October 23 — 26, 2000
Anaheim Marriott
Anaheim, California

Alonia (Lonnie) Coleman
acoleman@us.ibm.com
IBM Dallas Systems Center

IMS

E45

IMS Security

SESSION
1

Security Considerations for DBCTL

RETURN TO INDEX

Disclaimer

The information contained in this document is distributed on as "as is" basis, without any warranty either express or implied. The customer is responsible for use of this information and/or implementation of any techniques mentioned. IBM has reviewed the information for accuracy, but there is no guarantee that a customer using the information or techniques will obtain the same or similar results in its own operational environment.

In this document, any references made to an IBM licensed program are not intended to state or imply that only IBM's licensed program may be used. Functionally equivalent programs that do not infringe IBM's intellectual property rights may be used instead. Any performance data contained in this document was determined in a controlled environment and therefore, the results which may be obtained in other operating environments may vary significantly. Users of this document should verify the applicable data for their specific environment.

It is possible that this material may contain references to, or information about, IBM products (machines and programs), programming, or services that are not announced in your country. Such references or information must not be construed to mean that IBM intends to announce such IBM Products, programming or services in your country.

Trademarks or Registered Trademarks of IBM

The following are trademarks or registered trademarks of the International Business Machines Corporation:

IMS
IMS/ESA
MVS/ESA
MVS
ESA
RACF
S/390
System/390
OS/390
DB2
CICS
IBM

Objectives

- **Provide technical overview of the security options available when DBCTL is accessed from**
  - Customer Information Control System (CICS) environments
  - OS/390 address spaces that utilize the Open Database Access (ODBA) interface
  - IMS batch message processing (BMP) region
- **Provide sample RACF commands and/or IMS definitions required to implement security options**
  - Sample commands and definitions are provided for your reference.

Agenda

- **What is DBCTL?**
- **CICS - DBCTL**
  - Components
  - Security options
    - CICS program specification block (PSB) security
    - DBCTL application group name (AGN) security
    - IMS command security

Agenda ...

- **Open Database Access (ODBA) - DBCTL**
  - What it is and the components of an ODBA environment
  - Security options
    - DBCTL application group name (AGN) security
    - IMS command security
- **IMS batch message processing (BMP) - DBCTL**
  - Security options
    - DBCTL application group name (AGN) security
    - IMS command security

Available Education

Course title: **Implementing IMS Security**
Course number: **CM431**
Section: **AB8A**

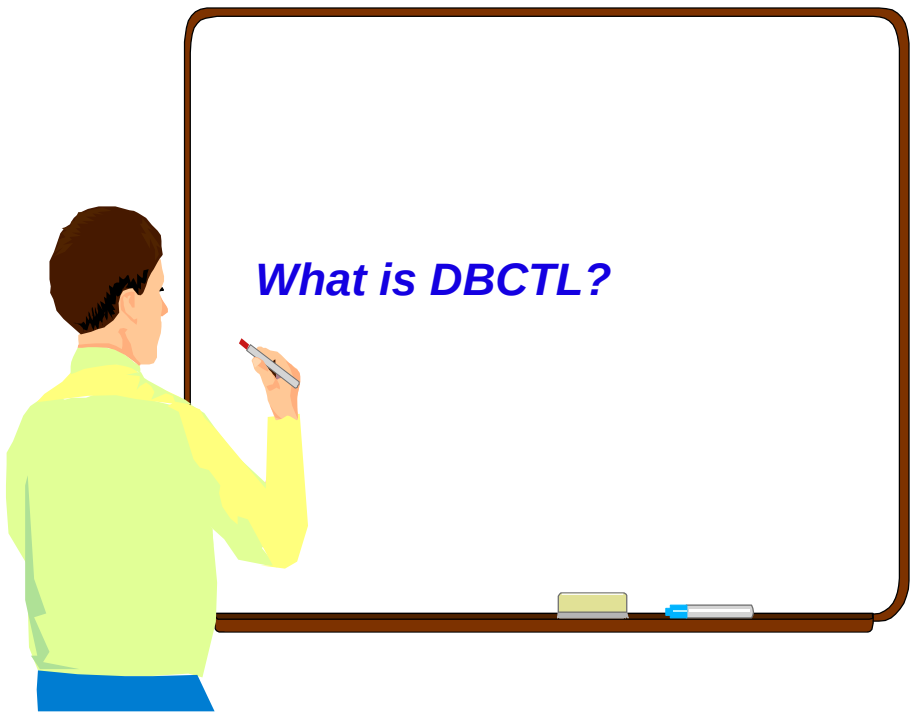
Duration: **4.0 days**
Class status: **Open**
Start date: **10/16/00**
End date: **10/19/00**
Start time: **09:00 AM**

Street address: **330 N Wabash Ave.**
City, state: **Chicago, IL**

Enrollments: **1-800-IBM-TEACH**
http://www.ibm.com/services/learning/us

IMS Technical Conference 2000

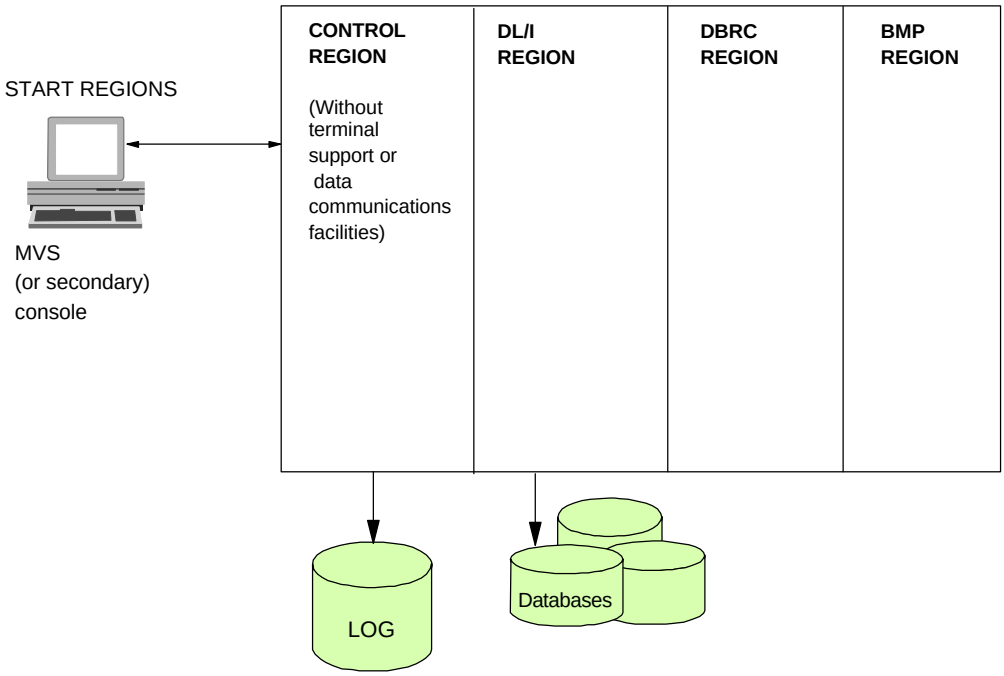
- **Speaker: Robert Hain**
- **Topic: 'Implementing the Command Authorization Exit Routine (DFSCCMD0) to Enhance IMS Command Security'**
- **Objective: Through customization of DFSCCMD0, achieve both IMS command verb and keyword security checking using RACF.**



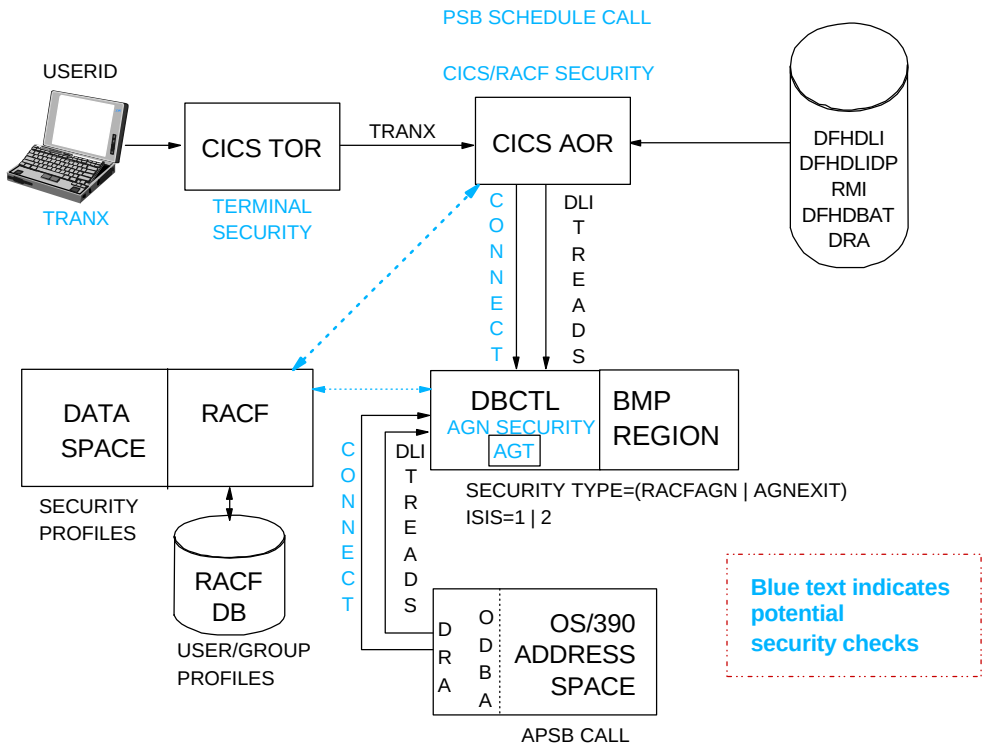
What Is Database Control (DBCTL)?

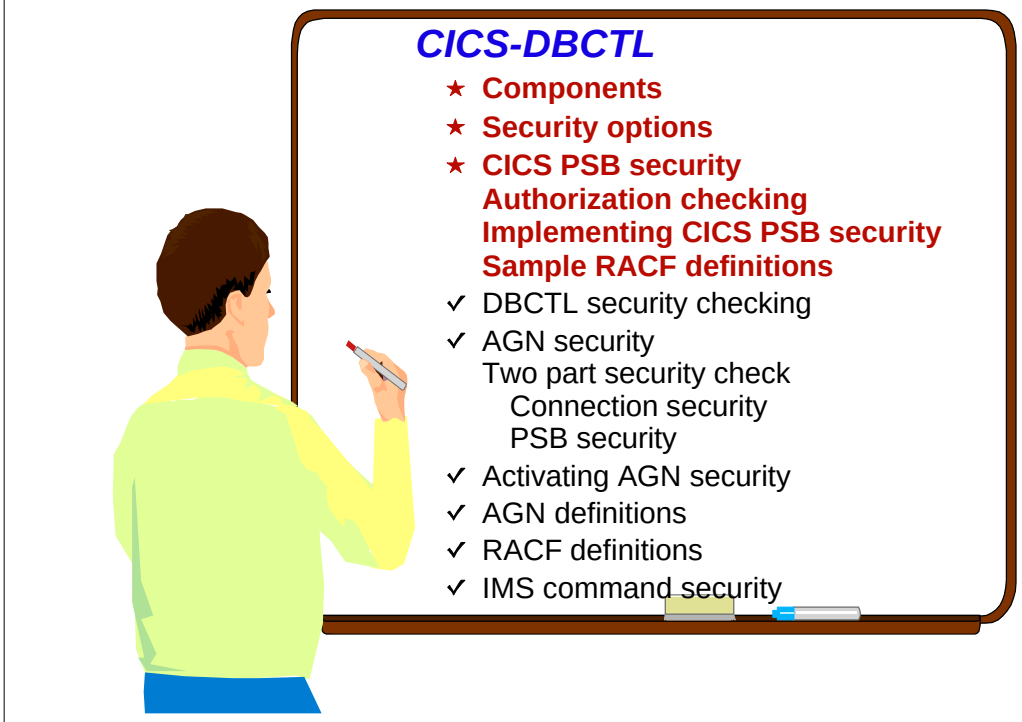
- **IMS Database Manager component**
  - Consists of
    - IMS control region
    - DL/I separate address space
      - Owns DL/I databases
    - Database Recovery Control (DBRC) address space
      - Manages logging, database recovery, database availability, and data sharing
    - Batch message processing (BMP) regions
- **DBCTL supports interfaces to**
  - Coordinator controller (CCTL), such as CICS,
    - User terminals, message handling, and application scheduling
    - Uses interface to pass DL/I calls to DBCTL
  - OS/390 address space using Open Database Access (ODBA)
  - IMS batch message program (BMP) region

Example of DBCTL Environment

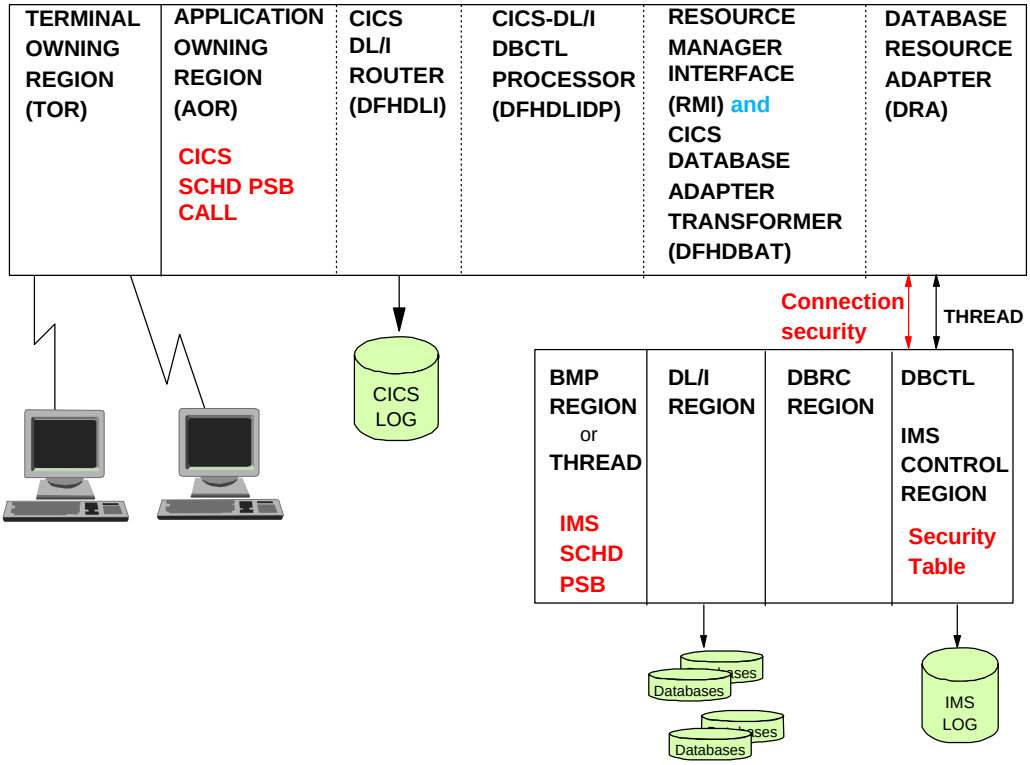


Database Control (DBCTL) Security





CICS - DBCTL Components



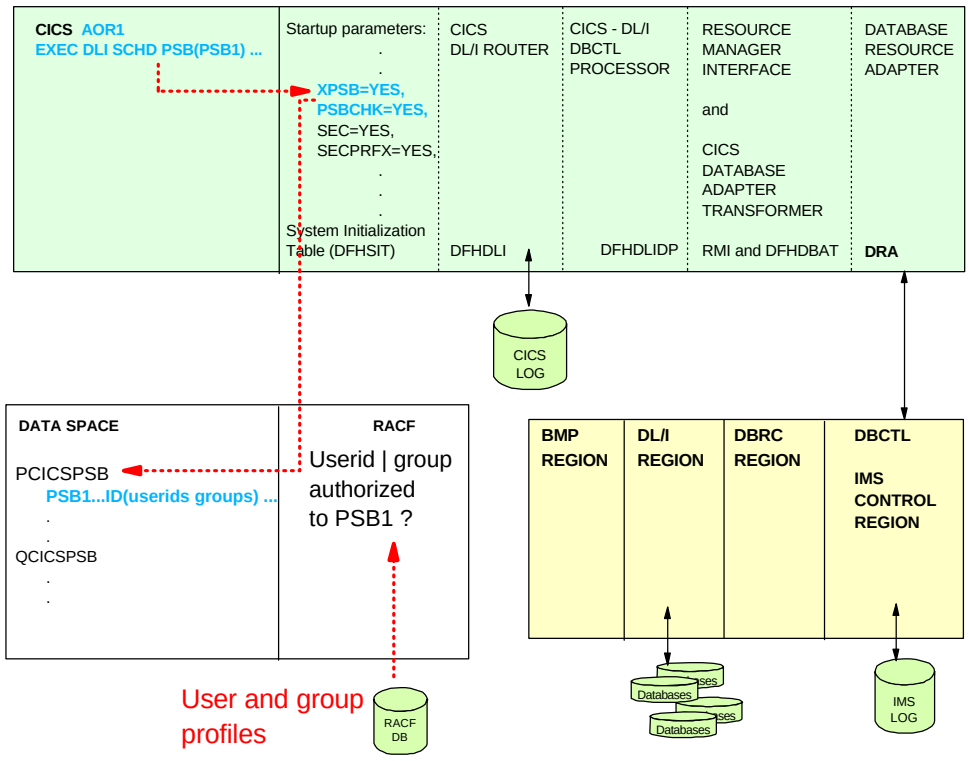
CICS - DBCTL Security Options

- **CICS PSB security**
  - Performed by CICS and RACF
- **DBCTL application group name (AGN) security**
  - Two-part security check
    - CICS-DBCTL connect time security
    - DBCTL PSB schedule security
  - Security checks performed by
    - DBCTL and RACF
      - or -
    - DBCTL and user exit routine
- **Command security checking**
  - DBCTL and RACF
  - DBCTL
- **CICS - DBCTL security checking is *optional***

CICS PSB Security

- **Program specification block (PSB) scheduling requests sent to DBCTL for *processing***
  - CICS requests PSB authorization checking
- **CICS invokes RACF at PSB schedule time**
  - **Determine if CICS terminal user is authorized to access the PSB**
  - RACF classes used in authorization process
    - PCICSPSB singular resource class
      - or -
    - QCICSPSB grouping resource class
- **RACF profile names**
  - Must match PSB names specified in CICS PSB schedule commands

PSB Authorization Checking By CICS



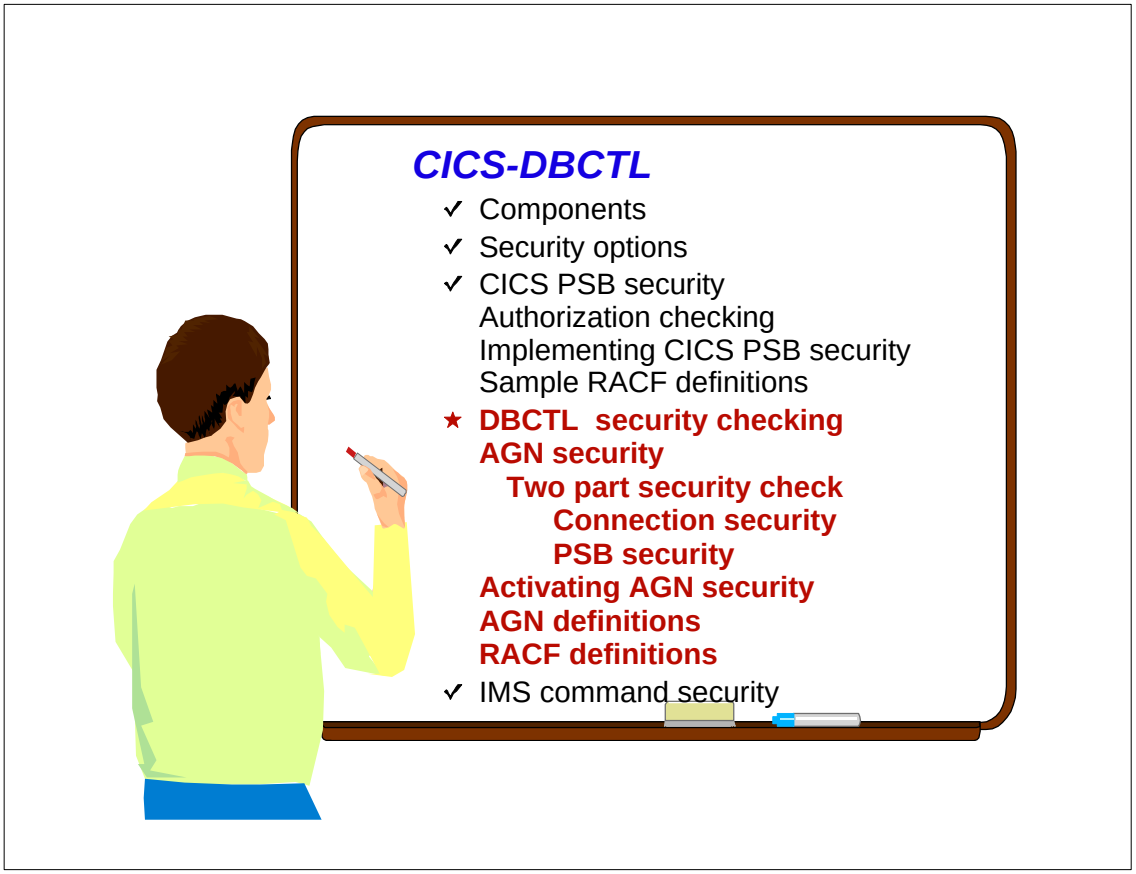
Implementing CICS PSB Security

- **CICS system initialization parameters**
  - SEC=YES
  - SECPRFX=YES
    - If RACF profiles defined with CICS region userid as a prefix
  - XPSB=YES
    - If using the RACF default classes PCICSPSB and QCICSPSB
      - Otherwise use XPSB=*user_defined_class_name*
  - PSBCHK=YES
    - PSB authorization checks for remote terminal users who use transaction routing
      - Initiate transaction in a CICS region that accesses a DBCTL system
- **Define the PSB profiles to RACF and authorize userid | groups**

CICS PSB RACF Definition Examples

Sample RACF commands to authorize the CICS end user's userid/group access to the PSB that is scheduled in a CICS application owning region:

```
RDEFINE  PCICSPSB  PSB1 UACC(NONE)
PERMIT PSB1 CLASS(PCICSPSB) ID(MIKEG GROUP1 GROUP2)
   ACCESS(READ)


RDEFINE  QCICSPSB  PAYPSBS UACC(NONE)
     ADDMEM(PSB2, PSB3, ..., PSBN)
PERMIT PAYPSBS CLASS(QCICSPSB) ID(GROUP3 MGONZO)
   ACCESS(READ)
```



DBCTL AGN Security

- **Application Group Name (AGN) security is provided by *IMS***

- **AGN security involves two part check**

1. Determine if the CICS userid can connect to DBCTL
   - CICS userid passed in PAPL portion of DRA
   - Database Resource Adapter (DRA) specifies AGN
   - CICS userid must be authorized to RACF profile protecting the AGN

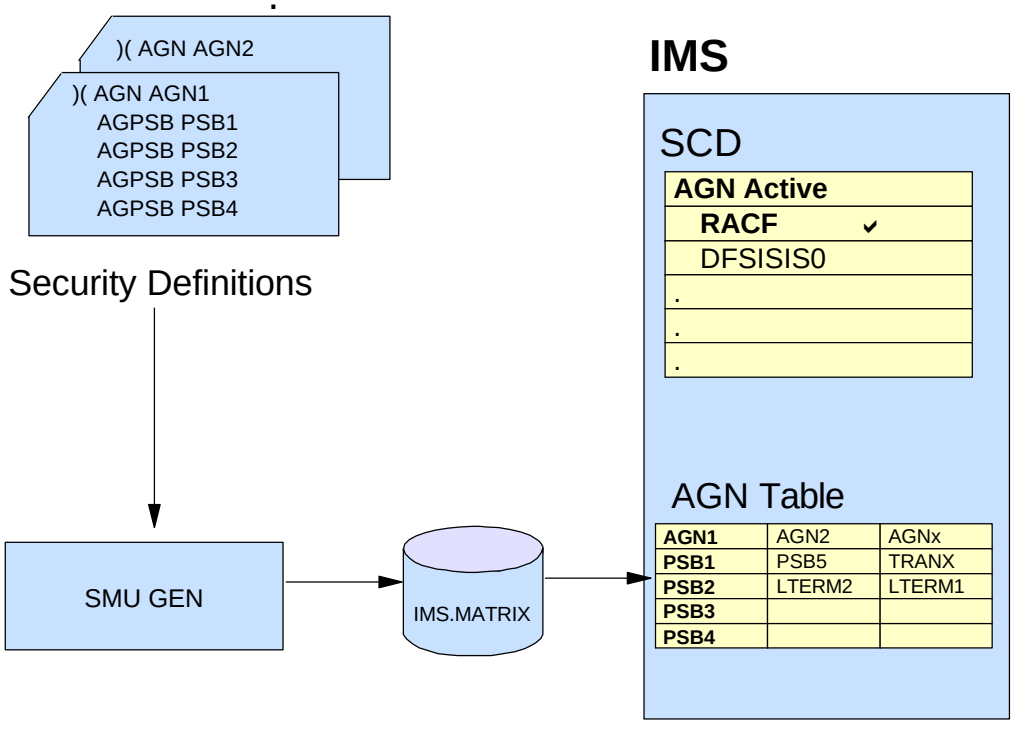
2. Determine if the PSB schedule request from CICS is authorized to be performed in DBCTL
   - Unrelated to CICS PSB security using PCICSPSB
   - DBCTL checks to make sure PSB requested is part of AGN

Activating AGN Security

- **When AGN security is active**
  - Both checks are required
    - Connect-time and PSB schedule-time checks

- **Activating AGN security in IMS**
  - Using the SECURITY macro
    - SECURITY TYPE=(RACFAGN) or
    - SECURITY TYPE=(AGNEXIT)
  - Defining AGNs
    - SMU definitions
    - SMU generation
  - Using IMS startup parameters
    - ISIS=1 or
    - ISIS=2

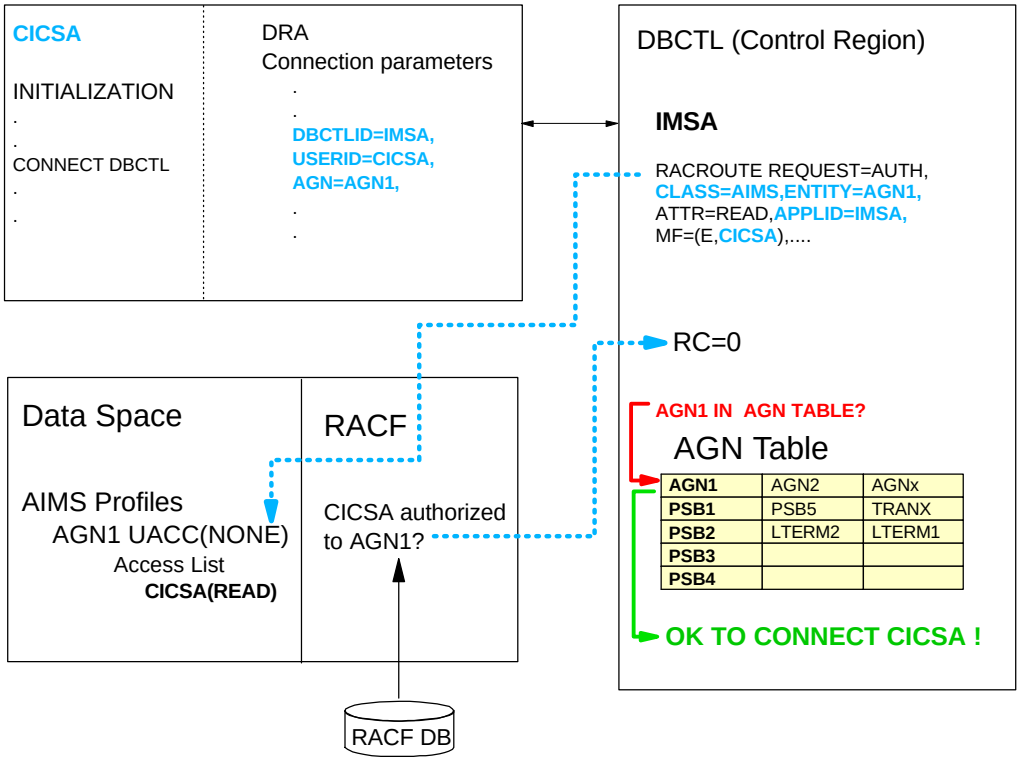
AGN Definitions



Database Resource Adapter (DRA)

```
EJECT
DFSPRP    DSECT=NO,
          DBCTLID=IMSA,
          DDNAME=CCTLDD,
          DSNAME=IMS.RESLIB,
          MAXTHRD=99,
          MAXTHRD=99,
          TIMER=60,
          USERID=CICSA,
          CNBA=10,
          FPBUF=,
          FPBOF=,
          TIMEOUT=60,
          SOD=A,
          AGN=AGN1
END
```

DBCTL AGN Connection Security

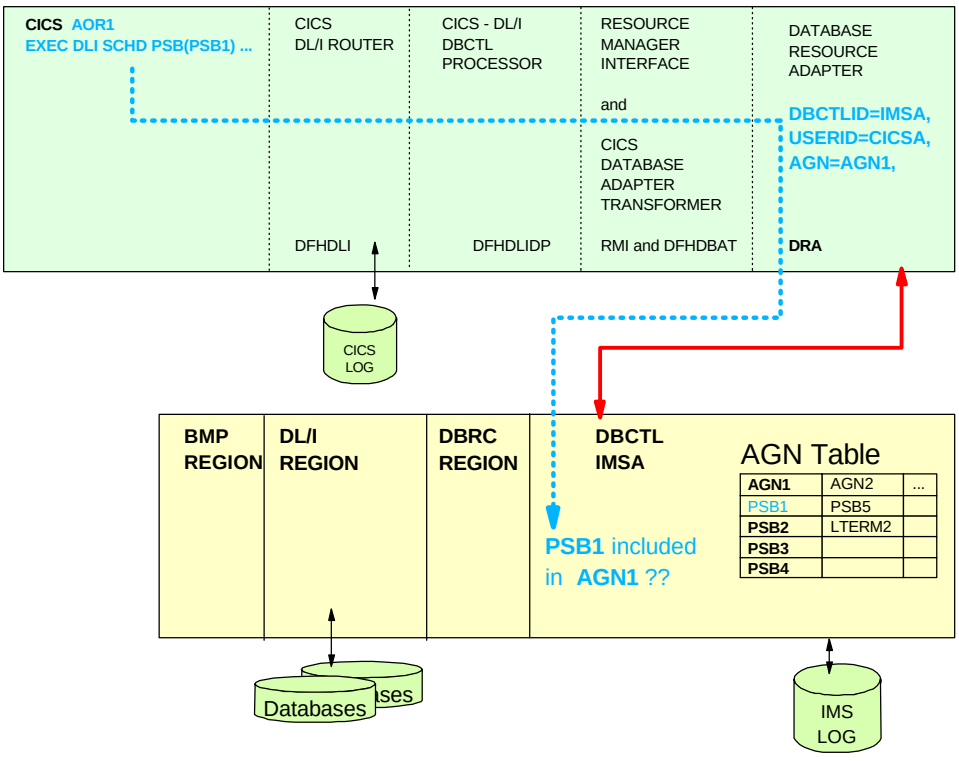


RACF Definitions

Sample RACF commands to define an AGN group (AGN1) and authorize (permit) the CICS userid (CICSA) to the AGN:

RDEFINE AIMS **AGN1** OWNER(IMSADMIN) UACC(NONE)
PERMIT AGN1 CLASS(AIMS) ID(**CICSA**) ACCESS(READ)

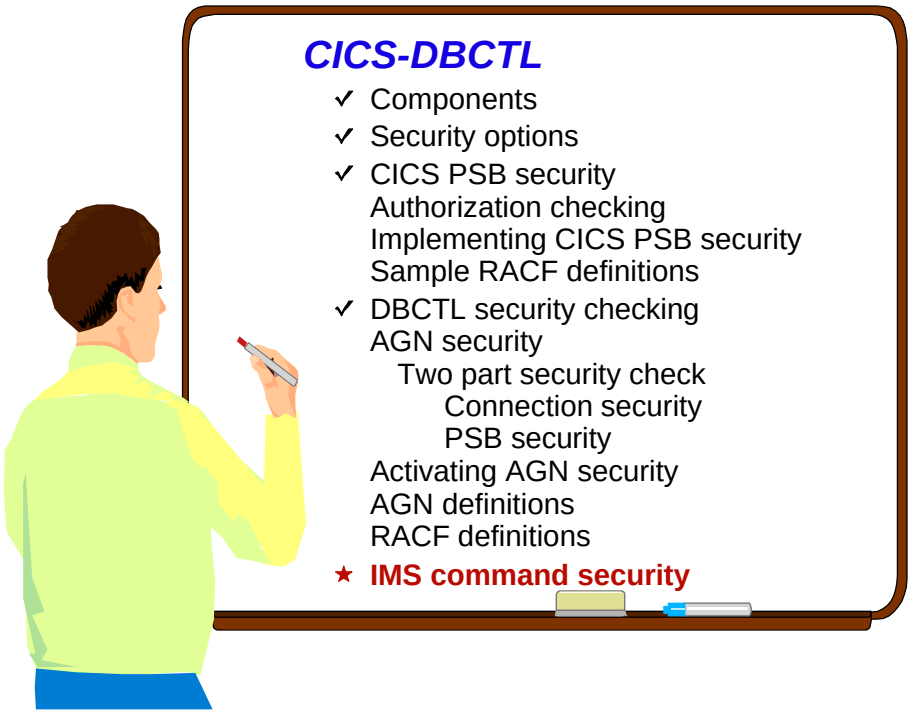
DBCTL PSB Scheduling Security



AGN Security Check Failures

DFS2854A jobname, stepname, region, reason--FAILED SECURITY CHECK

Code (HEX)	MEANING
004	AGN is not defined to RACF.
008	USER (CICS userid) is not authorized to use the specified AGN.
00C	RACF is inactive and class Axxx is active.
020	AGN is not defined in DFSAGT0x.
040	GETMAIN failed.
100	AGT entry address invalid.
104	PSBNAME is not included in the specified AGT entry.



IMS Commands Issued By CICS Users

- **CDBM**
  - CICS supplied transaction to issue DBCTL commands
  - Supports
    - DL/I Issue Command (ICMD) call
      - Issue a subset of IMS operator commands
    - DL/I Get Message (GMSG) call
      - Retrieve (get) messages 1st segment of command response from AO exit routine DFSAOE00
    - DL/I Retrieve Command (RCMD) call
      - Retrieve 2nd and subsequent command response segments from AO exit routine DFSAOE00

CDBM CICS Transaction

```
CDBM                    CICS-DBCTL Operator Transaction
98.135

13:24:20

Type the IMS command.
                  /DIS  DB CUSTOMER._____________________________________
                        _____________________________________________________
                        _____________________________________________________
                        _____________________________________________________


For /DBDUMP or /DBRECOVERY commands
    Choose one. __ 1.  Do not force end of volume
                   2.  Force end of volume

Press enter to display responses.


CICS APPLID CICSA
DBCTL ID IMSA


F1=Help      F2=Maintenance      F3=Exit      F5=Refresh      F12=Cancel
```

CDBM CICS Transaction ...

- **CDBM transaction authorization**
  - Security processing to determine if the CICS ***end user's userid*** is authorized to enter CICS automated operator transaction
  - Security checking is performed by CICS and RACF

- **Execution of the command in DBCTL**
  - Security processing to determine if ***userid of the CICS subsystem*** is authorized to issue the command in IMS
  - IMS start up parameter AOIS= influences whether automated operator issued commands are allowed
  - If AO commands are allowed, security checking performed by IMS and RACF

IMS Automated Operator Command Security

- **IMS commands issued from CICS environments may be secured**
  - DL/I ICMD security options
    - Controlled by IMS AOIS= startup parameter

- **AOIS=*N* | S | R | C | A**
  - **N** ICMD call ***cannot*** be issued (default)
  - **S** Skip command authorization, all application programs can issue ICMD calls
  - **R** RACF will perform command authorization
  - **C** Command Authorization Exit Routine (DFSCCMD0) will perform command authorization
  - **A** Call RACF first, then DFSCCMD0 for final command authorization

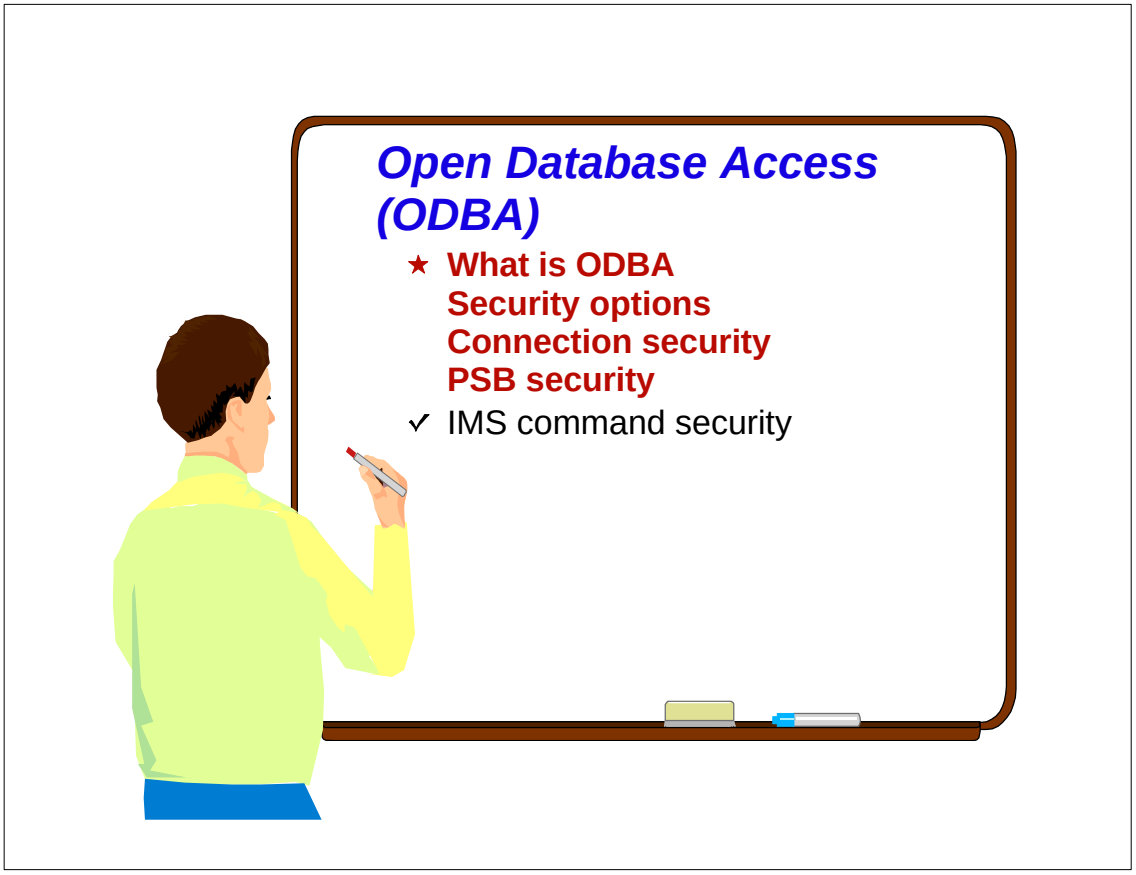
Authorizing the CICS Userid

- **RACF**
  - Authorize the userid of CICS to command profiles
    - CIMS | DIMS resource classes
- **Command Authorization Exit Routine (DFSCCMD0)**
  - Can be coded to perform command verb and keyword security checking
- **Both RACF and DFSCCMD0**
  - RACF called first
    - Return code passed to DFSCCMD0
  - DFSCCMD0 called for final decision
    - Has access to command string

Sample RACF Commands

Examples of RACF commands to authorize the userid of the CICS address space to IMS commands:

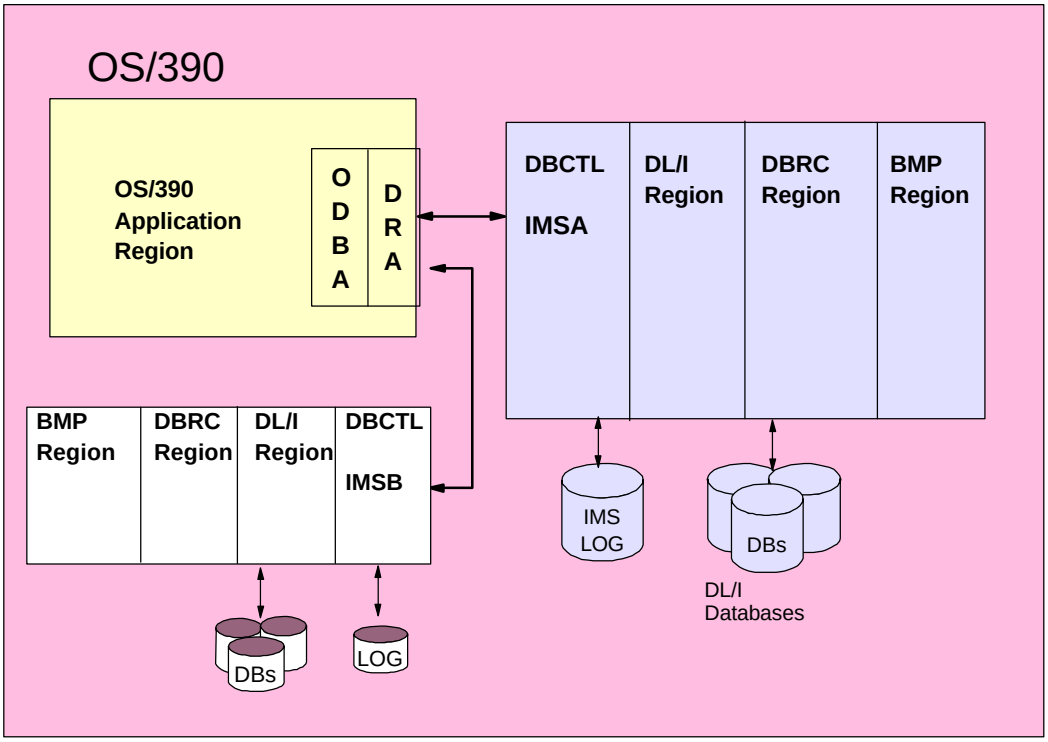
```
RDEFINE CIMS DIS OWNER(IMSADMIN) UACC(NONE)
PERMIT DIS CLASS(CIMS) ID(IMSGRP CICSA) ACCESS(READ)


RDEF DIMS IMSUSER ADDMEM(DBR STA STO)
      OWNER(IMSADMIN) UACC(NONE)
PERMIT IMSUSER CLASS(DIMS) ID(CICSA IMSGRP)
    ACCESS(READ)
```



What Is Open Database Access (ODBA)?

- **ODBA is a callable interface**
  - Resides in OS/390 address space
    - Address space ***recognized by IMS*** as an OS/390 application region
- **Provides ability to access IMS-managed databases from any OS/390 application**
  - Such as DB2 stored procedure address space
- **The OS/390 application**
  - Issues DL/I calls
  - Uses OS/390 Recovery Resource Services (RRS) as the sync-point manager
- **Application and IMS must coexist on same OS/390 image**

ODBA and DBCTL Address Spaces



ODBA Security Options

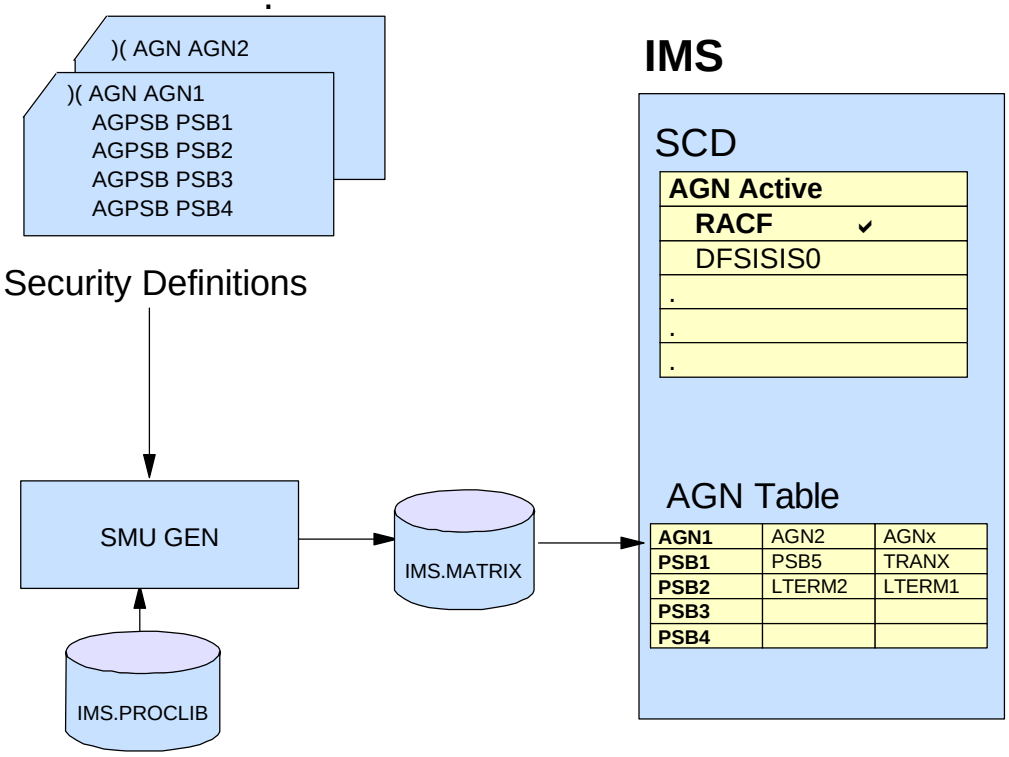
- **Application Group Name (AGN) security**
  - Controls connection of OS/390 address space to DBCTL
  - Allocation of program specification block (PSB)

- **IMS command authorization options**
  - Control security for commands issued by automated operator programs running in OS/390 address spaces
  - Standard ICMD security applies
    - AOIS=***N*** | S | R | C | A
    - RACF CIMS | DIMS profiles
    - Command Authorization Exit Routine (DFSCCMD0)
    - Both RACF and DFSCCMD0

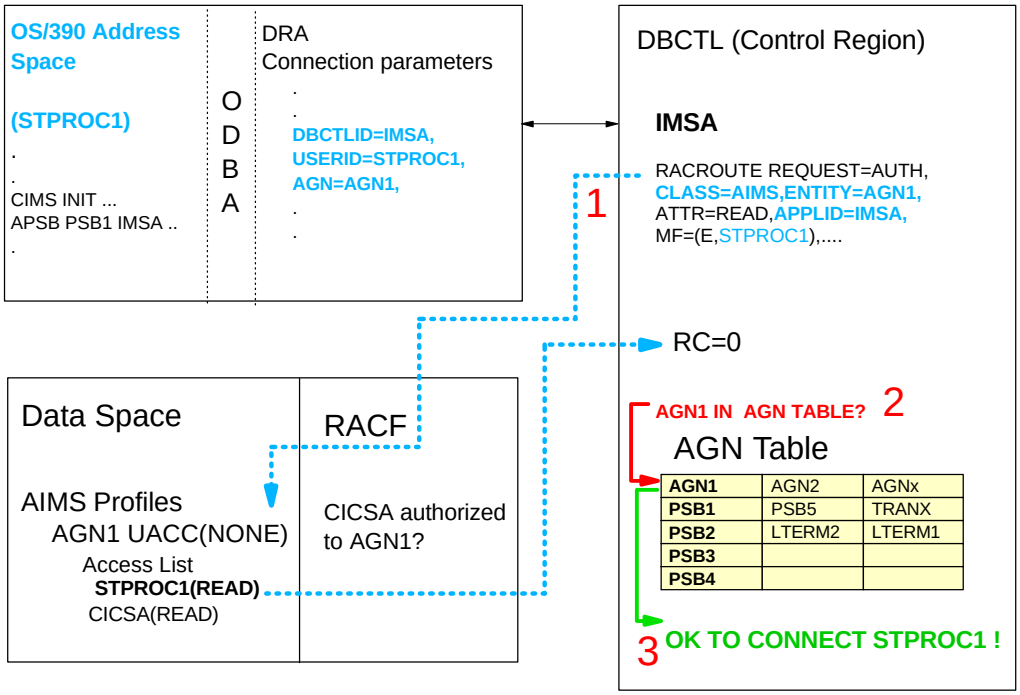
ODBA Connection and PSB Security

- **ODBA application access to DBCTL is controlled by Application Group Name (AGN) security**
  - Works like CICS access to DBCTL using AGN
  - Different Database Resource Adapter (DRA) generated for OS/390 applications
- **AGN security activated in DBCTL by**
  - SECURITY TYPE=(RACFAGN) or ISIS=1, or SECURITY TYPE=(AGNEXIT) or ISIS=2
- **Security definitions required**
  - Security Maintenance Utility (SMU) generation
    - Define AGNs and specify PSBs
    - PSB requested by OS/390 address space must be included in AGN
  - RACF profiles created in AIMS or Axxxxxx class
    - Userid(s) of OS/390 address space(s) must be authorized to connect to IMS

AGN Definitions



DBCTL AGN Connection Security

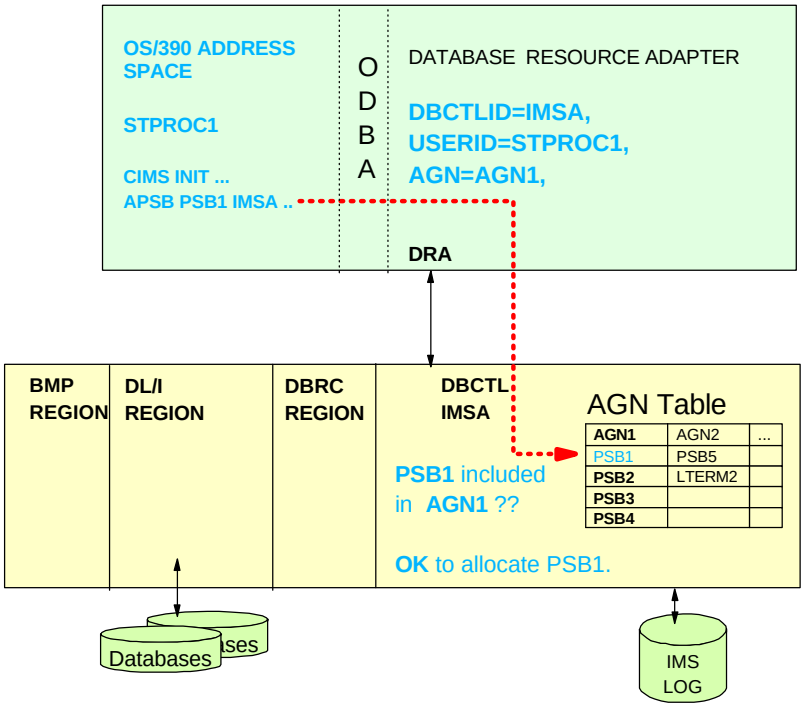


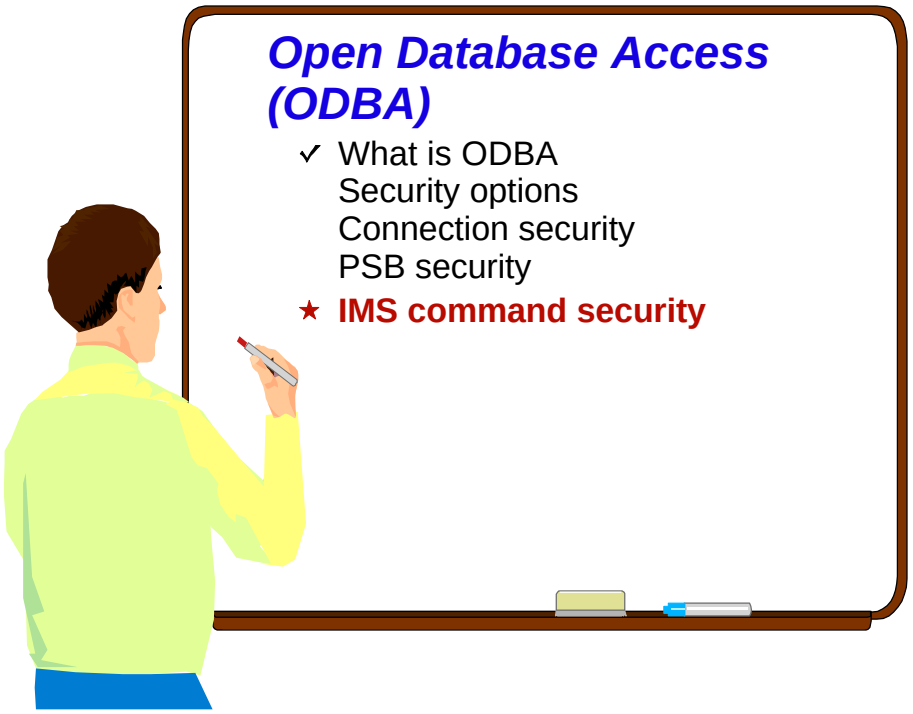
RACF Definitions

RDEFINE AIMS **AGN1** OWNER(IMSADMIN) UACC(NONE)
PERMIT AGN1 CLASS(AIMS) ID(*OS390_addrspace_userid*)
ACCESS(READ)

RDEFINE AIMS **AGN1** OWNER(IMSADMIN) UACC(NONE)
PERMIT AGN1 CLASS(AIMS) ID(STPROC1)
ACCESS(READ)

DBCTL - ODBA PSB Scheduling Security





IMS Automated Operator Command Security

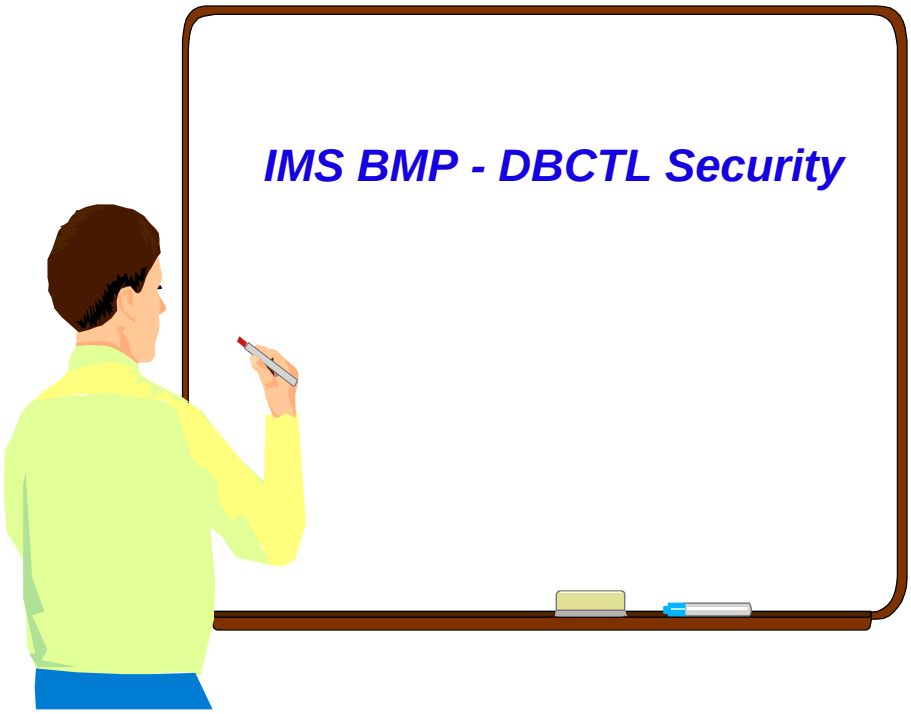
- **IMS commands issued from ODBA environments may be secured**
  - DL/I ICMD security options
    - Controlled by IMS AOIS= startup parameter
    - Implemented using RACF, DFSCCMD0, or both
- **AOIS=*N* | S | R | C | A**
  - **N** ICMD call ***cannot*** be issued (default)
  - **S** Skip command authorization, all application programs can issue ICMD calls
  - **R** RACF will perform command authorization
  - **C** Command Authorization Exit Routine (DFSCCMD0) will perform command authorization
  - **A** Call RACF first, then DFSCCMD0 for final command authorization

Authorizing the OS/390 Address Space Userid

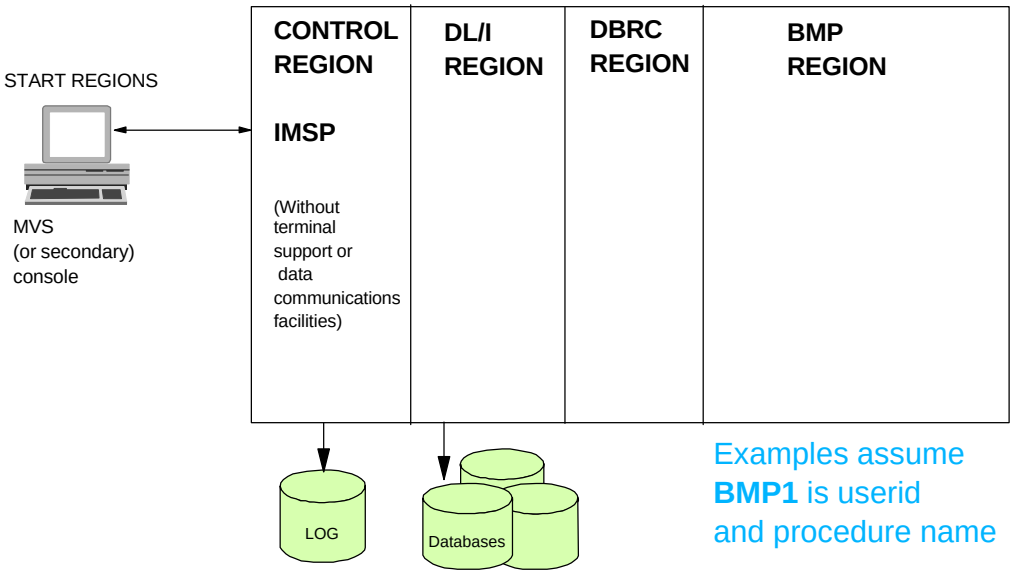
- **RACF**
  - Authorize the userid of the OS/390 address space to command profiles
    - Create profiles in CIMS | DIMS resource classes
- **Command Authorization Exit Routine (DFSCCMD0)**
  - Can be coded to perform command verb and keyword security checking
- **Both RACF and DFSCCMD0**
  - RACF called first
    - Return code passed to DFSCCMD0
  - DFSCCMD0 called for final decision
    - Has access to command string

Sample RACF Commands

```
RDEFINE CIMS DIS OWNER(IMSADMIN) UACC(NONE)
PERMIT DIS CLASS(CIMS) ID(STPROC1 GROUPX CICSA)
   ACCESS(READ)

RDEF DIMS IMSUSER ADDMEM(DBR STA STO)
      OWNER(IMSADMIN) UACC(NONE)
PERMIT IMSUSER CLASS(DIMS) ID(STPROC1 CICSA GROUPY)
    ACCESS(READ)
```

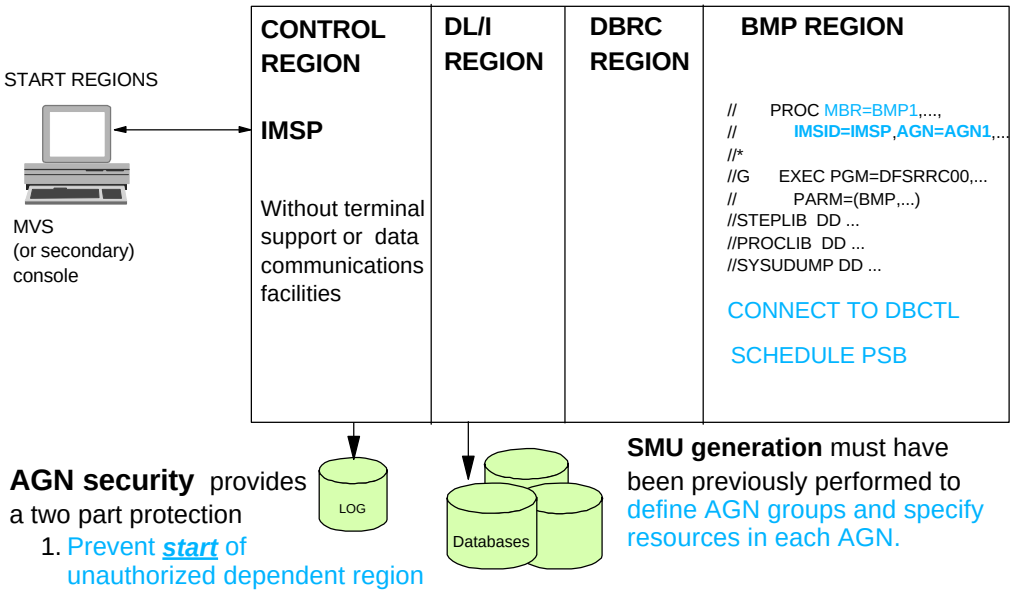


DBCTL Environment - BMP Region



Examples assume **BMP1** is userid and procedure name

DBCTL Environment - BMP AGN Security



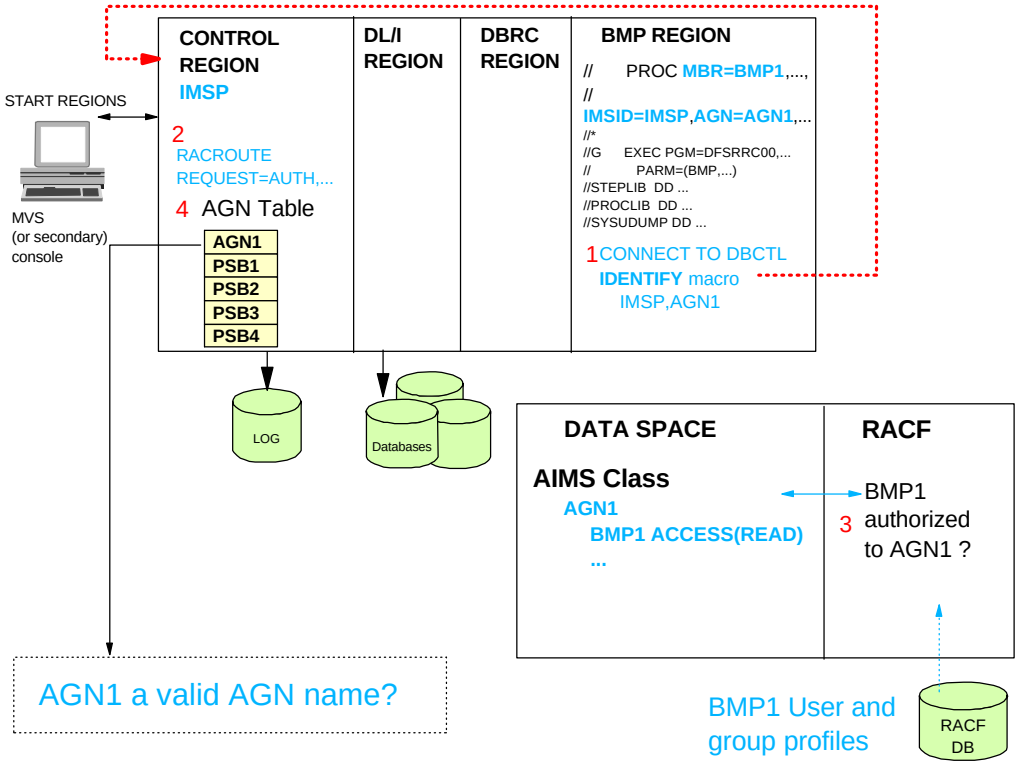
AGN security provides a two part protection

1. Prevent ***start*** of unauthorized dependent region
2. Prevent ***use*** of unauthorized resources (i.e. PSB) in dependent region

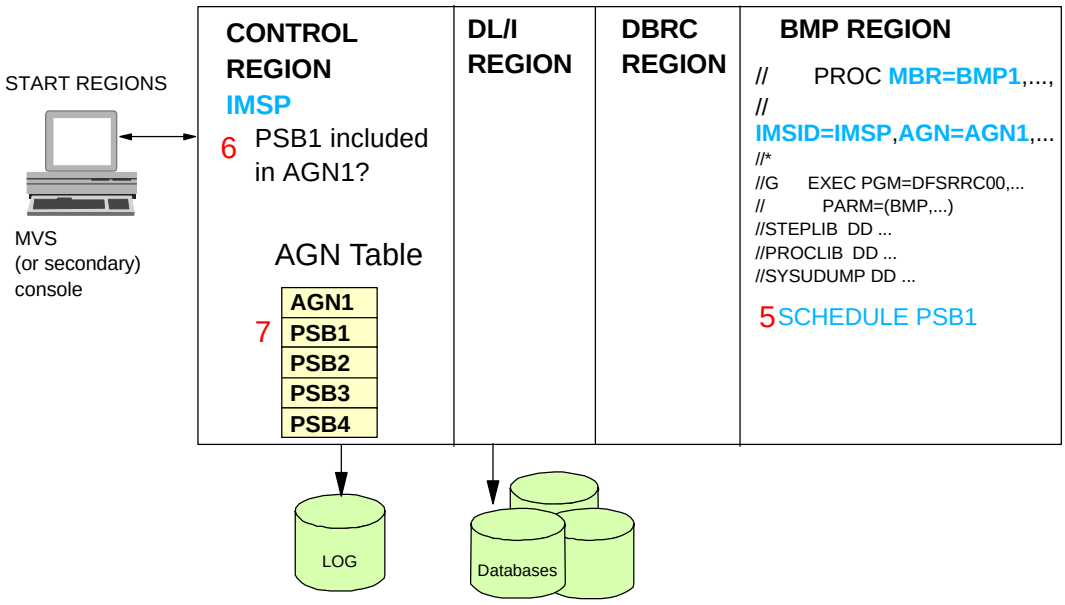
SMU generation must have been previously performed to define AGN groups and specify resources in each AGN.

RACF AIMS profiles must have been previously defined to authorize start of dependent region that request specific AGN.

BMP Connect To DBCTL



BMP Resource Request



Automated Operator BMP Programs

- **Same as for CICS and ODBA**
- **Ability to issue IMS commands set by**
  - AOIS=***N*** | S | R | C | A
    - **N** ICMD call ***cannot*** be issued (default)
    - **S** Skip command authorization, all application programs can issue ICMD calls
    - **R** RACF will perform command authorization
      - CIMS | DIMS resource class profiles
    - **C** Command Authorization Exit Routine (DFSCCMD0) will perform command authorization
    - **A** Call RACF first, then DFSCCMD0 for final command authorization
- **RACF command profiles required in CIMS | DIMS**
  - See CICS and ODBA examples

Summary

- **DBCTL**
  - IMS Database manager
- **Security philosophy**
  - Perform as much security checking as possible on source system
    - i.e. where transaction/command entered
- **DBCTL resources may be secured using**
  - Application group name (AGN) security
    - CICS
    - OS/390 address space using ODBA
    - IMS batch message processing (BMP) regions
- **CICS offers additional (or in lieu of) security**
  - CICS PSB security checking
    - Authorize CICS end user to CICS PSB
  - CICS transaction and/or terminal authorization

RETURN TO INDEX

GO TO PART 2