Remove the redundant keyword and retry the input process.

Module: CRLPRECP

CAS3038E OFFSET MUTUALLY EXCLUSIVE WITH VALUE

Reason: The RECORD definition record input processor encountered both an OFFSET and a VALUE definition in the input for a field definition. Input processing is terminated.

Action: OFFSET and VALUE are mutually exclusive. Remove the redundant keyword and retry the input process.

Module: CRLPRECP

CAS3039E TYPE SPECIFICATION REQUIRED

Reason: The RECORD definition record input processor did not encounter a TYPE specification for a record field definition. This is required. Input processing is terminated.

Action: Supply a valid TYPE definition and retry the input process.

Module: CRLPRECP

CAS3040E ROW MUTUALLY EXCLUSIVE WITH OFFSET

Reason: The RECORD definition record input processor encountered both a ROW and OFFSET definition in the input for a field definition. Input processing is terminated.

Action: ROW and OFFSET are mutually exclusive. Remove the redundant keyword and retry the input process.

Module: CRLPRECP

CAS3041E COL MUTUALLY EXCLUSIVE WITH OFFSET

Reason: The RECORD definition record input processor encountered both a COL and OFFSET definition in the input for a field definition. Input processing is terminated.

Action: COL and OFFSET are mutually exclusive. Remove the redundant keyword and retry the input process.

Module: CRLPRECP

CAS3042E ROW/COL, OFFSET OR VALUE MUST BE SPECIFIED

Reason: The RECORD definition record input processor requires that you specify one of the ROW/COL, OFFSET or VALUE keywords for each record field definition. None was supplied. Input processing is terminated.

Action: Supply the appropriate keyword and retry the input process.

Module: CRLPRECP

CAS3043E ROW REQUIRES COL

Reason: The RECORD definition record input processor found a ROW keyword with no COL keyword. Input processing terminates.

Action: Supply a COL definition; retry.

Module: CRLPRECP

CAS3044E MAXIMUM NUMBER OF INPUT LINES, TERMINATING

Reason: An internal error occurred. Input processing is terminated.

Action: Contact CA Technical Support.

Module: CRLPRECP

CAS3045E CRLPRECP FUNCTION=TERM, INIT PROCESSING NOT PERFORMED

Reason: An internal error occurred. Input processing is terminated.

Action: Contact CA Technical Support.

Module: CRLPRECP

CAS3046E CRLPRECP FUNCTION=TERM, NO PROCESS REQUESTS PERFORMED

Reason: An internal error occurred. Input processing is terminated.

Action: Contact CA Technical Support.

Module: CRLPRECP

CAS3047E CRLPRECP FUNCTION=TERM, SECURITY HEADER LENGTH IS ZERO

Reason: An internal error occurred. Input processing is terminated.

Action: Contact CA Technical Support.

Module: CRLPRECP

CAS3048E CRLPRECP FUNCTION=TERM, SECURITY HEADER LENGTH IS TOO BIG

Reason: An internal error occurred. Input processing is terminated.

Action: Contact CA Technical Support.

Module: CRLPRECP

CAS3049E CRLPRECP FUNCTION=TERM, OBJECT BUFFER ADDRESS IS REQUIRED

Reason: An internal error occurred. Input processing is terminated.

Action: Contact CA Technical Support.

Module: CRLPRECP

CAS3050E CRLPRECP FUNCTION=TERM, OBJECT BUFFER LENGTH IS REQUIRED OR INVALID

Reason: An internal error occurred. Input processing is terminated.

Action: Contact CA Technical Support.

Module: CRLPRECP

CAS3051E CRLPRECP FUNCTION=TERM, OBJECT BUFFER IS TOO SMALL

Reason: An internal error occurred. Input processing is terminated.

Action: Contact CA Technical Support.

Module: CRLPRECP

CAS3052E DUPLICATE FIELD NAMES FOUND

Reason: The RECORD definition record input processor found the FLDNAME names of two or more record fields identical. Input processing terminates.

Action: All field names must be unique. Remove the duplicate field definition or assign a unique name to the duplicate field; retry.

Module: CRLPRECP

CAS3053E RECNAME MUST BE 24 CHARACTERS OR LESS IN LENGTH

Reason: The RECORD definition record input processor found the RECNAME name longer than the allowable 24 characters. Input processing terminates.

Action: Supply a valid RECNAME name; retry.

CAS3054E NO CLOSING PARENTHESIS FOUND FOR KEYWORD=RECNAME

Reason: The RECORD definition record input processor determined that the RECNAME name specification did not end with a closing parenthesis. Input processing is terminated.

Action: Correct the input data to supply valid RECNAME data and retry the input process.

Module: CRLPRECP

CAS3055E DUPLICATE VALUE SPECIFICATION

Reason: The RECORD definition record input processor encountered a duplicate VALUE keyword for a definition of a field. Input processing is terminated.

Action: Remove the duplicate VALUE specification from the input data and retry the input process.

Module: CRLPRECP

CAS3056E INVALID SKIP VALUE SPECIFICATION

Reason: The RECORD definition record input processor encountered a SKIP keyword without data. Input processing is terminated.

Action: Correct the input data and retry the input process.

Module: CRLPRECP

CAS3057E INVALID VALUE SPECIFICATION

Reason: The RECORD definition record input processor encountered a VALUE keyword without data. Input processing is terminated.

Action: Correct the input data and retry the input process.

Module: CRLPRECP

CAS3058E INVALID FLDNAME VALUE SPECIFICATION

Reason: The RECORD definition record input processor encountered a FLDNAME keyword without data. Input processing is terminated.

Action: Correct the input data and retry the input process.

Module: CRLPRECP

CAS3059E INVALID TYPE VALUE SPECIFICATION

Reason: The RECORD definition record input processor found a TYPE keyword without data. Input processing terminates.

Action: Correct the input data and retry the input process.

Module: CRLPRECP

CAS3060E SUPPLIED FLDNAME IS TOO BIG

Reason: The RECORD definition record input processor found a FLDNAME name longer than 24 characters. Input processing terminates.

Action: Supply a valid FLDNAME name and retry the input process.

Module: CRLPRECP

CAS3101E CRLPRECL INVOKED FOR ILLEGAL FUNCTION

Reason: An internal error occurred. Input processing is terminated.

Action: Contact CA Technical Support.

Module: CRLPRECP

CAS3102E CRLPRECL INVOKED FOR UNSUPPORTED RECORD TYPE

Reason: An internal error occurred. Input processing is terminated.

Action: Contact CA Technical Support.

Module: CRLPRECP

CAS3103E MISSING OR INVALID TYPE DEFINED IN RECORD

Reason: An internal error occurred. Input processing is terminated.

Action: Contact CA Technical Support.

Module: CRLPRECP

CAS3126E SUPPLIED DATA BUFFER EXCEEDS MAXIMUM SIZE

Reason: An internal error occurred. Input processing is terminated.

Action: Contact CA Technical Support.

Module: CRLPRECP

CAS3127E DATA IS REQUIRED FOR KEYWORD

Reason: This SELECT definition keyword requires data; no data was found.

Action: SELECT input processing terminates; correct error and retry.

Module: CRLPRECP

CAS3128E REQUIRED KEYWORD NOT FOUND

Reason: SELECT definition processor cannot locate the SELECT keyword. Input processing is terminated.

Action: Check your input statements for correctness and retry the input process.

Module: CRLPRECP

CAS3129E INVALID KEYWORD FOUND

Reason: The SELECT definition input processor encountered an unknown keyword in the input data. Input processing is terminated.

Action: Check your input data for correctness and retry the input process.

Module: CRLPEXPP

CAS3130E CRLPEXPP INVOKED FOR ILLEGAL FUNCTION

Reason: An internal error occurred. Input processing is terminated.

Action: Contact CA Technical Support.

Module: CRLPRECP

CAS3131E CRLPEXPP INVOKED FOR INCORRECT RECORD TYPE

Reason: An internal error occurred. Input processing is terminated.

Action: Contact CA Technical Support.

Module: CRLPEXPP

CAS3132E CRLPEXPP FUNCTION=INIT, NO SOURCE BUFFERS SUPPLIED

Reason: An internal error occurred. Input processing is terminated.

Action: Contact CA Technical Support.

Module: CRLPEXPP

CAS3133E CRLPEXPP FUNCTION=INIT, NO SOURCE BUFFER LENGTH SUPPLIED

Reason: An internal error occurred. Input processing is terminated.

Action: Contact CA Technical Support.

Module: CRLPEXPP

CAS3134E CRLPEXPP FUNCTION=PROCESS, NO INPUT BUFFER SUPPLIED

Reason: An internal error occurred. Input processing is terminated.

Action: Contact CA Technical Support.

Module: CRLPEXPP

CAS3135E CRLPEXPP FUNCTION=PROCESS, NO INPUT BUFFER LENGTH SUPPLIED

Reason: An internal error occurred. Input processing is terminated.

Action: Contact CA Technical Support.

Module: CRLPEXPP

CAS3136E CRLPEXPP FUNCTION=PROCESS, INIT PROCESSING NOT PERFORMED

Reason: An internal error occurred. Input processing is terminated.

Action: Contact CA Technical Support.

Module: CRLPEXPP

CAS3137E MAXIMUM NUMBER OF INPUT LINES, TERMINATING

Reason: An internal error occurred. Input processing is terminated.

Action: Contact CA Technical Support.

Module: CRLPEXPP

CAS3138E CRLPEXPP FUNCTION=TERM, INIT PROCESSING NOT PERFORMED

Reason: An internal error occurred. Input processing is terminated.

Action: Contact CA Technical Support.

Module: CRLPEXPP

CAS3139E CRLPEXPP FUNCTION=TERM, NO PROCESS REQUEST PERFORMED

Reason: An internal error occurred. Input processing is terminated.

Action: Contact CA Technical Support.

Module: CRLPEXPP

CAS3140E CRLPEXPP FUNCTION=TERM, SECURITY HEADER LENGTH IS ZERO

Reason: An internal error occurred. Input processing is terminated.

Action: Contact CA Technical Support.

Module: CRLPEXPP

CAS3141E CRLPEXPP FUNCTION=TERM, SECURITY HEADER LENGTH IS TOO BIG

Reason: An internal error occurred. Input processing is terminated.

Action: Contact CA Technical Support.

Module: CRLPEXPP

CAS3142E CRLPEXPP FUNCTION=TERM, OBJECT BUFFER ADDRESS IS REQUIRED

Reason: An internal error occurred. Input processing is terminated.

Action: Contact CA Technical Support.

Module: CRLPEXPP

CAS3143E CRLPEXPP FUNCTION=TERM, OBJECT BUFFER LENGTH IS REQUIRED OR INVALID

Reason: An internal error occurred. Input processing is terminated.

Action: Contact CA Technical Support.

Module: CRLPEXPP

CAS3144E CRLPEXPP FUNCTION=TERM, OBJECT BUFFER IS TOO SMALL

Reason: An internal error occurred. Input processing is terminated.

Action: Contact CA Technical Support.

Module: CRLPEXPP

CAS3145E NO INPUT DATA SUPPLIED

Reason: The SELECT definition input processor encountered no input data. Input processing is terminated.

Action: Supply valid input data and retry the input process.

Module: CRLPEXPP

CAS3146E NO IF STATEMENT FOUND

Reason: The SELECT definition input processor encountered no input IF statement. Input processing is terminated.

Action: Supply valid input data and retry the input process.

CAS3201E CRLPEXPL INVOKED FOR ILLEGAL FUNCTION

Reason: An internal error occurred. Input processing is terminated.

Action: Contact CA Technical Support.

Module: CRLPEXPL

CAS3202E CRLPEXPL INVOKED FOR UNSUPPORTED RECORD TYPE

Reason: An internal error occurred. Input processing is terminated.

Action: Contact CA Technical Support.

Module: CRLPEXPL

CAS3203E MISSING OR INVALID LOGICAL OPERATOR FOR SELECT RECORD

Reason: An internal error occurred. Input processing is terminated.

Action: Contact CA Technical Support.

Module: CRLPEXPL

CAS3204E NO FSDTE ENTRIES EXIST FOR SELECT RECORD

Reason: An internal error occurred. Input processing is terminated.

Action: Contact CA Technical Support.

Module: CRLPEXPL

CAS3245E INVALID NESTING OF PARENTHESIS

Reason:

1. If any simple expressions are enclosed in parentheses, then the entire IF expression must be enclosed in parentheses. For instance,
SELDATA('IF (KEY GET 5) AND (KEY LE 1000)')
is invalid, but
SELDATA('IF ((KEY GET 5) AND (KEY LE 1000))')
is valid for this reason.
2. The number of left and right parentheses are unbalanced.

Action: Contact CA Technical Support.

CAS3252E TOO MANY OPERANDS

Reason: SELECT definition input processor found more than the maximum 255 operands. Input processing is terminated.

Action: Retry; supply fewer operands. Break security controls into smaller components if necessary.

Module: CRLPEXPL

CAS3253E EXPECTED OPERATOR NOT FOUND

Reason: The SELECT definition input processor was expecting a logical operator but did not encounter one. Input processing is terminated.

Action: Check your input data for correct syntax and retry the input process.

Module: CRLPEPOL

CAS3254E INVALID NESTING OF PARENTHESIS

Reason: SELECT definition input processor found an illegal nesting of parenthesis. Input processing is terminated.

Action: Check for odd number of parentheses. Correct and retry.

Module: CRLPEPOL

CAS3255E EXPECTED OPERATOR/SYMBOL NOT FOUND

Reason: The SELECT definition input processor expected an operator or symbol but did not encounter either. Input processing is terminated.

Action: Check your input data for correct syntax and retry the input process.

Module: CRLPEPOL

CAS3301E OPERATOR EVALUATION ROUTINE UNDEFINED

Reason: An internal error occurred. Input processing is terminated.

Action: Contact CA Technical Support.

Module: CRLPERSL

CAS3302E INVALID CONSTANT TYPE

Reason: The SELECT definition input processor encountered an invalid constant or literal specification for a right hand side (RHS) value. Input processing is terminated.

Action: Correct the input data and retry the input process.

Module: CRLPERSL

**CAS3303E INVALID NUMERIC CONSTANT - EXCEEDS
MINIMUM/MAXIMUM RANGE**

Reason: The SELECT definition input processor encountered an invalid binary constant value that did not fall into the proper range of values for such operands. Input processing is terminated.

Action: Correct the input data and retry the input process.

Module: CRLPERSL

CAS3304E INVALID DECIMAL CONSTANT

Reason: The SELECT definition input processor encountered an invalid binary constant value that did not contain valid numeric digits. Input processing is terminated.

Action: Correct the input data and retry the input process.

Module: CRLPERSL

CAS3305E INVALID HEX CONSTANT

Reason: The SELECT definition input processor encountered an invalid hex constant value that did not contain valid hex digits. Input processing is terminated.

Action: Correct the input data and retry the input process.

Module: CRLPERSL

CAS3306E ODD LENGTH HEX CONSTANT

Reason: The SELECT definition input processor encountered an invalid hex constant value that did not contain an even number of hex digits. Input processing is terminated.

Action: Correct the input data and retry the input process.

Module: CRLPERSL

CAS3307E INVALID OPERATOR/OPERAND TYPES

Reason: An internal error occurred. Input processing is terminated.

Action: Contact CA Technical Support.

Module: CRLPERSL

CAS3308E INTERNAL ERROR - INVALID TYPE

Reason: An internal error occurred. Input processing is terminated.

Action: Contact CA Technical Support.

Module: CRLPERSL

CAS3309E INTERNAL ERROR - INVALID PSCANX

Reason: An internal error occurred. Input processing is terminated.

Action: Contact CA Technical Support.

Module: CRLPERSL

CAS3310E INTERNAL ERROR - INVALID OPERATOR TYPE

Reason: An internal error occurred. Input processing is terminated.

Action: Contact CA Technical Support.

Module: CRLPERSL

CAS3352E INTERNAL ERROR, INCORRECT FSDT NUMBER

Reason: An internal error occurred. Input processing is terminated.

Action: Contact CA Technical Support.

Module: CRLPEFDT

CAS3363E INTERNAL ERROR IN PSCANX STACK PROCESSING

Reason: An internal error occurred. Input processing is terminated.

Action: Contact CA Technical Support.

Module: CRLPEFDT

CAS3364E INTERNAL ERROR ATTEMPTING TO POP PSCANX STACK

Reason: An internal error occurred. Input processing is terminated.

Action: Contact CA Technical Support.

Module: CRLPEFDT

CAS3401E ILLEGAL OR INVALID SELECT RECORD

Reason: An internal error occurred. Input processing is terminated.

Action: Contact CA Technical Support.

Module: CRLPEFDT

CAS3402E ERROR OCCURRED WHILE PERFORMING EVALUATION PROCESSING

Reason: An internal error occurred. Input processing is terminated.

Action: Contact CA Technical Support.

Module: CRLPFLDP

CAS3403E SELECT LEFT HAND SIDE (LHS) FIELD NOT FOUND

Reason: During evaluation processing, the logical comparison routine could not locate the record field defined as one of the left hand side values of the SELECT record used. The cause might be something simple such as an error in defining the record field definitions in the appropriate RECORD definition record.

Action: Evaluation processing terminates. The host security system denied the access attempt. Review the host security system logging/auditing mechanisms for information on the RECORD definition record and SELECT record used during the evaluation. If the RECORD definition record has the field properly defined, ensure that your site properly made these definitions available for RLP processing.

Module: CRLPFLDP

CAS3405E ERROR EXTRACTING FILE DATA

Reason: An internal error occurred. Input processing is terminated.

Action: Contact CA Technical Support.

Module: CRLPFLDP

CAS3406E CRLPFILE FILE EXTRACT ROUTINE CANNOT BE LOCATED

Reason: During evaluation of a logical expression the File extract processing routine could not be located during evaluation of a logical expression.

Action: Evaluation processing is terminates. The host security system denied the access attempt. Have site management review their installation of the host security system to verify that the record level protection (RLP) component was properly installed and is available for processing.

Module: CRLPFLDP

CAS3407E CRLPSCRN SCREEN EXTRACT ROUTINE CANNOT BE LOCATED

Reason: Screen extract processing routine could not be located during evaluation of a logical expression.

Action: Evaluation processing is terminated. The host security system denied the access attempt. Have site management review their install of the host security system to verify that the record level protection (RLP) component was properly installed and is available for processing.

Module: CRLPFLDP

CAS3408E ERROR EXTRACTING SCREEN DATA

Reason: An internal error occurred. Input processing is terminated.

Action: Contact CA Technical Support.

Module: CRLPFLDP

CAS3409E CRLPCOMP LOGICAL COMPARATOR ROUTINE CANNOT BE LOCATED

Reason: Logical comparison routine was not located during evaluation of a logical expression.

Action: Evaluation processing is terminated. The host security system denied the access attempt. Have site management review their install of the host security system to verify that the record level protection (RLP) component was properly installed and is available for processing.

Module: CRLPFLDP

CAS3410E ERROR IN LOGICAL COMPARISON PROCESSING

Reason: An internal error occurred. Input processing is terminated.

Action: Contact CA Technical Support.

CAS3411E CRLPMULT MULTIPLE EVALUATION ROUTINE CANNOT BE LOCATED

Reason: Multiple comparison processing routine could not be located during evaluation of a logical expression.

Action: Evaluation processing is terminated. The host security system denied the access attempt. Have management review their install of the host security system to verify that the record level protection (RLP) component was properly installed and is available for processing.

Module: CRLPFLDP

CAS3412E ERROR IN MULTIPLE EVALUATION PROCESSING

Reason: An internal error occurred. Input processing is terminated.

Action: Contact CA Technical Support.

Module: CRLPFLDP

CAS3413E SELECT RIGHT HAND SIDE (RHS) FIELD NOT FOUND

Reason: During evaluation processing, the logical comparison routine could not locate the constant value defined as one of the right hand side values of the SELECT record used. The cause might be something simple such as an error in defining the record field definitions in the appropriate RECORD or SELECT definition record.

Action: Evaluation processing terminated. The host security system denied the access attempt. Review the host security system logging and auditing mechanisms for information on the RECORD definition record and SELECT record used during the evaluation. If the RECORD definition record has the field properly defined, ensure that your site properly made these definitions available for RLP processing.

Module: CRLPFLDP

CAS3414E SELECT LEFT HAND SIDE (LHS) SYMBOLIC FIELD CANNOT BE A LITERAL

Reason: An internal error occurred. Input processing is terminated.

Action: Contact CA Technical Support.

Module: CRLPFLDP

**CAS3415E SELECT RIGHT HAND SIDE (RHS) SYMBOLIC FIELD CANNOT BE
A SCREEN FIELD**

Reason: During evaluation processing the logical comparison routine determined that a symbolic right hand side definition naming a screen record field instead of a VALUE definition was specified. The comparison is illegal and disallowed.

Action: Evaluation processing is terminated. The host security system denied the access attempt. Review the host security system logging and auditing mechanisms for information on the RECORD definition record and SELECT record used in the evaluation process and use this information to correct the erroneous SELECT or RECORD definition.

Module: CRLPFLDP

**CAS3416E SELECT RIGHT HAND SIDE (RHS) SYMBOLIC FIELD CANNOT BE
A RECORD FIELD**

Reason: During evaluation processing the logical comparison routine determined that a symbolic right hand side definition naming a file record field instead of a VALUE definition was specified. The comparison is illegal and disallowed.

Action: Evaluation processing is terminated. The host security system denied the access attempt. Review the host security system logging and auditing mechanisms for information on the RECORD definition record and SELECT record used in the evaluation process and use this information to correct the erroneous SELECT or RECORD definition.

Module: CRLPFLDP

**CAS3417E SELECT LEFT HAND SIDE (LHS) EXPLICIT ROW/COL SPECIFI-
CATION IS INVALID**

Reason: An internal error occurred. Input processing is terminated.

Action: Contact CA Technical Support.

Module: CRLPFLDP

**CAS3418E SELECT LEFT HAND SIDE (LHS) EXPLICIT ROW SPECIFICATION
IS ZERO**

Reason: An internal error occurred. Input processing is terminated.

Action: Contact CA Technical Support.

Module: CRLPFLDP

CAS3419E SELECT LEFT HAND SIDE (LHS) EXPLICIT COL SPECIFICATION IS ZERO

Reason: An internal error occurred. Input processing is terminated.

Action: Contact CA Technical Support.

Module: CRLPFLDP

CAS3422E OFFSET FOR MASK IS LARGER THAN BUFFER SIZE

Reason: A field defined in the MASKREC contains an offset value that is outside the range of the data record.

Action: Check the MASKREC definition and review the value for the offset, and compare it to the data record's length.

CAS3423E MASK NOT WITHIN RECORD BUFFER

Reason: A field defined in the MASKREC has an offset that begins prior to the end of the physical record length but overlaps past the data record size.

Action: Check the MASKREC definition and review the value for the offset, and compare it to the data record's length.

CAS3451E DATA BUFFER FOR EVALUATION IS TOO BIG

Reason: During evaluation of an expression involving file record fields, the logical comparison routine determined that the size of the input file record exceeded the maximum size of 65535 bytes.

Action: Evaluation processing terminates. The host security system denied the access attempt. Review host security system logging and auditing mechanisms for information on the file for which access was attempted. Review use of record level protection controls with your site personnel to determine validity of this condition.

Module: CRLPFILE

CAS3452E OFFSET FOR FIELD IS ZERO

Reason: An internal error occurred. Input processing is terminated.

Action: Contact CA Technical Support.

Module: CRLPFILE

CAS3453E OFFSET FOR FIELD IS LARGER THAN BUFFER SIZE

Reason: During evaluation of an expression involving file record fields, the logical comparison routine determined that the offset of a file record field was outside the range of the supplied file record.

Action: Evaluation processing terminates. The host security system denied the access attempt. Review host security system logging and auditing mechanisms for information on the file for which access was attempted. Review use of record level protection controls with your site personnel to determine validity of this condition.

Module: CRLPFILE

CAS3454E FIELD NOT WITHIN RECORD BUFFER

Reason: During evaluation of an expression involving file record fields, the logical comparison routine determined that a file record field started in the supplied file record, but ended outside of the supplied buffer.

Action: Evaluation processing terminates. The host security system denied the access attempt. Review host security system logging and auditing mechanisms for information on the file for which access was attempted. Review use of record level protection controls with your site personnel to determine validity of this condition.

Module: CRLPFILE

CAS3476E DATA BUFFER FOR EVALUATION IS TOO BIG

Reason: During evaluation of an expression involving screen record fields, the logical comparison routine determined that the size of the input file record exceeded the maximum size of 65535 bytes.

Action: Evaluation processing terminates. The host security system denied the access attempt. Review host security system logging and auditing mechanisms for information on the file for which access was attempted. Review use of record level protection controls with your site personnel to determine validity of this condition.

CAS3477E OFFSET FOR FIELD IS ZERO

Reason: An internal error occurred. Input processing is terminated.

Action: Contact CA Technical Support.

Module: CRLPSCRN

CAS3478E OFFSET FOR FIELD IS LARGER THAN BUFFER SIZE

Reason: During evaluation of an expression involving screen record fields, the logical comparison routine determined that the offset of a screen record field was outside the range of the supplied screen record.

Action: Evaluation processing terminates. The host security system denied the access attempt. Review host security system logging and auditing mechanisms for information on the file for which access was attempted. Review use of record level protection controls with your site personnel to determine validity of this condition.

Module: CRLPSCRN

CAS3479E FIELD NOT WITHIN RECORD BUFFER

Reason: During evaluation of an expression involving screen record fields, the logical comparison routine determined that a screen record field started in the supplied screen record, but ended outside of the supplied buffer.

Action: Evaluation processing terminates. The host security system denied the access attempt. Review host security system logging and auditing mechanisms for information

on the file for which access was attempted. Review use of record level protection controls with your site personnel to determine validity of this condition.

Module: CRLPSCRN

CAS3480E COLUMN SPECIFIED WITHOUT ROW

Reason: An internal error occurred. Input processing is terminated.

Action: Contact CA Technical Support.

CAS3481E ROW SPECIFIED WITHOUT COLUMN

Reason: An internal error occurred. Input processing is terminated.

Action: Contact CA Technical Support.

Module: CRLPSCRN

CAS3482E ROW NUMBER USED EXCEEDS TERMINAL SIZE

Reason: The logical comparison routine attempted to extract data from an input screen buffer during evaluation of an expression. The calling environment supplied the terminals with physical characteristics and the input screen buffer. The ROW number used in the evaluation processing exceeded the physical capability of the input terminal.

Action: Evaluation processing terminated. The host security system denied the access attempt. Review your site's use of record level protection controls for screen input protection. Verify that these controls match the physical capabilities of the terminals.

Module: CRLPRECP

CAS3483E COL NUMBER USED EXCEEDS TERMINAL SIZE

Reason: The logical comparison routine attempted to extract data from an input screen buffer during evaluation of an expression. The calling environment supplied the terminals with physical characteristics and the input screen buffer. The COL number used in the evaluation processing exceeded the physical capability of the input terminal.

Action: Evaluation processing is terminated. The host security system denied the access attempt. Review your site's use of record level protection controls for screen input protection. Verify that these controls match the physical capabilities of the terminals.

Module: CRLPRECP

CAS3484E DATA AT ROW/COL VECTOR NOT FOUND

Reason: The logical comparison routine attempted to extract data from an input screen buffer at a specific screen location during evaluation of an expression. The screen extractor could not locate data for the specified vector.

Action: Evaluation processing is terminated. The host security system denied the access attempt. Review your site's use of record level protection controls for screen input protection. Verify that these controls match the physical capabilities of the terminals.

Module: CRLPRECP

CAS3486E MISSING OR ILLEGAL AID VALUE SUPPLIED

Reason: An internal error occurred. Input processing is terminated.

Action: Contact CA Technical Support.

Module: CRLPSCRN

CAS3501E ILLEGAL LHS DATA TYPE

Reason: An internal error occurred. Input processing is terminated.

Action: Contact CA Technical Support.

Module: CRLPCOMP

CAS3502E ILLEGAL LOGICAL OPERATOR IN FSDTE

Reason: An internal error occurred. Input processing is terminated.

Action: Contact CA Technical Support.

Module: CRLPCOMP

CAS3503E ERROR WHILE PERFORMING COMPARISON PROCESSING

Reason: An internal error occurred. Input processing is terminated.

Action: Contact CA Technical Support.

CAS3504E MISMATCHED LENGTHS FOR HEX COMPARISON

Reason: During evaluation of an expression that involved two hex fields, the logical comparator routine determined that the length values for the LHS and RHS fields was not equal. When comparing a hex field to a hex constant or literal, both lengths must match.

Action: Evaluation processing is terminated. The host security system denied the access. Review the host security system's logging and auditing mechanisms for assistance in finding the mismatched comparison.

Module: CRLPCOMP

CAS3508E ILLEGAL RHS DATA TYPE

Reason: An internal error occurred. Input processing is terminated.

Action: Contact CA Technical Support.

Module: CRLPCOMP

CAS3526E ILLEGAL LOGICAL OPERATOR FOUND IN FSDTE

Reason: An internal error occurred. Input processing is terminated.

Action: Contact CA Technical Support.

Module: CRLPMULT

CAS3551E INVALID QUOTED STRING

Reason: The SELECT definition input processor encountered an invalid quoted string that did not end with a closing quote. Input processing is terminated.

Action: Correct the input data and retry the input process.

Module: CRLPESCN

Chapter 3. Codes

3.1 Detailed Reason Codes

Detailed reason codes (abbreviated DRC) appear in CA-Top Secret messages, TSSUTIL, and Diagnostic Traces. Each code represents a detailed explanation of the cause of a violation. This section of the *Messages and Codes Guide* is designed to explain the following:

- the detailed reason codes (in decimal and hexadecimal)
- the violation's corresponding message id
- the error message
- a corrective action.

3.1.1 Reserved DRCs

The following DRC hexadecimal codes are reserved for internal error conditions:

- 29, 2B
- 2D through 38
- 3A through 45
- 4A, 4B

Reason:

An internal error condition was detected during security environment create or update processing.

Action:

Report the error to CA Technical Support for analysis. Retain a detailed log of system and security events surrounding the error in the event that additional diagnostic information is required.

3.1.2 Conventions

- The detailed reason codes are listed in **decimal** order.
- The hexadecimal number is in parenthesis following the decimal number.
- The applicable CA-Top Secret user messages.

Here is a sample entry:

001 (01) 7141 Use of ACID suspended.

001 is the decimal code number
(01) is the hexadecimal code number
7141 is the violation message

- Each code is followed by a reason and, if appropriate, a user action for correcting the situation.

3.1.3 Detailed Reason Codes

001 (01) 7141 Use of ACID suspended

Reason: Check VTHRESH and PTHRESH control options for violation thresholds that result in automatic suspension of users. The SUSPEND control option may also have been issued by the console operator.

Action: TSS REMOVE(acid) SUSPEND

002 (02) 7175 Initiation failed by site security exit

Reason: Your site security exit (TSSINSTX) determined that it was not valid for your job or session to initiate. Exit may have issued a message.

Action: Determine the reason for the violation and correct the job.

003 (03) 7144 ACID not supplied on jobcard

Reason: CA-Top Secret could not derive an ACID for your batch job or STC.

Action: Code USER= on the jobcard. Submit the job from a defined or authorized ACID. A default ACID could also be set up for the BATCH facility. The JOBACID control option can also be set to automatically generate the USER JOB operand.

004 (04) 7182 Facility deactivated by Administrator

Reason: Administrator issued FACILITY(fac=INACTIVE) control option.

Action: F TSS,FACILITY(fac=ACTIVE)

005 (05) 7140 ACID expired

Reason: Authority to use ACID has lapsed.

Action: TSS REMOVE(acid) FOR(1)

006 (06) 7161 Access to facility not authorized

Reason: ACID does not have authority to use the accessed facility.

Action: TSS ADD(acid) FACILITY(facility) will explicitly authorize acid to facility.

007 (07) 7102 Password missing

Reason: ACID requires a password but it was not supplied.

Action: Code PASSWORD= on jobcard; supply password with logon; supply password after STC prompt; submit job from defined or authorized ACID.

008 (08) 7121 Password supplied with LOGON

Reason: Via TSO (not TSO/E) logon, user entered "LOGON userid/password"

Action: LOGON with userid only. Wait for CA-Top Secret to prompt for your password. To allow a password with LOGON: F TSS,FAC(TSO=NOPROMPT)

009 (09) 7101 Password incorrect

Reason: The password supplied for the ACID is not correct.

Action: User correct password. If using multiple TSO password option, remember to use UADS password.

010 (0A) 7110 Password expired and new password missing

Reason: The current password for the ACID has expired and is no longer valid.

Action: Specify the new password according to the facility entry method.

011 (0B) 7111 New password invalid.

Reason: Supplied password does not follow the rules set via the NEWPW control option, is a restricted password, or the site exit has ruled it invalid.

Action: Examine message TSS7111E for the specific reason. Change NEWPW control option.

012 (0C) 7181 Security inactive - end of day

Reason: TSS terminated with "Z EOD" option. Normally, this requires an IPL.

Action: TSS,RESETEOD or re-IPL

013 (0D) 7130 Operator ID card required for logon

Reason: The ACID has the OID attribute.

Action: LOGON userid OID; then insert OID card when prompted.

014 (0E) 7131 Operator ID card invalid

Reason: Using incorrect OID

Action: May have to re-record OID by TSS REPLACE(acid) OID

015 (0F) 7251 New password reverify failed

Reason: User incorrectly entered a password in response to a reverify request.

Action: No action required.

016 (10) 7191 Cancellation due to excessive violations

Reason: VTHRESH control option action is CANCEL.

Action: Check/change the VTHRESH control option.

019 (13) 7192 Terminal locked up due to excessive violations

Reason: User has caused too many violations and the terminal has become permanently locked. The user's ACID may also have been suspended.

Action: Only SIGNOFF or LOGOFF is accepted. TSS REMOVE(acid) SUSPEND may also be required.

020 (14) 7172 Userid already in use elsewhere

Reason: User is attempting to sign on twice in the same online region. Ability to do so is governed by: FACILITY(fac=SIGN(M)) or SIGN(S)

Action: Check/change FACILITY(facility=SIGN(?)) or SIGN(?) control option.

021 (15) 7174 Division, Department, or Profile cannot be used

Reason: Attempt to log on or run job using a Profile, Department, or Division ACID.

Action: Use and ACID defined as TYPE(USER | DCA | VCA | SCA) for system entry.

022 (16) 7170 Protected POWER reader or remote not authorized

Reason: Job was submitted from RJE reader that is implicitly or explicitly protected, or ACID has ACTION(DENY).

Action: TSS PERMIT(acid) TERMINAL(reader) explicitly authorizes acid to reader.

023 (17) 7180 Security inactive

Reason: DOWN option specifies FAIL.

Action: Check the status of CA-Top Secret and DOWN control option.

024 (18) 7142 ACID temporarily suspended

Reason: Administrator has temporarily suspended the ACID.

Action: TSS REMOVE(acid) ASUSPEND FOR (0)

025 (19) 7173 ACID not eligible for automatic terminal signon

Reason: User attempted to perform automatic signon based upon terminal ID, and found that the ACID for the terminal had the NOATS attribute.

Action: Sign on by specifying a valid ACID name and password.

026 (1A) 7171 Use of terminal or reader source not authorized

Reason: ACID has SOURCE restrictions and this reader or terminal is not in the list.

Action: TSS ADD/REMOVE(acid) SOURCE(reader)

027 (1B) 7120 Too many incorrect password attempts

Reason: Too many attempts were made at guessing the ACID's password.

Action: Check/change PTHRESH control option. May have to REMOVE the SUSPEND attribute from the user ACID, in order to reinstate security access for the user.

028 (1C) 7143 ACID inactive too long

Reason: Attempt to use an ACID that has not been used for some time.

Action: Check/change the INACTIVE control option.
TSS REPLACE(acid) PASSWORD(password)

029 (1D) 7132 Voice or image authentication failed

Reason: Signon failed because voice or image did not match ACID.

Action: Check CA-Top Secret site installation exit message for details.

030 (1E) 9406 Internal reader - usually bad parameters

Reason: Security driver passed invalid or incorrect parameters via the RACROUTE, RACINIT, RACHECK, or RACDEF SVCs.

Action: If site-written code, check macro expansions. Check for invalid parameter list length. Ensure proper specification of MF=E versus MF=L and skeleton macros. Also check that the ACEE= parameter is present for multi-user address spaces.

031 (1F) 9406 Not authorized for function

Reason: Security driver call does not have adequate authority.

Action: If DUFXTR or DUFUPD: TSS ADDTO(acid) DUFXTR/DUFUPD. If RACINIT, program must be APF-authorized.

032 (20) 9407 RACF SVC classname unknown

Reason: The type of security check is not defined to CA-Top Secret.

Action: If site-written code, check macro expansion for proper CLASS value or classname length. If IBM code, check for possible new IBM function. If installation-defined resource, it must be added to the RDT via a TSS command.

033 (21) 9407 Internal system error

Reason: Abnormal condition or abend has occurred.

Action: If site-written code, check macro expansion for proper values. Obtain dump and contact CA.

034 (22) 9407 TSS command failed

Reason: A logic error has occurred during RACROUTE REQUISVA processing.

Action: If problem persists, contact CA technical support.

035 (23) 9406 Cannot determine facility

Reason: Site-written interface to support new facility. Program in control (TOP PRB) does not match the program (prefix key) in the matrix.

Action: Check the facilities matrix entry via FAC(fac) control option. Change the program name via FAC(fac=PGM=pgmname) to the first three letters of the program in control at the time the RACINIT macro is issued.

036 (24) 9406 Internal system error

Reason: Abnormal condition or abend has occurred.

Action: If site-written code, check macro expansion for proper values. Obtain dump and contact CA.

037 (25) 9407 Error obtaining security record

Reason: Abnormal condition or abend has occurred.

Action: If site-written code, check macro expansion for proper values. Obtain dump and contact CA.

038 (26) 7171 Integrity check

Reason: The ACID (job or userid) cannot be used from this terminal or reader.

Action: No action required. macro expansion for proper values. Obtain dump and contact CA.

040 (28) 9403 Insufficient SVA or LSQA storage

Reason: Not enough memory to initiate user.

Action: Try again later.

042 (2A) 7111 Multiple password update has failed.

Reason: The new password supplied is invalid.

Action: Issue a valid new password (see message text for more information) and retry.

043 (2B) 9407 AREC has no password

Reason: A logic error has occurred during RACROUTE request processing.

Action: If problem persists, contact CA technical support.

044 (2C) 9403 Insufficient SVA or Local Storage

Reason: CA-Top Secret was unable to satisfy a cross-memory request due to either insufficient SVA or insufficient local storage.

Action: If problem is insufficient SVA, enlarge SVA/SVA31 site and IPL. (In this case, the message will be issued by multiple address spaces at the same time.)

If the problem is insufficient local storage, decrease the region size and restart the address space.

057 (39) 9015 Incorrect Customer Key

Reason: A probable cause is that the Security File's Customer Encryption Key is not correct.

Action: If CA-Top Secret Security File size was reduced or enlarged, check the TSSXTEND JCL (see the *Installation Guide*). Contact CA Technical Support.

64 (40) Write without ENQ

Reason: SFS logic error.

Action: Contact the Support Center.

65 (41) Invalid volser

Reason: SFS logic error.

Action: Contact the Support Center.

67 (43) 9407 SFS I/O error

Reason: SFS logic error.

Action: Contact the Support Center.

68 (44) 9407 SFS internal error

Reason: SFS logic error.

Action: Contact the Support Center.

69 (45) 9407 SFS abend

Reason: SFS logic error.

Action: Contact the Support Center.

070 (46) 7145 ACID not defined

Reason: Specified ACID does not exist.

Action: TSS CREATE(acid)...

Check default ACID value. If installation exit is generating ACID, then the value is not being built or returned correctly.

071 (47) ACID already defined

Reason: Attempt to define an ACID that is already defined to CA-Top Secret.

Action: Define the ACID using a different user id.

072 (48) ENQ Failure

Reason: SFS logic error.

Action: Contact the support center.

076 (4C) Invalid resource name/length

Reason: SFS logic error.

Action: Contact the Support Center.

077 (4D) Error doing backup

Reason: An open/close error occurred during an attempt to access the backup file.

Action: See accompanying TSS message for clarification.

078 (4E) 9700 DUF/EXTRACT FAILED - user has no (INST)DATA

Reason: A DUFUPD, DUFXTR or EXTRACT request (RACHECK) failed because the specified ACID did not have INSTALLATION data.

Action: No action required.

79 (4F) The MAX size of SECREC has been exceeded

Reason: The SECREC pointer for the ACID has exceeded the 256K maximum.

Action: Move ownership of the target resource to a new ACID.

81 (51) Volume not found

Reason: SFS logic error.

Action: Contact the Support Center.

82 (52) Volume not owned

Reason: SFS logic error.

Action: Contact the Support Center.

84 (54) Volume already defined generically

Reason: Self-explanatory.

Action: See accompanying TSS message(s) for clarification.

85 (55) Volume already defined

Reason: Self-explanatory.

Action: See accompanying TSS message(s) for clarification.

86 (56) Volume prefix not owned

Reason: Self-explanatory.

Action: See accompanying TSS message(s) for clarification.

87 (57) DSN/prefix not defined

Reason: Self-explanatory.

Action: See accompanying TSS message(s) for clarification.

88 (58) DSN/prefix already defined

Reason: Self-explanatory.

Action: See accompanying TSS message(s) for clarification.

89 (59) Prefix owned

Reason: Self-explanatory.

Action: See accompanying TSS message(s) for clarification.

90 (5A) Resource already defined

Reason: Self-explanatory.

Action: See accompanying TSS message(s) for clarification.

91 (5B) Resource not found

Reason: Self-explanatory.

Action: See accompanying TSS message(s) for clarification.

92 (5C) Resource not owned

Reason: Self-explanatory.

Action: See accompanying TSS message(s) for clarification.

100 (64) 9707 TSS address space inactive

Reason: A function cannot be performed because the Security File cannot be indirectly accessed.

Action: Restart TSS started task.

101 (65) 7221 Data set not authorized

Reason: A data set is protected by a defined data set prefix or by default, but the ACID does not have authority to access it.

Action: TSS ADDTO(acid) DSN(dataset prefix), or
TSS PERMIT(acid) DSN(dsname), or
Check for DEFPROT control option.

102 (66) 7227 Data set accessed at unauthorized level

Reason: ACID has been permitted data set access but not at the attempted level.

Action: TSS PERMIT(acid) DSN(dsname) ACCESS(correct-access-level)
Perform TSS WHOHAS or LIST DATA(XAUTH) and look for conflicts. Refer to the discussion of the Security Validation Algorithm in the *User Guide*.

103 (67) 7235 Global dataset access is denied

Reason: Access has been denied to the data set while using CA-TAPE or an attempt was made to open a VSAM data set component (INDEX, DATA, etc.) without going through the CLUSTER.

Action: Refer to violation 101.

104 (68) 7232 FETCH-only library opened for other than read

Reason: Data set is FETCH protected through ACCESS(FETCH) but an open was attempted for other than FETCH access.

105 (69) 7233 Unable to erase residual data

Reason: A scratch operation was attempted and the AUTOERASE control option was set. CA-Top Secret could not overwrite the data set with binary zeroes.

Action: Contact CA.

106 (6A) 7225 Data set accessed with unauthorized program

Reason: Data set access restricted via a privileged program or the program was not found in the library.

Action: Check PERMIT(acid) DSN(dsname) PRIVPGM(pgmname) restrictions.

108 (6C) 7234 Fetch violation

Reason: An illegal I/O operation was attempted against a data set that was restricted with ACCESS(FETCH).

Action: Check permissions or program.

109 (6D) 7226 Dataset access denied by installation exit

Reason: Your security exit determined that access was illegal.

Action: Check any site-issued violation message for reason of denial.

110 (6E) 7222 Dataset accessed at unauthorized time of day

Reason: A DAY restriction is active for the data set.

Action: TSS PERMIT(acid) DSN(dsname) DAYS(list-of-days)

111 (6F) 7223 Dataset accessed on unauthorized day of week

Reason: A DAY restriction is active for the data set.

Action: TSS PERMIT(acid) DSN(dsname) DAYS(list-of-days)

112 (70) 7224 Dataset accessed through unauthorized facility

Reason: A facility restriction is active for the data set.

Action: TSS PERMIT(acid) DSN(dsname) FACILITY(facility-list)

115 (73) 7206 Volume access denied by installation exit

Reason: Your security exit determined that access was illegal.

Action: Check any site-issued violation message for reason of denial.

116 (74) 7210 BLP access unauthorized

Reason: Acid is not authorized to use BLP.

Action: PERMIT acid to volume with ACCESS (BLP)

117 (75) 7201 Volume access not authorized

Reason: An ACID tried to access a volume he or she was not authorized to access.

Action: PERMIT acid to volume.

119 (77) 7207 Volume accessed at unauthorized (wrong) level

Reason: A permitted volume has an access level restriction.

Action: TSS PERMIT(acid) VOLUME(volser) ACCESS(level)

120 (78) 7208 Volume not available for dataset creation

Reason: Data set cannot be created on this volume due to no permission or ACCESS(NOCREATE) restriction.

Action: TSS PERMIT(acid/ALL) VOLUME(volser) ACCESS(CREATE)

121 (79) 7201 Tape volume error

Reason: An ACID tried to access a tape volume he or she was not authorized to access.

Action: Permit ACID to tape volume if necessary

122 (7A) 7209 Volume accessed without dataset specification

Reason: A TAPEVOL or DASDVOL request was performed against a volume that only had ACCESS(CREATE) authority. A data set name was not passed with the request but is required for CREATE restrictions.

Action: TSS PERMIT(acid) VOLUME(volser)
For volume backup/restore, use PRIVPGM as well.

126 (7E) 7203 Volume accessed on unauthorized day of week

Reason: Volume permission has a DAYS restriction.

Action: TSS PERMIT(acid) VOLUME(volser) DAYS(days)

127 (7F) 7202 Volume accessed at unauthorized time of day

Reason: Volume permission has a TIME restriction.

Action: TSS PERMIT(acid) VOLUME(volser) TIMES(tt,tt)
Also check for time zone (TZONE) adjustments.

128 (80) 7204 Volume accessed through unauthorized facility

Reason: Volume permission has a FACILITY restriction.

Action: TSS PERMIT(acid) VOLUME(volser) FACILITY(facility)

129 (81) 7205 Volume access not allowed through this program

Reason: Volume permission has a PRIVPGM restriction.

Action: TSS PERMIT(acid) VOL(volser) PRIVPGM(pgmname)

132 (84) 7251 Minidisk not owned

Reason: User is not allowed to access the minidisk.

Action: TSS PERMIT(acid) VMMDISK (minidisk)

133 (85) 7251 No authorization for minidisk

Reason: User is not allowed to access the minidisk.

Action: TSS PERMIT(acid) VMMDISK (minidisk)

136 (88) 7251 Resource access denied

Reason: CA-Top Secret's authorization algorithm has denied access.

Action: TSS PERMIT(acid)...

140 (8C) 7250 IMS transaction denied - no password

Reason: The attempted IMS transaction is password protected and the password was not supplied.

Action: Supply password with the transaction as follows:
transid(password) ... data ...

142 (8E) 7250 IMS transaction denied - bad password

Reason: An invalid password was supplied for the IMS transaction.

Action: Supply valid password.

144 (90) 7256 Resource access denied by installation exit

Reason: Your site exit denied access to the resource

Action: Check for any site-issued violation message to determine cause.

145 (91) 7252 Resource accessed on unauthorized day of week

Reason: Access denied to resource due to DAYS restriction.

Action: TSS PERMIT(acid) resource DAYS(days)
Also check for time zone (TZONE) adjustments.

146 (92) 7253 Resource accessed at unauthorized time of day

Reason: Access denied to resource due to TIME restriction.

Action: TSS PERMIT(acid) resource TIME(tt,tt)

147 (93) 7194 Terminal locked

Reason: Terminal activity denied due to previous TSS LOCK.

Action: Unlock the terminal via TSS UNLOCK

148 (94) 7193 Terminal unlock failed

Reason: TSS UNLOCK failed because the wrong password was entered.

Action: Enter correct password for UNLOCK.

149 (95) 7255 Resource accessed by unauthorized program

Reason: Wrong program was in control when resource was accessed.

Action: TSS PERMIT(acid) resource(res) PRIVPGM(pgmname)

150 (96) 7254 Unauthorized facility for resource

Reason: Resource not accessed from proper facility.

Action: TSS PERMIT(acid) resource FACILITY(fac)

151 (97) 7257 Unauthorized access level for resource

Reason: Permitted resource accessed with wrong level.

Action: TSS PERMIT(acid) resource ACCESS(accesslevel)

152 (98) 7192 Terminal locked due to excessive violations

Reason: Further use of terminal denied.

Action: LOGOFF or SIGNOFF. Determine reason for violations and take corrective actions (PERMIT user or reprimand user). Check VTHRESH control option.

153 (99) 7054 Security bypass active for this job or user

Reason: Job or session will execute without security restrictions. This may also occur if jobs start while CA-Top Secret is reinitialized.

Action: Check BYPASS control option for correctness. Check site security exit code for correctness.

154 (9A) 7254 ACID submission through wrong facility

Reason: Submission was attempted but ACID has restriction set up by:
TSS PERMIT(acid) ACID(acid) FACILITY(fac)

Action: Check permission restrictions.

155 (9B) 7255 ACID submission through wrong program

Reason: Submission was attempted but ACID has restriction set up by: TSS
PERMIT(acid) ACID(acid) PRIVPGM(privpgm)

Action: Check permission restrictions.

156 (9C) 7270 Job submission failed by installation exit

Reason: Site security exit determined that the submission was illegal.

Action: Check for site message giving reason for denial.

157 (9D) 7271 Job submission ACID not authorized

Reason: Submitting ACID does not have authority to submit job with another ACID.

Action: TSS PERMIT(acid) ACID(submit-ACID)
TSS ADDTO(acid) NOSUBCHK

158 (9E) 7258 Attempt to use restricted TSO command

Reason: An attempt was made to use a TSO command that is not present in the ACIDs LCF list.

Action: TSS ADDTO(acid) CMDS(TSO(cmd, cmd, ...))

159 (9F) 7258 Attempt to use restricted program

Reason: A protected program cannot be used by the ACID.

Action: TSS PERMIT(acid) PROGRAM(pgmname)

160 (A0) 7161 Facility not authorized during this time

Reason: An attempt was made to log on to a facility at a restricted time.

Action: Check FACILITY restrictions for the ACID.

161 (A1) 7162 Facility not authorized on this day

Reason: An attempt was made to log on to a facility on a restricted day.

Action: Check FACILITY restrictions for the ACID.

162 (A2) 219 (DB) Internal TSS command codes

Action: Provide CA with dumps and/or trace/logs.

163 (A3) 7250 Port of ENTRY POE APPCPORT(poe) not authorized

Reason: APPCPORT resource is owned and but is not PERMITTED to user issuing APPC conversation request.

Action: PERMIT user to APPCPORT resource.

164 (A4) 7251 Access denied to PWRJOBS

Reason: PWRJOBS resource is owned and but is not PERMITTED to user issuing PWRJOBS request.

Action: PERMIT user to PWRJOBS resource.

165 (A5) 7251 Record (RLP) access denied.

Reason: CA-Top Secret has denied access to a record within a file. In CICS, it would be an FCT.

Action: PERMIT(acid) FCT(fctname) SELECT(selname)

174 (AE) - 324 Admin's ACID does not exist

Reason: A TSS command has been send to another node using CPF but the ACID for the administrator issuing the command does not exist on the remote system.

Action: Define administrator's ACID on the remote node.

220 (DC) Cross-memory communication failure

Action: Provide CA with dumps and/or trace/logs.

3.1.4 DRC To Message Cross-Reference

This section summarizes CA-Top Secret Detailed Violation Codes, associated messages, and attributes. The table headings represent the following:

Table Heading	Description
DRC CODE	Decimal code
HEX CODE	Hexadecimal code
TSS MSG	The CA-Top Secret user message number related to the violation
SEC9 MSG	The summary violation message sent to the security console
ATTRIBUTES	States code attributes, where:
FAIL	The violation results in real denial of access in all security modes.
FAILWARN	Like FAIL, except in all modes but DORMANT
AUDIT	Violation is flagged as an audited event
PASSWORD	Password violation that honors ARNPW controls
NOVIOL	Do not treat as a violation

DRC attributes can be modified (for site customization) via the DRC control option.

3.1 Detailed Reason Codes

DRC Code	HEX Code	TSS MSG	SEC9	Attributes	Meaning
001	01	7141	7100	AUDIT, FAILWARN	ACID suspended
002	02	7175	7100	AUDIT, FAILWARN	Initiation failed by site exit
003	03	7144	7100		ACID missing (from job card)
004	04	7182	7100	FAILWARN	Facility is inactive
005	05	7140	7100	FAILWARN	ACID access has expired
006	06	7160	7100		Cannot use this facility
007	07	7102	7100	PASSWORD	Password is missing
008	08	7121	7100	NOVIOL	Password supplied with LOGON
009	09	7101	7100	PASSWORD, AUDIT	Incorrect password
010	0A	7110	7100	PASSWORD	Password has expired
011	0B	7111	7100	PASSWORD	New Password invalid
012	0C	7181	7100	FAILWARN	End-of-Day Access revoked
013	0D	7130	7100	FAILWARN, AUDIT	Operator ID card required
014	0E	7131	7100	AUDIT, FAILWARN, PASSWORD	Incorrect OID card
015	0F	7111	7100	PASSWORD	New password reverified incorrectly
016	10	7191	7100		VTHRESH (cancellation)
017	11	7153	7100		Undefined Started Task
018	12				
019	13	7192	7100	AUDIT	Terminal locked due to violations
020	14	7172	7100		Already signed on
021	15	7174	7100		Not a User, Control ACID
022	16	7170	7100		Reader is protected
023	17	7180	7100		TSS DOWN - cannot LOGON
024	18	7142	7100	FAILWARN	User still on vacation
025	19	7173	7100	AUDIT	NOATS
026	1A	7171	7100		Invalid source of submission

DRC Code	HEX Code	TSS MSG	SEC9	Attributes	Meaning
027	1B	7120	7100	AUDIT, FAILWARN	PTHRESH limit exceeded
028	1C	7143	7100	AUDIT, FAILWARN	ACID inactive too long
029	1D	7132	7100	AUDIT, FAILWARN, PASSWORD	Bad image
030	1E	9406	7100	AUDIT, FAILWARN	Invalid internal parameter passed
031	1F	9405	7100	AUDIT, FAIL	No authority for internal function
032	20	9410	7100	AUDIT, NOVIOL	classname unrecognized
033	21	9407	7100	AUDIT, FAILWARN	Internal system error or abend
034	22	9407	7100	AUDIT	TSS command failed
035	23	9406	7100	AUDIT, FAILWARN	Unknown Facility
036	24	9406	7100	AUDIT, FAILWARN	GETAR error
037	25	9407	7100	AUDIT, FAILWARN	Unable to obtain security record
038	26	7171	7100	AUDIT, FAIL	Internal integrity check failed
039	27				
040	28				
041	29				
042	2A	7111	7100	AUDIT, FAIL	SFS - MULTIPW PW update
043	2B	9407	7100	AUDIT, FAIL	SFS - AREC has no PW
044	2C	9403	7100	AUDIT, FAIL	No SVA for GETAR
045	2D				SFS - Internal error
046	2E				SFS - Internal error
047	2F				SFS - Internal error
048	30				SFS - Internal error
049	31				SFS - Internal error

3.1 Detailed Reason Codes

DRC Code	HEX Code	TSS MSG	SEC9	Attributes	Meaning
050	32				SFS - Internal error
051	33				SFS - Internal error
052	34				SFS - Internal error
053	35				SFS - Internal error
054	36				SFS - Internal error
055	37				SFS - Internal error
056	38				SFS - Internal error
057	39				Incorrect customer key
058	3A				SFS - Internal error
059	3B				SFS - Internal error
060	3C				SFS - Internal error
061	3D				SFS - Internal error
062	3E				SFS - Internal error
063	3F				SFS - Internal error
064	40				SFS - Internal error
065	41				SFS - Invalid volser
066	42				SFS - Internal error
067	43	9407	7100		SFS - I, O error
068	44	9407	7100		SFS - Internal error
069	45	9407	7100		SFS - abend
070	46	7145	7100		ACID not defined
071	47				SFS - ACID already exists
072	48				SFS - Internal error
073	49				SFS - Internal error
074	4A				SFS - Invalid resource name length
075	4B				SFS - Internal error
076	4C				SFS - Internal error
077	4D				SFS - Error during backup
078	4E	9700	900	NOVIOL	ACID has no INSTDATA for DUF.
079	4F				SFS - Internal error

DRC Code	HEX Code	TSS MSG	SEC9	Attributes	Meaning
080	50				SFS - Internal error
081	51				SFS - Volume not found
082	52				SFS - Volume not owned
083	53				SFS - Volume not owned
084	54				SFS - Volume already defined
085	55				SFS - Volume already defined
086	56				SFS - Volume prefix not owned
087	57				SFS - DSN/prefix not defined
088	58				SFS - DSN/prefix already defined
089	59				SFS - Prefix owned
090	5A				SFS - Resource already defined
091	5B				SFS - Resource not found
092	5C				SFS - Resource not owned
093	5D				SFS - Internal error
094	5E				SFS - Internal error
095	5F				SFS - Internal error
096	60				SFS - Internal error
097	61				SFS - Internal error
098	62				SFS - Internal error
099	63				SFS - Internal error
100	64	9407	7100	AUDIT	TSS is down - unable to perform
101	65	7221	7220		Data set not defined
102	66	7227	7220		Unauthorized access
103	67	7235	7220		Bad VSAM opn, no ABS(CATAPE)
104	68	7232	7220		FETCH-only data set violation
105	69	7233	7220		Unable to erase residual data on a scratch request
106	6A	7225	7220		Data set accessed with wrong program
107	6B	7231	7220		Data set accessed from wrong library
108	6C	7234	7220		FETCH violation
109	6D	7226	7220	FAILWARN	Dataset access rejected by exit

3.1 Detailed Reason Codes

DRC Code	HEX Code	TSS MSG	SEC9	Attributes	Meaning
110	6E	7222	7220		Data set accessed at wrong time
111	6F	7223	7220		Data set accessed on wrong day
112	60	7224	7220		Data set accessed thru wrong facility
113	71				
114	72				
115	73	7206	7200	FAILWARN	Volume access denied by exit
116	74	7210	7200		BLP violation
117	75	7201	7200		Volume access not authorized
118	76				
119	77	7207	7200		Volume access at wrong level
120	78	7208	7200		Cannot create on this volume
121	79	7201	7200		System error getting volume info
122	7A	7209	7200		Cannot access volume w, o data set
123	7B				
124	7C				
125	7D				
126	7E	7203	7200		Volume accessed on wrong day
127	7F	7202	7200		Volume accessed at wrong time
128	80	7204	7200		Volume accessed thru wrong facility
129	81	7205	7200		Volume accessed with wrong program
130	82				
131	83				
132	84	7251	7250		Minidisk not owned
133	85	7251	7250		No authority for minidisk
134	86				
135	87				
136	88	7251	7250		Resource - Access denied
137	89				
138	8A				
139	8B				

DRC Code	HEX Code	TSS MSG	SEC9	Attributes	Meaning
140	8C				IMS
141	8D				
142	8E				IMS
143	8F				TSS, VM
144	90	7256	7250	FAILWARN	Resource access denied by site exit
145	91	7252	7250		Resource accessed on wrong day
146	92	7253	7250		Resource accessed at wrong time
147	93	7194	7250	FAIL	Terminal locked
148	94	7193	7250	FAIL, PASS-WORD	Unlock failed - bad password
149	95	7255	7250		Resource accessed via wrong program
150	96	7254	7250		Resource accessed via wrong facility
151	97	7257	7250		Resource access level not authorized
152	98	7192	7250		VTHRESH locked
153	99	7054	7100	NOVIOL	Bypass active - not a violation
154	9A	7272	7250		ACID submit through wrong facility
155	9B	7273	7250		ACID submit through wrong program
156	9C	7270	7250	FAILWARN	ACID submit failed by site exit
157	9D	7271	7250		Not authorized to submit this acid
158	9E	0000	7250		Not authorized to use this command
159	9F	0000	7250		Not authorized to use this program
160	A0	7161	7250		Facility accessed at wrong time
161	A1	7162	7250		Facility accessed on wrong day
165	A5	7259	7250		Resource access denied to a record
166	A6	7260	7250		Resource access denied to a screen
167	A7	7163	7100		Illegal facility for this system
168	A8	7259	7250		RLP logic error--access denied to a record
169	A9	7260	7250		SLP logic error--access denied to a screen
174	AE	0324			Target node admin ACID missing

3.2 TSSMAINT Abend Codes

Code	Explanation
1500	Unable to open MAINTIN.
1501	Unable to open MAINTOUT.
1502	Invalid control statement verb (not CREATE).
1503	CA-Top Secret cannot be active for CREATE.
1504	Invalid control statement.
1505	Syntax error in control statement.
1506	Unable to open Security File.
	Note: This abend is also displayed as a normal part of running TSSMAIND. (TSSMAIND is used during installation to calculate the number of blocks required for the Security File).
1508	Password required for SCA definition.
1509	Non-numeric specified.
1510	Error creating Security File. See SYSPRINT output for further details.
1513	Not Master SCA.
1514	Same as 1506 for DUMP option.
1515	Security File BLOCKSIZE is different from JCL-supplied BLOCKSIZE. Do not code the BLKSIZE keyword in the JCL.
1516	Unable to open Audit/Tracking File.
1517	Unable to open Recovery File or the Recovery File was specified incorrectly with Keys.
1518	Blocksize too small.
1519	Unable to open CPF Recovery File.
Note:	Always review the sysprint output of the TSSMAINT job for further information about the error or abend.

3.2.1 TSSUTIL Abend Codes

Code	Explanation
1600	User not authorized to use TSSUTIL (i.e., user is not a control ACID or does not have REPORT authority)
1601	CA-Top Secret is not active
1602	No authority
1603	No report administration authority
1604	Referenced department is not yours
1605	Referenced division is not yours
1606	Department unknown
1607	ACID not defined to CA-Top Secret
1608	Referenced ACID not in your department
1609	Syntax error in control statement
1610	Unknown option in control statement
1611	DCA can not supply departments
1612	Specified department not in your division
1613	Division unknown
1614	Division not within your scope of authority
1615	Department not within your scope of authority
1616	ACID not within your scope of authority
1617	No report authority (i.e., a user who is not an SCA attempted to use the ACID() keyword
1618	Unable to open SYSPRINT
1619	Unable to open SYSIN
1620	Invalid date or time span
1621	Unable to open GRO file
1690	Storage GETVIS failed
1692	Unable to open SMFIN
1693	Unable to open SMFOUT
1699	CA-Top Secret cross-memory communications failure

3.2.2 TSSRECVR Abend Codes

Code	Explanation
1700	No authority to use utility (not an SCA).
1701	Unable to open RECVFILE, RECVCMDS, or RECVPRT.
1702	CA-Top Secret is not active; abort requested.
1703	Invalid option supplied via EXEC PARM.
1717	I/O error occurred when processing the Recovery File. Refer to message TSS88112E.

3.2.3 TSSTRACK Abend Codes

Code	Explanation
1801	Server error occurred.
1802	Diagnostic trap location reached.
1804	Terminal I/O Interface routine error.
1805	Terminal I/O Interface routine error.

3.2.4 TSSAUDIT Abend Codes

Certain error conditions cause TSSAUDIT to abend with one of the user abend codes shown below.

Code	Explanation
2700	User not authorized to perform function
2701	CA-Top Secret inactive
2702	CA-Top Secret is down
2703	Unable to open RECOVERY data set
2704	Unable to open AUDITIN data set
2705	Unable to open AUDITOUT data set
2706	Invalid function specified
2708	Could not obtain security information
2709	Could not obtain security information
2717	Could not obtain user's security record
2718	Could not access Security File
2719	Insufficient storage in region running report.
2720	Unable to free storage
2729	Permanent I/O error-accessing RECOVERY data set

3.2.5 TSSCHART Abend Codes

Code	Explanation
0998	Produced immediately after TSS1004E message issued to determine if the error was caused by CA-Top Secret or another vendor product.

3.2.6 TSSXTEND Abend Codes

Code	Explanation
0001	SYSIPT INPUT missing or KEY= missing
0002	SYSPRINT DD missing
0003	CAISOCL DLBL missing
0004	SECFNEW DLBL missing
0005	ACID supplied is not the MSCA
0006	CA-Top Secret is not active
0007	Key parameter is invalid
0008	New file not formatted
0999	DEBUGabend
1001	Volume index full
1002	Resource index full
1003	Prefix index full
1004	ACID index full
1005	ARLB segments full
1006	QMAN failure
1007	RARB not returned from SFS
1010	Error converting RDT
1011	Allocated too many blocks for AREC
1012	Allocated an ARLB out of range
1013	Block map out of synch with key
1014	Free ARLB not nulls
1015	Allocated block out of range
1016	BAD ENTRY IN VIX
1017	BAD ENTRY IN PIX
3000	No function supplied
3001	Cannot open SECFOLD
3002	Cannot open SECFNEW
3003	Cannot open MAINTOUT
3004	Cannot open MAINTIN
3005	Encryption Key (existing) is incorrect

3006	Invalid Encryption Key or Damaged Acid
3007	New file incorrectly formatted
3008	New file is too small
3009	New File is not new, i.e., prior EXTEND failed and file is not reformatted
3010	Logical error. Contact CA with dump.
3013	SECFOLD missing
3014	Not Master SCA
3015	Unknown function specified in the control statements input file.
3016	Unknown input parameter specified in the control statements input file.
3018	Invalid parameter in control statement
3020	Encryption Key not supplied
3021	Invalid Key
3028	Security File repair function was unable to verify unexpected anomaly
3031	Invalid Parameter encountered
3032	Illegal syntax specified for parameter
3033	Hexadecimal value must be 0-9, A-F
3034	Length value must be between 01 and FFFF
3035	Invalid hexadecimal number
3036	Data is missing
3037	Invalid acidname
3038	RBA not within file
3039	ACID not defined

3.2.7 TSSFAR Abend Codes

Code	Explantion
2700	Not the MSCA
2701	Failed getmain
2702	Bad input parameters
2703	KEY= card missing
2704	Bad hex character in supplied key
2705	Error trying for security file lock
2706	Error trying for security file unlock
2707	Target XE area too small for input

3.2 TSSMAINT Abend Codes

2708	Duplicate or missing file specification
2709	RACVT missing
2710	SYSPRINT open error
2711	SYSIPT open error
2712	CAISOGR open error
2800	Error reading resource index (RIE)
2801	Error reading volume index (VIE)
2802	Error reading volume prefix index (VIE)
2803	Error reading prefix index (PIE)
2804	Block read is not a valid reader record
2805	Get ARLB error
2806	Error reading ACID index (AXE)

3.2.8 CICS Abend Codes

Code	Module That Issued the Abend and Explanation
KS01	CAKSIGN - Maximum signon limit reached.
KV01	CAKSRVAL - File open error.
KR01	CAKSROUT - Allocation task token failure.
KR02	CAKSROUT - Allocation session related token failure.
TBZ5	TSSCPW - Password prompt send/receive error.
TAZ6	TSSCMS - Message send command error.
TAZ7	TSSCMS - Abend request from message exit routine.
TAZ8	TSSCMS - Message send to invalid device error.
TEZ0	TSSCST - Command error.
TG1B	TSSCPOST - ACEE/SECREC getmain failure.
TG1C	TSSCPOST - DFHTRAC0 attach failure due to lack of SVA.
TG1D	TSSCPOST - DFHTRAC0 attach failure.
TG1E	TSSCPOST - Invalid parameter list passed to DFHTRAC0.
TG1F	TSSCPOST - TSSCRINT STCB getmain error (lower Maxsign parameter).
TG1G	TSSCPOST - TSSCSMGR logic error.
TG1H	TSSCPOST - MAXSIGN limit reached. Maximum SIGNON/SIGNOFF requests, No Retry Specified.
TG8W	TSSCPOST - Storage manager DUSB getmain failure.
TG8X	TSSCPOST - Storage manager DUSB invalid parameter list.
TMOS	Sending CICS region has MOS feature active, but receiving system does not.
TUZ3	TSSCICS - CA-Top Secret is not active.
TUZ4	TSSCICS - TSS/CICS control block location error.
TZZ1	TSSCAI - TSS/CICS application interface transaction is not associated with a terminal.
TZZ2	TSSCAI - TSS/CICS application interface logic error (Assign Command Error).
TZZ3	TSSCAI - TSS/CICS application interface parameter list address invalid.
TZZ4	TSSCAI - TSS/CICS application interface Read Temporary Storage Queue ID error.
TZZ5	TSSCAI - TSS/CICS application interface parameter list length error.
TZZ6	TSSCAI - TSS/CICS application interface Write Temporary Storage Queue ID error.

- TZZ7** TSSCAI - TSS/CICS application interface parameter list length does not equal parameter list type or invalid value in header field.
- TZZ8** TSSCAI - TSS/CICS application interface call was unable to attach a subtask to complete the request.
- T11W** TSSCRT - Storage manager USCB/TTCB bad parameter list.
- T11X** TSSCRT - MAXUSER limit reached (reset maxuser).
- T11Y** TSSCRT - Storage manager USCB/TTCB getmain failure.
- T26Z** TSSCXS - CICS control block address error.
- T283** TSSCXS - DSNB/FILE access error.
- T310** TSSCXE - Invalid function request parameter.
- T634** TSSCFM - DSNB/FILE access error.
- T6??** TSSCFM - CICS resource control block not found.

In addition to these CICS abends, CA-Top Secret invokes the External Security Manager and makes checks against the PSB at scheduling time. If the installation is able to schedule the PSB, it returns the DBD names. If you are not authorized to access the DBD, a DHA4 abend will occur.

3.2.9 IBM CICS Abend Codes

Code:	Explanation:
AEY7	Transaction or resource access violation. Refer to the associated CA-Top Secret message for details.

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: _____

Reader Comment Form

CA-Top Secret Message and Codes Guide

Release 3.0 VSE

Document Number: R101TS30MCE

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:
