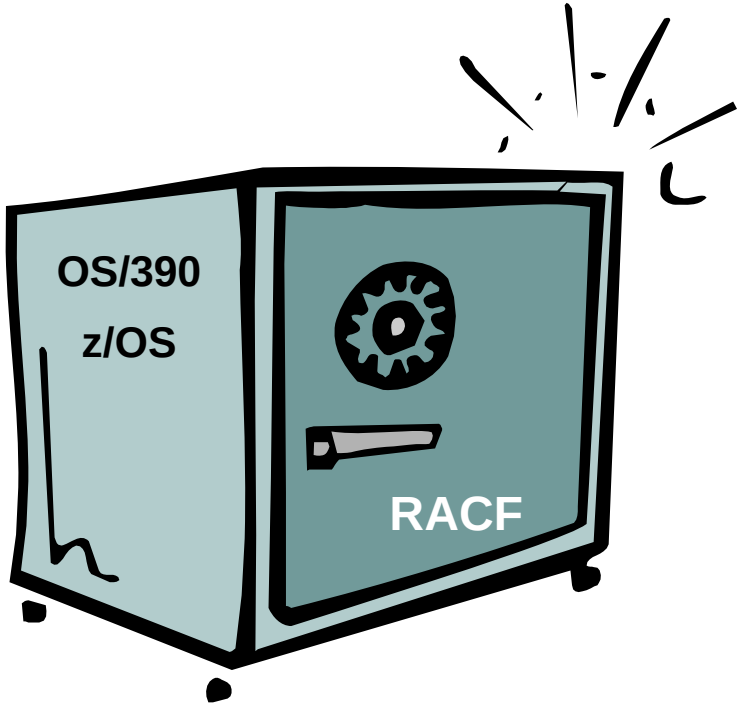
RACF & CICS - THE BASICS

KOIRUG - June 2006



Robert S. Hansel

RACF Specialist - RSH Consulting, Inc.

R.Hansel@rshconsulting.com - 617-969-9050 - www.rshconsulting.com

CICS

Introduction to CICS

RACF Security for CICS

User Identification & Logon Control

Transaction Security

Resource Protection

Command Security

RACLIST and Profile Refresh

CICS BASICS

CICS - Customer Information Control System

- **Provides general-purpose online transaction processing (OLTP)**
- **Data-base/data-communication (DB/DC) system**

Specialized "Operating System" - supports multiple users and processes multiple application system programs concurrently

CICS regions can communicate and share resources

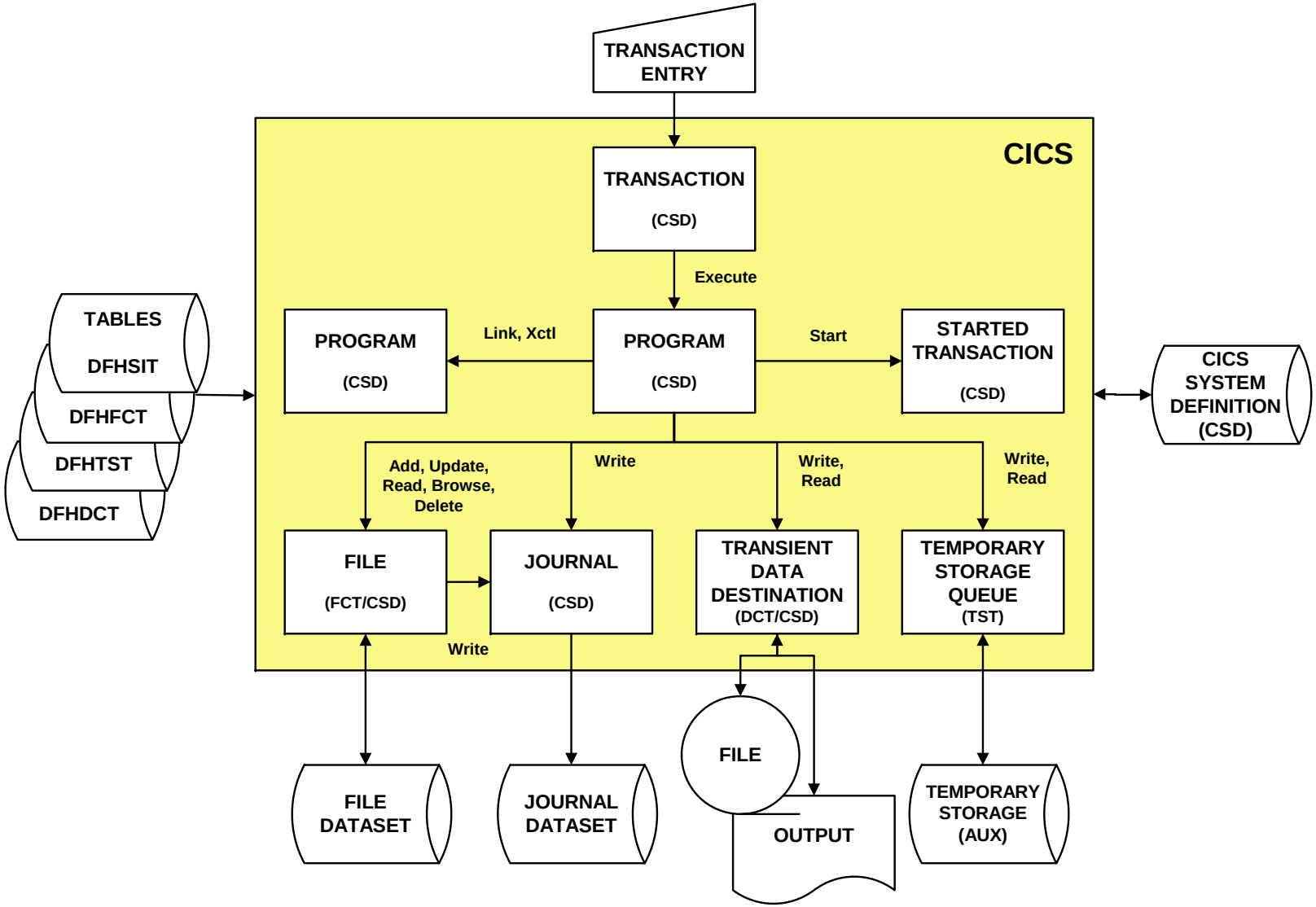
- **Multi-Region Operation (MRO) - within one MVS image or Sysplex**
- **Inter-System Communication (ISC) - within & between MVS images**

Provides interface to other systems - DB2, IMS, IDMS

Recovery and workload balancing

- **Extended Recovery Facility (XRF)**
- **CICSplex**

CICS RESOURCES



CICS SYSTEM DEFINITION (CSD) FILE

Resource Definition Online (RDO) - facility for dynamically defining and configuring resources

CICS System Definition (CSD) file - VSAM file where resource definitions are stored

CSD is updated using transactions CEDA and CEDB, and viewed using CEDC

CICS utility DFHCSDUP provides a listing of the CSD

Table and CSD definitions are used in combination -- CSD takes precedence

SYSTEMS INITIALIZATION TABLE (SIT)

Defines configuration options for a CICS region

SIT parameters govern the RACF interface

Parameter settings obtained from:

- **Built-in CICS defaults**
- **DFHSITxx Macro assembly modules (default DFHSIT)**
- **SYSIN DD Statement**
- **EXEC Statement PARM**
- **Console commands (cannot change security parameters)**

Last parameter definition obtained is the one used

```
//STEP001 EXEC PGM=DFHSIP,PARM='SIT=6$,DLI=YES,CONSOLE,SYSIN,.END'
//SYSIN   DD  *
 APPLID=CICSDEV2
 XUSER=NO
```

SYSTEMS INITIALIZATION TABLE (SIT)

```
SIT      TITLE 'DFHSIT - CICS DEFAULT SYSTEM INITIALIZATION TABLE'
           DFHSIT TYPE=CSECT,
               APPLID=DBDCCICS,  VTAM APPL identifier
               CMDSEC=ASIS,      API command security checking
               DFLTUSER=CICSUSER, Default user
               PLTPISEC=NONE,    No PLT security checks on PI programs
               PLTPIUSR=,        PLT PI userid = CICS region userid
               RESSEC=ASIS,      Resource security check
               SEC=YES,          External security manager option
               SECPRFX=NO,       Security prefix
               USRDELAY=30       Delay before ACEE refresh
               XAPPC=NO,         RACF class APPCLU required
               XCMD=YES,         SPI use default name for RACF check
               XDCT=NO,          DCT do not perform RACF check
               XFCT=$CPFCT,      FCT use local class for RACF check
               XJCT=NO,          JCT do not perform RACF check
               XPCT=YES,         PCT use default name for RACF check
               XPPT=YES,         PPT use default name for RACF check
               XPSB=YES,         PSB use default name for RACF check
               XTRAN=YES,        Transid use default name, RACF check
               XTST=YES,         TST use default name for RACF check
               XUSER=YES         Surrogate user checking to be done
```

RACF PROTECTION

CICS relies on RACF to provide security

RACF controls

- **Who can logon to CICS**
- **Who can execute a transaction**
- **Who can use a transaction resource (RESSEC)**
  - **Started Transaction**
  - **Program**
  - **File**
  - **Journal**
  - **Transient Data Destination**
  - **Temporary Storage Queue**
  - **DL/1 PSBs**
- **Who can execute a CICS command (CMDSEC)**

APPLICATION SECURITY

Many legacy applications provide internal security in addition to or in lieu of RACF

User identification based on:

- **RACF USERID**
- **OPIDENT from CICS Segment**
- **Application USERID and/or password, independent of RACF**

Transaction and function access control:

- **Internal tables or files**
- **Application RACF calls - often incorporating unused CICS resource class (e.g., PCICSPSB)**
- **EXEC CICS QUERY SECURITY command can offer an alternative to internal application tables and controls**

RACF PROTECTION

RACF interface must be activated in SIT parameters

```
SEC=YES,          External security manager option
```

CICS SIT parameters determine what resources are protected

```
XCMD=YES,         SPI use default name for RACF check
XDCT=NO,          DCT do not perform RACF check
XFCT=$CPFCT,      FCT use local class for RACF check
XJCT=NO,          JCT do not perform RACF check
XPCT=YES,         PCT use default name for RACF check
XPPT=YES,         PPT use default name for RACF check
XPSB=YES,         PSB use default name for RACF check
XTRAN=YES,        Transid use default name, RACF check
XTST=YES,         TST use default name for RACF check
```

CICS SIT parameter enables control over ID assignment

```
XUSER=YES,        Enables use of SURROGAT profile checks
```

TERMINAL USER LOGON

RACF validated logon

- CESN sign-on transaction
- Program with EXEC CICS SIGNON command

RACF logon checks

- USERID & Password
- TERMINAL *terminal-id* or CONSOLE *console-name*
- APPL applid - as determine by one of these SIT parameters
  - APPLID= Region's application ID
  - APPLID= XRF generic application ID (when XRF=YES)
  - GRNAME= TOR Group ID (CICSplex)
  - READ access required

CICS concurrent logon restrictions

- SNSCOPE=NONE | CICS | MVSIMAGE | SYSPLEX
  - NONE No restriction
  - CICS Only once in each CICS region
  - MVSIMAGE Only once for entire MVS image
  - SYSPLEX Only once for entire Sysplex
- Only effects user logon via CESN (not pre-set terminal logons)

CICS DEFAULT USER

ID used for transactions when the user is unknown

Supports mandatory transaction authorization checking

SIT DFLTUSER=*userid* - names the default USERID

Default default user - CICSUSER

Default USERID requires access permissions

- **APPL applid**
- **CICS Transactions intended for everyone's use (without logon)**
- **Trigger-transactions (if TD defined with no ATI USERID)**

SURROGAT Class profile (when XUSER=YES)

- ***default-user*.DFHINSTL**
- **READ access allows the CICS region to use the USERID**
- **Prevents substitution of different default USERID**

PROGRAM LOAD TABLE POST-INITIALIZATION (PLTPI) USER

ID optionally assigned for PLTPI program execution

Applies when SIT PLTPISEC = CMDSEC | RESSEC | ALL

SIT PLTPIUSR=*userid* - USERID to use for PLT authorization

PLTPI USERID requires access permissions

- **APPL applid**
- **PLTPI programs and associated resources**

SURROGAT Class profiles (when XUSER=YES)

- ***pltiuser-user*.DFHINSTL**
- **READ access allows the CICS region to use the USERID**

PLTPI programs run under the authority of the CICS region's USERID if PLTPIUSR is not specified

PRESET TERMINAL USER

ID optionally assigned to a terminal in CSD TERMINAL definition

USERID automatically logged on - no password check performed; cannot be logged off

Applications

- **Public kiosk-type terminals**
- **APPC connections**
- **Consoles**

USERID requires access permissions

- **APPL applid**
- **Appropriate transactions and resources**

Restrict use of CEDA INSTALL command in assigning terminal USERIDs - SURROGAT Class profiles (when XUSER=YES)

- ***assignable-user*.DFHINSTL**
- **READ access allows user to make assignment of USERID**

STARTED TRANSACTION

ID optionally assigned to a Started Transaction

EXEC CICS START TRANID(trans-id) USERID(userid)

Started Transaction USERID requires access permissions

- **APPL applid**
- **Resources accessed by the transaction**

SURROGAT Class profiles (when XUSER=YES)

- ***started-userid*.DFHSTART**
- **READ access allows the user executing the program with the START command to use the USERID**

The USERID specified for a non-terminal started transaction only obtains the authority of its default group

AUTOMATIC TRANSACTION INITIATION (ATI) USER

ID optionally assigned to a Trigger transaction

- **USERID= CSD Transient Data definition (DFLTUSER is the default)**
- **EXEC CICS SET TDQUEUE ATIUSERID(userid) command**

ATI USERID requires access permissions

- **APPL applid**
- **Trigger transactions and associated resources**

SURROGAT Class profiles (when XUSER=YES)

- ***atiuser-user*.DFHINSTL**
- **Grant READ access to**
  - **CICS region in which defined**
  - **Users who will assign USERID with INSTALL**
  - **Users who will create the queue with the EXEC CICS CREATE command**
  - **Users who issue the EXEC CICS SET command**

CICS SEGMENT

Used to assign attributes formerly defined in the defunct CICS signon table

CICS Segment Fields

- OPCLASS(operator-class ...)
- **OPIDENT(operator-id)**
- OPPRTY(operator-priority)
- **TIMEOUT(timeout-value)**
- XRFSOFF(FORCE | NOFORCE)

```
ALU RSH CICS NORACF

USER=RSH

CICS INFORMATION
----------------
 OPIDENT= A1C
 OPPRTY= 00000
 TIMEOUT= 60
 XRFSOFF= NOFORCE
```

CICS SEGMENT

FIELD	OPTIONS	SYSTEM DEFAULTS
OPCLASS	decimal 1-24	1
OPIDENT	1-3 character ID	blank
OPPRTY	decimal 0-255	0
TIMEOUT	0-9959 (hhmm)	0
XRFSOFF	FORCE | NOFORCE	NOFORCE

If a USERID does not have a CICS segment …

- **If the CICS Default User has a segment, these values are assigned to the ID (can be used to set a default timeout value for all users)**
- **If the CICS Default User does not have a segment, the system defaults are assigned to the ID**

ACTIVATING RESOURCE PROTECTION

Xxxx= parameters direct CICS to call RACF for associated resource authorization checking

- **XTRAN** **Transactions**
- **XPCT** **Started Transactions**
- **XPPT** **Programs**
- **XFCT** **Files**
- **XJCT** **Journals**
- **XDCT** **Transient Data Destinations**
- **XTST** **Temporary Storage Queues**
- **XPSB** **DL/1 PSBs**
- **XDB2** **DB2ENTRY**
- **XCMD** **CICS Command Functions**

Xxxx= NO | <u>YES</u> | *class-suffix*

- **NO** **Do not protect**
- **YES** **Use default RACF class (default setting)**
- ***suffix*** **Use a locally defined class name with the specified suffix (only means of controlling XDB2)**

RACF CLASSES & PREFIXING

Class names

- Standard prefix character for each Resource class (e.g., MCICSPPT) and Grouping class (e.g., NCICSPPT)
- Default class or locally-defined suffix (e.g., CICSTRN or $CP2TRN)
  - Default XTRAN=YES Use TCICSTRN & GCICSTRN
  - Local XTRAN=$TTRN Use T$TTRN & G$TTRN

RACF class prefix characters & default classes

• T/G	TCICSTRN	GCICSTRN	- Transactions
• A/B	ACICSPCT	BCICSPCT	- Started Transactions
• M/N	MCICSPPT	NCICSPPT	- Programs
• F/H	FCICSFCT	HCICSFCT	- Files
• J/K	JCICSJCT	KCICSJCT	- Journals
• D/E	DCICSDCT	ECICSDCT	- Transient Data Destinations
• S/U	SCICSTST	UCICSTST	- Temporary Storage Queues
• P/Q	PCICSPSB	QCICSPSB	- DL/1 PSBs
• C/V	CCICSCMD	VCICSCMD	- CICS Command Functions

RACF CLASSES & PREFIXING

Class configuration options

- Share default classes among CICS regions
- Create locally-defined independent classes for each region or set of related regions (e.g., production, specific application)
- Use some combination of the above

Classes shared by dissimilar CICS regions

- May need to differentiate resources belonging to specific regions
- Resource names can be prefixed with CICS region's USERID
- SIT Parameter - SECPRFX=YES | NO
- Ex: Transaction PAY1 in region running under ID CICS01 becomes CICS01.PAY1

RACF CLASSES & PREFIXING

```
RLIST TCICSTRN CICT1.CEMT ALL
CLASS       NAME
-----       ----
TCICSTRN    CICT1.C*

GROUP CLASS NAME
----- ----- ----
GCICSTRN

RESOURCE GROUPS
-------- ------
NONE

LEVEL   OWNER      UNIVERSAL ACCESS    YOUR ACCESS   WARNING
-----   --------   -----------------   ----- ------   -------
 00     CICSSPT         NONE              NONE         NO
```

```
RLIST T$TTRN CEMT ALL
CLASS       NAME
-----       ----
T$TTRN      CEMT

GROUP CLASS NAME
----- ----- ----
G$TTRN

RESOURCE GROUPS
-------- ------
NONE

LEVEL   OWNER      UNIVERSAL ACCESS    YOUR ACCESS   WARNING
-----   --------   -----------------   ----- ------   -------
 00     CICSSPT         NONE              NONE         YES
```

RACF CLASSES & PREFIXING

Locally defined class names

- Require entries in:
  - Class Descriptor Table or CDT Class profile (z1.6)
  - RACF Router Table (pre-z1.6)
- Must use standard prefix characters
- Must be defined in pairs - ex: T$CPTRN and G$CPTRN
- Coded in the SIT by suffix - ex: XTRAN=$CPTRN

Considerations / Best Practices

- Devise naming standards to help identify related CICS regions
- Design classes to differentiate environments (e.g. Production, Test)
- Need not be created for all resource classes; can be used in combination with default classes for other resources
- Class names should include a national character (#, @, $) to prevent conflict with future IBM supplied classes
- Assign unique POSIT values to logically interrelated sets of classes
- Define with same characteristics as default CICS classes

CLASS DESCRIPTOR TABLE/PROFILE

ICHERCDE MACRO

```
T$CTSTRN  ICHERCDE CLASS=T$CTSTRN,
                   GROUP=G$CTSTRN,
                   ID=145,
                   MAXLNTH=13,
                   FIRST=ANY,
                   OTHER=ANY,
                   POSIT=130,
                   DFTUACC=NONE,
                   OPER=NO

G$CTSTRN  ICHERCDE CLASS=G$CTSTRN,
                   MEMBER=T$CTSTRN,
                   ID=145,
                   MAXLNTH=13,
                   FIRST=ANY,
                   OTHER=ANY,
                   POSIT=130,
                   DFTUACC=NONE,
                   OPER=NO
```

CDT Class Profile

```
RLIST CDT T$CTSTRN CDTINFO NORACF
CLASS      NAME
-----      ----
CDT        T$CTSTRN

CDTINFO INFORMATION
-------------------
CASE = UPPER
DEFAULTRC = 004
DEFAULTUACC = NONE
FIRST = ALPHA,NUMERIC,NATIONAL,SPECIAL
GENLIST = DISALLOWED
GROUP = G$CTSTRN
KEYQUALIFIERS = 0000000000
MACPROCESSING = NORMAL
MAXLENGTH = 13
MAXLENX = NONE
MEMBER =
OPERATIONS = NO
OTHER = ALPHA,NUMERIC,NATIONAL,SPECIAL
POSIT = 0000000130
PROFILESALLOWED = YES
RACLIST = DISALLOWED      …
```

TRANSACTION SECURITY

Transaction 'Always-call'

- **Terminal user initiated transactions**
- **Started transactions**
- **Trigger transactions (ATI)**

SIT Parm - XTRAN=

Default Classes - TCICSTRN / GCICSTRN

Access - READ

Default security for 'profile not found' is no access

Conditional Access

- **WHEN(TERMINAL(terminal-id))**
- **WHEN(CONSOLE(console-id))**

Does not govern what the transaction does or whether it updates files - simply controls use of the transaction

TRANSACTION SECURITY

CICS-Supplied transactions

- Category 1
  - Ex: CSKP - Writes system log activity keypoint
  - CICS internal use only
  - Only CICS region USERID requires access
- Category 2
  - Ex: CEMT - CICS Master Terminal
  - CICS management, administration, and control
  - Restricted access
  - Recommend no access to CEDF or CEBR in production
- Category 3
  - Ex: CESN - Logon
  - Required by all users - exempt from security checking

RESOURCE SECURITY - SIT PARAMETERS

RESSEC= ASIS | ALWAYS

- **Determines when to perform resource checking for transactions**
- **ASIS Use RESSEC setting on the transaction (default)**
- **ALWAYS Check all resources (Not recommended)**

CMDSEC = ASIS | ALWAYS

- **Determines when to perform command checking for transactions**
- **ASIS Use CMDSEC setting on the transaction (default)**
- **ALWAYS Check all commands (Not recommended)**

PLTPISEC = NONE | CMDSEC | RESSEC | ALL

- **Determines whether to perform checks on PLT programs during CICS initialization**

RESOURCE SECURITY

Activated by parameter on the CSD definition for each individual transaction accessing resources

RESSEC=YES provides resource protection; NO is the default

Performs authorization checks on all resources used by the transaction

Default security for 'profile not found' is no access

Intended for transactions performing diverse functions where not all transaction users are authorized for all accessible resources and functions

Consider ‘catch-all’ profile of ** with UACC of NONE or READ as appropriate

RESOURCE SECURITY

RESOURCE	SIT PARM	ACCESS LEVELS	COMMENTS
Started Transaction	XPCT=	READ	
Program	XPPT=	READ	
File	XFCT=	UPDATE READ	FCT definition also governs access; uses CICS file name - not dsname
Journal	XJCT=	UPDATE	CICS log - DFHLOG - should be UACC(NONE)
Transient Data Destination	XDCT=	UPDATE	System TDs - CPLI, CSSL, CSSO - should be UACC(NONE)
Temporary Storage Queue	XTST=	UPDATE READ	Only checks if DFHTST entry has TYPE=SECURITY; only applies if queue resides on auxiliary storage
Program Status Block	XPSB=	READ	

COMMAND SECURITY

Activated by parameter on the CSD definition for each individual transaction executing System Programming type commands

CMDSEC=YES provides command protection; NO is the default

CICS-supplied transaction with CMDSEC=YES

- **CECI - CICS Command Interpreter**
- **CEDF - Execution Diagnostics Facility**
- **CEMT - CICS Master Terminal**
- **CEST - CICS Supervisor Terminal**

Default security for 'profile not found' is no access

COMMAND SECURITY

SIT Parm - XCMD=

Default Classes - CCICSCMD / VCICSCMD

Resources

- ***target-object-type***
- **Ex: FILE, PROGRAM, TCPIPSERVICE**

Access levels & associated actions

- **ALTER CREATE, DISCARD, INSTALL**
- **UPDATE DISABLE, ENABLE, EXTRACT, PERFORM, RESYNC, SET**
- **READ COLLECT, INQUIRE**

If the target object (e.g., FILE PAYMSTR) also happens to be a type of resource protected by another RACF class (e.g., FCICSFCT) and RESSEC is active, another RACF check is made for access to the target object in its own class and at the same level of access needed for the command (e.g., ALTER to FCICSFCT PAYMSTR to perform DISCARD)

RACLIST AND PROFILE REFRESH

CICS automatically RACLISTs its resource classes

- Uses RACROUTE REQUEST=LIST with GLOBAL=YES
- Profiles are loaded into a shared dataspace in memory
- Classes appear in SETROPTS LIST - GLOBAL=YES RACLIST ONLY
- Once RACLISTed, uses Fast RACF Checking for access authorization - RACROUTE REQUEST=FASTAUTH

Implementing profile changes

- Changes made with RACF commands only effect profiles in the database, not those in memory
- To implement changes, RACLISTed dataspace must be replaced
- Replaced with SETROPTS RACLIST(*member-class*) REFRESH
- Non-disruptive - new dataspace is built before transfer of control
- Need to perform refresh in each OS image where class is RACLISTed
- Be cognizant of POSIT links and Sysplex configuration